Van: art 5 1-2e
Verzonden: 2023-09-28 21:49:03+00:00
Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: Re: Advies datalek A 103135
"
Akkoord, art 5 1-2e

<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAAb9ysg&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl%7C52f9d29b156645803c7608dbc05bf81a%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638315273456568688%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=tWW1C%2F1M7okVakJgQCBaVjgwlG7IRkSp%2FvNjPcRxKc4%3D&reserved=0>

Met vriendelijke groet,

art 5 1-2e art 5 1-2e
Functionaris voor Gegevensbescherming

Gerechtelijk Deskundige

<olm://attachment/AQADAAAAyQAAAAAAAAAAM74HAAAAAAAA1AAAAAAABD9sAAAAAAAHvjMAAAAAAAQ_bAMAAIAAAAAAJW5lLmJvbnNAcHpoLm5sX0FjdGl2ZVN5bmNFeGNoYW5nZV9IeFM%3D/AQADAAABagAAAAAAAAAAPL4HAAAAAAABZwAAAAAABD1TAAAAAAAHvjwAAAAAAAQ9UwMAAIAAAAAAJW5lLmJvbnNAcHpoLm5sX0FjdGl2ZVN5bmNFeGNoYW5nZV9IeFM%3D>

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e %40pzh.nl%7C52f9d29b156645803c7608dbc05bf81a%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638315273456568688%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=XWgKxpOfdZsQ8Kq5xvE1W6Vgz4x0MJoPpW5CSLJacYI%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

From: art 5 1-2e < art 5 1-2e pzh.nl>
Sent: Thursday, September 28, 2023 4:18:52 PM
To: art 5 1-2e < art 5 1-2e pzh.nl>
Cc: art 5 1-2e < art 5 1-2e pzh.nl>
Subject: Advies datalek A 103135

Ha art 5 1-2e

Bijgaand het concept-advies voor datalek A 103135. Ik hoor graag of je akkoord gaat.

Groeten,

art 5 1-2e

art 5 1-2e

Privacy Officer

Eenheid Privacy

T art 5 1-2e

M

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e %40pzh.nl%7C52f9d29b156645803c7608dbc05bf81a%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638315273456568688%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=XWgKxpOfdZsQ8Kq5xvE1W6Vgz4x0MJoPpW5CSLJacYI%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Krachtig Zuid-Holland.

Van: loket@pzh.nl <loket@pzh.nl>
Verzonden: woensdag 27 september 2023 19:43
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; privacy <privacy@pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Melding mogelijk datalek A 103135

Beste collega,

Er is een melding gedaan van een mogelijk datalek:

Zie voor meer informatie:
Activiteitnummer: A 103135
Wijzigingsnummer: W23 09 00309

Hier kan je de activiteit <https://eur03.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fpvzh.topdesk.net%2Ftas%2Fsecure%2Fcontained%2Fchangeactivity
%3Funid%3Dcfa1f9ae1a864b04aa9e0d6d4d73ce2b&data=05%7C01%7 art 5 1-2e art 5 1-2e 40pzh.nl
%7C52f9d29b156645803c7608dbc05bf81a
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638315273456568688%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=rgOhBFyIbgxhm8VKWHztnbqHqvWLDTqpx0hfu%2BDnhRs
%3D&reserved=0> bekijken.

Met vriendelijke groet,

<HTTPS://pvzh.topdesk.net/tas/images/email_footer.jpg>

Het Loket telefoon 070 4417777 pvzh.topdesk.net
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Fpvzh.topdesk.net%2F&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7C52f9d29b156645803c7608dbc05bf81a
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638315273456568688%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=%2BqCg8mcTD6LTDS%2FRKrf6iB5XtVQ2zJH4u7DmoDbsDzI
%3D&reserved=0>

"


provincie
Zuid-Holland

Van: art 5 1-2e
Verzonden: 2023-10-06 15:45:05+00:00
Aan: art 5 1-2e
CC:
Onderwerp: FW: Datalek Youforce: advies melden aan AP
"
Hoi art 5 1-2e

Antwoord voor in het dossier.

Met vriendelijke groet,

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e
%40pzh.nl
%7Ced35f6c6fa3b4a831d4408dbc6727272%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638321967092194150%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=HtmCfR66p
%2BFHeFJGsjyHxGrLO0pa3e7uDUgHTidXf08%3D&reserved=0>

Werkdagen: ma, di, wo (middag), do, vr (ochtend)

Krachtig Zuid-Holland

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: vrijdag 6 oktober 2023 15:35
Aan: art 5 1-2e < art 5 1-2e pzh.nl>

CC: art 5 1-2e <art 5 1-2e pzh.nl>; Frank Rijkaart <f.rijkaart@pzh.nl>; privacy <privacy@pzh.nl>
Onderwerp: FW: Datalek Youforce: advies melden aan AP

Dag art 5 1-2e

Dankjewel. Voor de eerste keer volg ik je advies niet helemaal.

Ik zal dat toelichten. Secretaresses hebben een vergaande vertrouwensfunctie en doen veel inhoudelijk-administratieve handelingen af voor hun manager, daar is inderdaad allerlei soort van informatie mee gemoeid. Daartoe 'zijn ze op aarde' zogezegd, dit deel van de functie opheffen is mijns inziens een illusie, dan mogen managers dat allemaal zelf gaan doen wat letterlijk ondoenlijk is. Anderzijds neem ik de melding wel degelijk serieus, want de melding lijkt er (deels/mogelijk) op te duiden dat rechten voor bepaalde secretaresses mogelijk te ruim staan afgesteld. Maar dat wil ik dan eerst nog wel zien of dat inderdaad zo is.

Daarom kom ik tot het volgende besluit:

* Deze situatie wel intern registreren als mogelijk datalek, maar níet melden aan de AP.
* Ik ga zo aan een directeur art 5 1-2e de opdracht geven een en ander zorgvuldig uit te zoeken: hoe ziet de functiebeschrijving van een secretaresse er dienaangaande uit, in welk beleid is dit wel/niet geborgd, zijn de rechten goed afgesteld, e.d. Ik kom over een tijdje terug met de resultaten van dit onderzoek en, áls nodig, te ondernemen acties.

Hartelijke groet, art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> >
Verzonden: vrijdag 6 oktober 2023 13:58
Aan: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
CC: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; Frank Rijkaart <f.rijkaart@pzh.nl <mailto:f.rijkaart@pzh.nl> >; privacy <privacy@pzh.nl <mailto:privacy@pzh.nl> >
Onderwerp: Datalek Youforce: advies melden aan AP

Beste art 5 1-2e

We hebben een melding gekregen dat 9 personen van de secretariële ondersteuning in Youforce zijn gemachtigd om voor in totaal 21 P-managers werkzaamheden uit te voeren in Youforce binnen het proces 'self-service' (denk aan ziekmeldingen, beheren nieuwe medewerkers, etc.). Daarmee hebben deze 9 personen toegang gehad tot een volledige set aan personeelsgegevens van - naar schatting – ruim 400 medewerkers, waaronder bijzondere persoonsgegevens (ziekmeldingen) en gevoelige persoonsgegevens (zoals financiële gegevens en gegevens van het goede gesprek). Dit is meer dan nodig is voor de uitvoering van de werkzaamheden als secretariële ondersteuning. Deze taken behoren - gelet op het gevoelige karakter - uitgevoerd te worden door de P-managers zelf.

Omdat er toegang is geweest tot gegevens die niet nodig zijn en niet bedoeld zijn voor het uitvoeren van de functie secretariële ondersteuning kwalificeert dit voorval als een datalek. Omdat het mede gaat om bijzondere- en gevoelige persoonsgegevens adviseren wij van dit datalek een melding te doen bij de AP.

Graag hoor ik per ommegaande of je ons advies volgt. De termijn van 72 uur voor melden aan de AP loopt namelijk in het weekend af.

Met vriendelijke groet,

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e %40pzh.nl
%7Ced35f6c6fa3b4a831d4408dbc6727272%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638321967092194150%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=HtmCfR66p
%2BFHeFJGsjyHxGrLO0pa3e7uDUgHTidXf08%3D&reserved=0>

Werkdagen: ma, di, wo (middag), do, vr (ochtend)

Krachtig Zuid-Holland

"


provincie
Zuid-Holland

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e (FG)
Registratienummer van het incident	:	M23 10 00723
Datum en tijdstip van de melding	:	5 oktober 2023, 15:50
Route van de melding	:	melding bestanden in te zien zonder de juiste rechten (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e art 5 1-2e
Datum en tijdstip advies	:	6 oktober 2023 11:06
Advies besproken met	:	Besproken met art 5 1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Gedeeld met eenheid Privacy

Situatie

Inzage in teveel persoonsgegevens in Youforce door medewerkers die deze gegevens niet nodig hebben voor de uitoefening van hun functie. Er zijn 9 personen gemachtigd om (voor 21 P-managers) ziek- en betermeldingen te doen en nieuwe medewerkers toe te voegen in Youforce. Deze medewerkers kunnen dan naast deze gegevens ook andere personeelsgegevens inzien die behoren tot het 'self-service' proces van managers.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Onbekend.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Zeker 9.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	In principe alles.
Welke persoonsgegevens betreft het?	NAW-gegevens Schaal Salaris Toelage Opleidingsgegevens Ziek- en betermeldingen Contract beëindigen Boter bij de vis Invoeren externen

Vraag	Antwoord
	Verlengen dienstverband Overplaatsing Declaraties Lief en leed Buitengewoon verlof Goede gesprek Archief van ingevoerde mutaties
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Gezondheidsgegevens
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Negen personen in de secretariële ondersteuning zijn gemachtigd om voor 21 p-managers zaken in Youforce (proces 'self-service') te regelen. Geschat wordt dat het gaat om persoonsgegevens van 400-500 betrokkenen werkzaam bij PZH.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Ja. Naast gezondheidsgegevens ook gevoelige gegevens zoals financiële gegevens en gegevens over goede gesprek.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja.
Betreft het een datalek?	Ja.
Ondernomen beperkende maatregelen.	Geen.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Bestaande machtigingen moeten per direct worden ingetrokken. Daarnaast moet worden gezorgd dat er in de toekomst geen machtigingen meer worden afgegeven aan secretariële ondersteuning om zaken voor een p-manager in Youforce te regelen. Er moet ook gecommuniceerd worden dat p-managers dit uitsluitend zelf mogen doen, of bij afwezigheid een andere p-manager machtigen.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

<u>Analyse van dit specifieke geval</u>
Er zijn 9 (negen) personen in de secretariële ondersteuning gemachtigd om handelingen in Youforce uit te voeren die eigenlijk door een p-manager gedaan moeten worden. Er is daardoor voor deze 9 personen (ten behoeve van 21 p-managers) toegang tot alle persoonsgegevens binnen het proces ‘self-service’. Het uitvoeren van de taken binnen het proces ‘self-service’ behoort tot de functie van P-managers zelf en niet tot de functie van secretariële ondersteuning. De 9 personen hebben dus toegang tot meer gegevens dan voor hun functie noodzakelijk is. Tot de persoonsgegevens die inzichtelijk zijn horen naast gewone persoonsgegevens ook gegevens over iemands gezondheid (bijzondere persoonsgegevens) en gegevens over financiële situatie en functioneren, gevoelige gegevens dus.

Conclusie en advies
De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt WEL gemeld bij de Autoriteit Persoonsgegevens of betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e (FG)
Registratienummer van het incident	:	M23 10 00723
Datum en tijdstip van de melding	:	5 oktober 2023, 15:50
Route van de melding	:	melding bestanden in te zien zonder de juiste rechten (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e art 5 1-2e
Datum en tijdstip advies	:	6 oktober 2023 11:06
Advies besproken met	:	Besproken met art 5 1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Gedeeld met eenheid Privacy

Situatie

Inzage in teveel persoonsgegevens in Youforce door medewerkers die deze gegevens niet nodig hebben voor de uitoefening van hun functie. Er zijn 9 personen gemachtigd om (voor 21 P-managers) ziek- en betermeldingen te doen en nieuwe medewerkers toe te voegen in Youforce. Deze medewerkers kunnen dan naast deze gegevens ook andere personeelsgegevens inzien die behoren tot het 'self-service' proces van managers.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Onbekend.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Zeker 9.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	In principe alles.
Welke persoonsgegevens betreft het?	NAW-gegevens Schaal Salaris Toelage Opleidingsgegevens Ziek- en betermeldingen Contract beëindigen Boter bij de vis Invoeren externen

Vraag	Antwoord
	Verlengen dienstverband Overplaatsing Declaraties Lief en leed Buitengewoon verlof Goede gesprek Archief van ingevoerde mutaties
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Gezondheidsgegevens
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Negen personen in de secretariële ondersteuning zijn gemachtigd om voor 21 p-managers zaken in Youforce (proces 'self-service') te regelen. Geschat wordt dat het gaat om persoonsgegevens van 400-500 betrokkenen werkzaam bij PZH.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Ja. Naast gezondheidsgegevens ook gevoelige gegevens zoals financiële gegevens en gegevens over goede gesprek.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja.
Betreft het een datalek?	Ja.
Ondernomen beperkende maatregelen.	Geen.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Bestaande machtigingen moeten per direct worden ingetrokken. Daarnaast moet worden gezorgd dat er in de toekomst geen machtigingen meer worden afgegeven aan secretariële ondersteuning om zaken voor een p-manager in Youforce te regelen. Er moet ook gecommuniceerd worden dat p-managers dit uitsluitend zelf mogen doen, of bij afwezigheid een andere p-manager machtigen.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

<u>Analyse van dit specifieke geval</u>
Er zijn 9 (negen) personen in de secretariële ondersteuning gemachtigd om handelingen in Youforce uit te voeren die eigenlijk door een p-manager gedaan moeten worden. Er is daardoor voor deze 9 personen (ten behoeve van 21 p-managers) toegang tot alle persoonsgegevens binnen het proces ‘self-service’. Het uitvoeren van de taken binnen het proces ‘self-service’ behoort tot de functie van P-managers zelf en niet tot de functie van secretariële ondersteuning. De 9 personen hebben dus toegang tot meer gegevens dan voor hun functie noodzakelijk is. Tot de persoonsgegevens die inzichtelijk zijn horen naast gewone persoonsgegevens ook gegevens over iemands gezondheid (bijzondere persoonsgegevens) en gegevens over financiële situatie en functioneren, gevoelige gegevens dus.

Conclusie en advies
De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt WEL gemeld bij de Autoriteit Persoonsgegevens of betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.

Van: art 5 1-2e
Verzonden: 2023-10-24 22:40:17+00:00
Aan: art 5 1-2e
CC:
Onderwerp: Fw: Data IDMS
"

From: art 5 1-2e < art 5 1-2e pzh.nl>
Sent: Sunday, October 1, 2023 8:19 PM
To: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Subject: RE: Data IDMS

Beste collega’s,

Deze e-mail vraagt tijdige actie van een aantal van ons morgen denk ik. art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e en ik houden iedere ochtend om 09.00 uur een stand up van 15 minuten. Ik stuur de uitnodiging aan jullie door met het verzoek aan degenen die naar aanleiding van de opmerkingen van art 5 1-2e inhoudelijke input moeten/willen leveren om morgenochtend even aan te sluiten.

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art 5 1-2e art 5 1-2e 40pzh.nl%7Ca0355e0e2358420e3e2708dbd4d16ec9%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638337768205858744%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=Gd6xwqDqvJAcDM0cQQGaO1psW%2BtvAIwSA%2FUVYZ6K5XU%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: zaterdag 30 september 2023 17:25
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: FW: Data IDMS
Gevoeligheid: Vertrouwelijk

Beste art 5 1-2e en alle anderen,

Ik heb het allemaal gelezen, er een nachtje over geslapen, opnieuw gelezen, en dan nu mijn reactie. In drie punten:

1. Heel veel dank voor de gepleegde inspanning en inzet om dit op zo korte termijn op papier te krijgen door jullie!
2. Ik heb nog enkele vragen/opmerkingen bij de verschillende stukken. Die som ik hieronder op.
3. Alles overziende, zie ik dat er allerlei lopende activiteiten zijn die stukjes van de hele puzzel bevatten (informatietransitie, nieuw beleid IenA, GS-nota, BIO, e.d.). Maandag zal ik aan de orde stellen hoe we komen tot een samenhangend Plan van Aanpak / samenhangend Overzicht van de totale puzzel, met aandacht voor systemen, processen, gedrag en verantwoordelijkheden, inclusief een kalender.

Dan de uitwerking van bovenstaande punt 2:

* Memo data idsm: graag de notie toevoegen dat we meerdere zelfgecreëerde lekken netjes gaan melden + ik lees nix over de FG die de afgelopen maanden onderzoek deed en mij daarvan via een brief op de hoogte stelde + ik zoek in deze notitie of ergens anders een timeline van de afgelopen paar weken waarin we steeds opeenvolgende iteraties doen van onderzoek&actie + ik mis nog de update van de 2 tabellen vorige week in de presentatie met allerlei kolommen waarin aantal staan per zoekterm + in de paragraaf ‘verantwoordelijkheden tav idsm’ worden vanuit OGO verantwoordelijkheden geduid maar waarop is dat gebaseerd?
* Memo datalek: wat betekent ECM + in 2016 is blijkbaar besloten 6 mln uit te trekken voor vervanging idms, is dat toen ook gebeurd?
* Memo beschrijving idsm: graag aanvullen met inzicht hoe het geregeld is met rechtenbeheer/autorisaties.

Tenslotte, nogmaals veel dank. Zou het jullie mogelijk zijn maandag einde dag de genoemde opmerkingen verwerkt te hebben? Dan ga ik er dinsdag mee richting DT en gedeputeerde.

Hartelijke groet, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 29 september 2023 16:39
Aan: art 5 1-2e art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >; art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e art 5 1-2e

< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Data IDMS
Gevoeligheid: Vertrouwelijk

Beste art 5 1-2e

Zoals afgesproken hierbij een memo over het proces tot op heden, een blik op de te ondernemen acties en de bredere context om een en ander in perspectief te plaatsen. Daarnaast vind je als bijlagen een document over IDMS en een document over de weg naar informatietransitie aan. Tot slot de planning op hoofdlijnen t/m 5 oktober.

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art 5 1-2e art 5 1-2e 40pzh.nl%7Ca0355e0e2358420e3e2708dbd4d16ec9%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638337768205858744%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=Gd6xwqDqvJAcDM0cQQGaO1psW%2BtvAIwSA%2FUVYZ6K5XU%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

"


provincie
Zuid-Holland

Van: art 5 1-2e
Verzonden: 2023-10-24 22:40:58+00:00
Aan: art 5 1-2e
CC:
Onderwerp: Fw: Spoedoverleg datalek
"

From: art 5 1-2e < art 5 1-2e pzh.nl>
Sent: Thursday, September 21, 2023 4:57 PM
To: art 5 1-2e < art 5 1-2e pzh.nl>
Cc: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Subject: RE: Spoedoverleg datalek

Voor onze afspraak morgen kunnen ook uitgenodigd worden:

* Functioneel behee art 5 1-2e
* BI team - art 5 1-2e art 5 1-2e

Groet,

art 5 1-2e

-----k-----
Van: art 5 1-2e pzh.nl>
Verzonden: donderdag 21 september 2023 11:40
Aan: art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: Spoedoverleg datalek
Tijd: donderdag 21 september 2023 14:00-14:45 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
Locatie: Microsoft Teams-vergadering
Urgentie: Hoog
Gevoeligheid: Privé

In overleg met art 5 1-2e Overleg vindt plaats via ms teams, duur +/- 30-45 min.

art 5 1-2e 1-09-2023

Microsoft Teams-vergadering

Neem deel vanaf uw computer, mobiele app of apparaat voor vergaderruimte

Klik hier om deel te nemen aan de vergadering
<https://teams.microsoft.com/l/meetup-join/19%3ameeting_MWVjZmNjZmMtMjhiYS00NjIwLTk1NTAtZDc1MjFhMWJiOTM2%40thread.v2/0?context=%7b%22Tid%22%3a%226d99bc28-8f28-4a73-a501-63a8e1eb3040%22%2c%22Oid%22%3a%2260ca2822-a24e-466f-858d-0b2687af1079%22%7d>

Vergadering-id: 392 270 975 314
Wachtwoordcode: zrL98A

Teams downloaden <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.microsoft.com%2Fen-us%2Fmicrosoft-teams%2Fdownload-app&data=05%7C01 art 5 1-2e art 5 1-2e 40pzh.nl%7C56f3ef088b0e40043ca408dbd4d18770%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638337768598963755%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=yls%2BGC%2FDGU2xrQaU%2B%2F%2Fd7eAoEu%2FsE1Iz%2Bc9ivg7zUaY%3D&reserved=0> | Deelnemen op het web <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.microsoft.com%2Fmicrosoft-teams%2Fjoin-a-meeting&data=05%7C01% art 5 1-2e art 5 1-2e %40pzh.nl%7C56f3ef088b0e40043ca408dbd4d18770%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638337768598963755%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=%2Bow7Pb%2BpOVznhGYdArMc%2FgVvTPls%2FQ25s%2BJDn5aK%2F7c%3D&reserved=0>

Meer informatie <https://eur03.safelinks.pr tion.outlook.com/?url=https%3A%2F%2Faka.ms%2FJoinTeamsMeeting&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl%7C56f3ef088b0e40043ca408dbd4d18770%7C6d99b f284a73a50163a8e1eb3040%7C0%7C0%7C638337768598963755%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=z%2BHR3WilOrcSWTfLcQGceVNXwLCwEBfNZ5Nl%2BE7nyUw%3D&reserved=0> | Opties voor vergadering <https://teams.microsoft.com/meetingOptions/?organizerId=60ca2822-a24e-466f-858d-0b2687af1079&tenantId=6d99bc28-8f28-4a73-a501-63a8e1eb3040&threadId=19_meeting_MWVjZmNjZmMtMjhiYS00NjIwLTk1NTAtZDc1MjFhMWJiOTM2@thread.v2&messageId=0&language=nl-NL>

"

Van: art 5 1-2e
Verzonden: 2023-10-25 14:26:54+00:00
Aan: art 5 1-2e
CC:
Onderwerp: FW: M23 03 03991 Datalek - printer postkamer
"
Tav. WOO datalek

art 5 1-2e

Adviseur Informatieveiligheid / CISO

Afdeling Informatisering & Automatisering

Bureau Advies & Beleid

art 5 1-2e

art 5 1-2e pzh.nl

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7Ccac6efc037a640bd4dd508dbd555acc0%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638338336165628545%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C
%7C&sdata=otnX2VfYMuDZoba4Uab3252zG5tLto6vtOuXJJz03Y0%3D&reserved=0>

Elke dag beter. Zuid-Holland

"


provincie
Zuid-Holland

Van: art 5 1-2e
Verzonden: 2023-10-25 14:25:24+00:00
Aan: art 5 1-2e
CC:
Onderwerp: FW: verstuurde versie
"
Tav. WOO datalek

art 5 1-2e

Adviseur Informatieveiligheid / CISO

Afdeling Informatisering & Automatisering

Bureau Advies & Beleid

art 5 1-2e

art 5 1-2e pzh.nl

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl%7Ccf46c73d9a2b4a6ab1fb08dbd55576b9%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638338335722343870%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=dPrIFXJJ3rdF79NLJClOVUdtjOUpGWtGjm2v4bZd0Y0%3D&reserved=0>

Elke dag beter. Zuid-Holland

"

provincie
Zuid-Holland

Van: art 5 1-2e
Verzonden: 2023-10-25 14:27:28+00:00
Aan: art 5 1-2e
CC:
Onderwerp: FW: RE- Datalek printer postkamer
"
Tav. WOO datalek

art 5 1-2e

Adviseur Informatieveiligheid / CISO

Afdeling Informatisering & Automatisering

Bureau Advies & Beleid

art 5 1-2e

art 5 1-2e pzh.nl

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7Cc4ab37220d654efae4ca08dbd555c0e2%7C6d99bc288f284a73a50163 eb3040%7C0%7C0%7
C638338336497818536%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=EXccxt1yw1a2qcp2WKdI2JhxDfKoZ1nQ08dRLR4jI8o
%3D&reserved=0>

Elke dag beter. Zuid-Holland

"


provincie
Zuid-Holland

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e (Afdeling FZ, inkoop)
Registratienummer van het incident	:	A 97 999
Datum en tijdstip van de melding	:	24-03-2023, 10:24
Route van de melding	:	Melding vermist ICT middel Security formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	24 maart 2023 om 13.00 uur
Advies besproken met	:	Besproken met art 5 1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Gedeeld met eenheid Privacy

Situatie: Vermiste laptop.

art 5 1-2e meldde:

Na afloop van een vergadering in de vergaderzaal Beresteijn op C3 ben ik naar het toilet geweest die om de hoek op C3 bij de vergaderzaal zich bevindt. Daarna naar de parkeergarage. tijdens het overleg heb ik mijn laptop gebruikt. Bij thuiskomst zag ik de laptop niet in mijn tas.

Locatie: PZH hoofdkantoor, C3 gebouw 3e etage, 23-3-2023, 17.03 uur

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Onbekend. Volgens art 5 1-2e onden er zowel werkgegevens als privé gegevens op de laptop.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend. De gegevens zijn versleuteld en het apparaat stond uitgeschakeld ten tijde van de diefstal.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Onbekend.
Welke persoonsgegevens betreft het?	Onbekend.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in	Onbekend.

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.

Vraag	Antwoord
artikel 9 AVG?	
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Onbekend.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Onbekend.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Onbekend.
Betreft het een datalek?	Ja.
Ondernomen beperkende maatregelen.	Melding aangemaakt, doorgezet naar team privacy: M23 03 0299 Wipe op afstand uitgevoerd. Wachtwoordreset uitgevoerd. CMDB aangepast. Gebruiker heeft diefstalformulier ingevuld. Vervangende laptop uitgegeven. Wijziging gesloten door bij de Status - 'Afgerond' Acties Eenheid Privacy - vermissing ICT middel De beveiliging is gevraagd of zij nog iets op de camerabeelden in het C-gebouw heeft kunnen zien.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Geen.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.

[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

<u>Analyse van dit specifieke geval</u>
PZH-laptop vermist na overleg op provinciehuis. Vermissing is pas thuis geconstateerd.
Op de laptop stonden er zowel werkgegevens als privé gegevens.
Diverse beveiligingsactiviteiten uitgevoerd. De Laptop is ‘gewiped’ en aan de medewerker is een nieuwe Laptop verstrekt. Wachtwoorden zijn gereset.

Conclusie en advies
De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt NIET gemeld bij de Autoriteit Persoonsgegevens of betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.

Ontvangstbevestiging van melding inbreuk

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596 AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

AUTORITEIT
PERSOONSGEGEVENS

[✓] Provincie

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	art 5 1-2e
Functie	Adviseur Informatieveiligheid
E-mailadres	art 5 1-2e @pzh.nl
Telefoonnummer	art 5 1-2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Ja

Geef aan welke andere organisaties betrokken waren bij de inbreuk?

Naam	Op welke wijze betrokken	Toelichting (optioneel)
PostNL	verzending	verloren tijdens hun proces

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Onbekend
(Mogelijke) startdatum van de inbreuk	24-8-2021
4.2 Wanneer is het incident ontdekt?	24-8-2021
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Leeg envelop aangetroffen
4.4 Is dit het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis	heeft gekregen van de inbreuk?

AUTORITEIT PERSOONSGEGEVENS

Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	USB stick met beelden van een brug is verloren geraakt bij het retour krijgen van de politie/recherche. Envelop aantroffen in ons postvak met schade. Mogelijk USB stick verloren gegaan bij het sorteerproces van PostNL

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Onbekend

U dient moet binnen twee 2 weken een vervolgmelding te doen indienen, waarin u aangeeft welke persoonsgegevens betrokken zijn bij het datalekgetroffen.

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("**-gegevensregisters**") zijn getroffen door het datalek	1

AUTORITEIT PERSOONSGEGEVENS

Geef een toelichting op bovengenoemd aantal:	Onbekend

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	onbekend
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Provincie Zuid-Holland is niet in staat om te achterhalen om welke beelden het gaat gezien de contactgegevens van de verzender ontbreken (meerdere politie-eenheden vragen beelden op) - De USB-stick is niet beveiligd
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1
Het maximum aantal betrokkenen is:	1

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

AUTORITEIT PERSOONSGEGEVENS

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Niet mogelijk om vast te stellen, gezien er geen kennis is van de inhoud.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Aanzienlijk
Licht uw keuze toe:	Er is onzekerheid of betrokkenen herkenbaar op beeld staan. Mochten de beelden na vondst misbruikt worden door de vinder, dan kan dit gevolgen hebben voor de persoonlijke levenssfeer van eventuele op beeld herkenbare betrokkenen. In zijn algemeenheid is, gezien de gevoelige aard van beeldmateriaal van incidenten, de kans groter dat de verwerking ervan leidt tot nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkenen. Bij bijzondere persoonsgegevens in de zin van de AVG is er per definitie sprake van een hoog risico voor betrokkenen.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nog niet bekend

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

AUTORITEIT PERSOONSGEGEVENS

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namellijk: Indien wij in staat zijn om een melding te doen aan de betrokkenen, dan zullen wij dat doen. Op dit moment is de USB verloren en kunnen wij niet vaststellen of de USB wel persoonsgegevens bevat, en zo ja, van wie. Bij terugvinden zullen wij beoordelen of wij betrokkenen moeten informeren.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken? Ja, namelijk:

Toelichting:

- Toepassing digitale uitwisseling van beeldmateriaal onderzoeken (eventueel in samenwerking met Politie)
- Beveiliging USB (indien men niet over kan gaan op digitale uitwisseling van beelden)
- Verzenden per post niet toestaan, enkel persoonlijk afgifte (indien men niet over kan gaan op digitale uitwisseling van beelden)
- Melding maken van vermissing bij PostNL

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen? Ja, namelijk:

Toelichting:

- Toepassing digitale uitwisseling van beeldmateriaal onderzoeken (eventueel in samenwerking met Politie)
- Beveiliging USB (indien men niet over kan gaan op digitale uitwisseling van beelden)
- Verzenden per post niet toestaan, enkel persoonlijk afgifte (indien men niet over kan gaan op digitale uitwisseling van beelden)
- Melding maken van vermissing bij PostNL

AUTORITEIT
PERSOONSGEGEVENS

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Privacyverklaring

AUTORITEIT
PERSOONSGEGEVENS

Meldloket

Ontvangstbevestiging

- Uw verzoek tot het indienen van een melding wordt in behandeling genomen.

  U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

  Tijdstip ontvangst
  29-05-2020 13:06:26
  Uniek nummer
  art 5 1-2e

---

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?
Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?
Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Naam van het bedrijf of de organisatie
Provincie Zuid-Holland
Adres
Zuid-Hollandplein 1
Postcode
2596AW
Plaats
Den Haag
In welke sector is de organisatie of het bedrijf actief?
Openbaar bestuur - Provincie

Wie meldt het datalek?

Naam
art 5 1-2e
Functie
Adviseur informatieveiligheid
E-mailadres
art 5 1-2e pzh.nl
Telefoonnummer
art 5 1-2e
Tweede telefoonnummer
art 5 1-2e

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon
Ja

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?
Nee

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend
13-05-2020
Startdatum van de periode waarbinnen de inbreuk was
13-05-2020
Einddatum van de periode waarbinnen de inbreuk was
28-05-2020
Duurt de inbreuk op dit moment nog voort?
Nee
Wanneer werd de inbreuk ontdekt?
28-05-2020

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens
Ja
Inbreuk op de integriteit van de gegevens
Nee
Inbreuk op de beschikbaarheid van de gegevens
Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?
Persoonsgegevens per ongeluk gepubliceerd
Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest
Publicatie op de website van de provincie Zuid-Holland van een (geheim) GS besluit met persoonsgegevens van de burger aan wie het geadresseerd is.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam
Ja
Geslacht, geboortedatum en/of leeftijd
Nee
Burgerservicenummer (BSN)
Nee
Contactgegevens
Ja
Toegangs- of identificatiegegevens
Nee
Financiële gegevens
Ja
(Kopieën van) paspoorten of andere legitimatiebewijzen
Nee
Locatiegegevens
Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

Nee
Onbekend / anders, namelijk:
Naam, adres, schadebedrag

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt
Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken
Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken
Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt
Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
Nee
Gegevens over iemands gezondheid
Nee
Genetische gegevens
Nee
Biometrische gegevens
Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk
1

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers
Nee
Klanten (huidig en potentieel)
Nee
Leerlingen of studenten
Nee
Patiënten
Nee
Minderjarigen

Nee
Personen uit kwetsbare groepen
Nee
Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
Burger
Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
1
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
1

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?
Nee

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens
Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt
Nee
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt
Nee
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties
Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen
Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen
Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie
Nee
Identiteitsdiefstal of -fraude
Nee
Financiële verliezen
Nee
Reputatieschade
Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens
Nee
Ongeoorloofde ongedaanmaking van pseudonimisering
Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen
Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen
Nee
Andere gevolgen, namelijk:
Het besluit bevat een aan betrokkene uit te keren schadebedrag. Het openbaar worden van deze informatie in combinatie met de genoemde persoonsgegevens kan een nadelig effect hebben op de persoonlijke levenssfeer van betrokkene.
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen
2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?
Nee
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?
0
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?
-

Waarom ziet u af van het melden van het datalek aan de betrokkenen?
Anders, namelijk:
Als het informeren van alle betrokkenen een onevenredige inspanning zou vergen, licht dan toe hoe u door een openbare mededeling of een soortgelijke maatregel de betrokkenen gaat informeren.
Betrokkene heeft het datalek zelf (via een tussenpersoon) gemeld bij de provincie.

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
Het betreft een menselijke fout. Het besluit is van de provinciale website verwijderd en ook uit het webarchief (https://zuidholland.archiefweb.eu) van de provincie. Enkele regels zijn nog zichtbaar in de zoekresultaten van Google. Er is bij Google een verwijderingsverzoek ingediend.

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?
Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?
Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?
Nee

9. Overig

Is naar uw mening deze melding compleet?
Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig

---

"Van: art 5 1-2e
Verzonden: 2020-01-24 16:52:14+00:00
"Aan: art 5 1-2e art 5 1-2e
"CC: Zoete - van der Hout, WH, de; art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: Aankondiging: adviesrapporten 2 datalekken komen er aan
"
Hallo art 5 1-2e

Vandaag 2 gemelde datalekken.

In beide gevallen adviseert het Privacy team dat het datalekken zijn met laag risico, die om die reden niet gemeld hoeven te worden aan de Autoriteit Persoonsgegevens.

We zullen ze wel in onze interne registratie opnemen.

Ik ben nog bezig met de adviesrapporten; die volgen later op de avond.

Vast een korte beschrijving:

1. Vandaag:
   De secretaresses van Water en Groen hebben een gezamenlijk e-mail account.
   Zij hebben in Outlook een lijst met contactpersonen aangelegd, waar zij allen toegang toe hebben.
   Bij een aantal contactpersonen zijn in het notitieveld persoonsgegevens ingevuld. Waarschijnlijk door een van de secretaresses die nu niet aanwezig was.
   Dit was bijvoorbeeld het geval bij art 5 1-2e ie als afdelingshoofd ook als contactpersoon was opgevoerd.

In zijn geval: inloggegevens voor het netwerk en voor bepaalde websites en zijn e-sign code.
Bij enkele andere contactpersonen: zagen we ook inloggegevens en hier en daar een geboortedatum.
Is besproken met de aanwezige secretaresses en met art 5 1-2e
Is niet de bedoeling dat dat zo gebeurt. Aangezien alleen de secretaresses inzage hadden achten we het risico laag.
Moet wel worden hersteld.

2. Gisteren:
   Melding van een (mogelijk) datalek in een database van en bij Microsoft.

Dit betreft een interne database van Microsoft die ze gebruiken voor analyse over support calls die klanten over het Azure platform hebben ingediend.

Die informatie wordt normaal gesproken geanonimiseerd opgenomen in de database, maar daar zijn uitzonderingen op.

De database stond een kleine maand (december) open. Microsoft heeft onderzoek gedaan en geen misbruik kunnen constateren.

Staat inmiddels weer dicht.

We hebben bij Microsoft opgevraagd welke informatie het van PZH betreft, maar hebben nog geen antwoord.
Slechts enkele I&A medewerkers (<10) plaatsen wel eens support vragen bij Microsoft.
Geregistreerd wordt naam, locatie, ip-adres en dergelijke. In de zakelijke context is dit ongevaarlijk en voor de betrokken persoon een zeer laag risico.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>
"


provincie
ZUID HOLLAND

Aanpak berichtgeving datalek

Vertrouwelijk

art 5 1-2e 9-09-2019

Situatie

Er is een proces ingericht voor de aanmelding van statenleden en fractiemedewerkers tussen Statengriffie en P&O. Het gaat om tussentijdse wisselingen bij vertrek en vervanging.
Eigenaar van dit proces is de afdeling P&O. Er zijn twee procesbeschrijvingen: Indiensttreding PS-lid en Indiensttreding Fractiemedewerkers
De aanmeldingen worden geïnitieerd door de Statengriffie.
De aanmelding bevat veel persoonsgegevens; naast contactgegevens ook gevoelige informatie zoals kopie ID, financiële gegevens en BSN. Deze informatie gebruikt P&O voor de salarisadministratie en afhandeling van personeelszaken.

Het proces wordt ondersteund door een ICT-systeem (Topdesk). De Statengriffie vult in dit systeem de aanmelding met de bovenstaande persoonsgegevens in. P&O ontvangt en verwerkt deze informatie.
Via het systeem worden ook deeltaken uitgezet bij medewerkers van I&A en FZ. Dit is voor het aanmaken van werkplek gerelateerde zaken (account, tablet, telefoon) en het verzorgen van toegangspassen, OV-abonnement en dergelijke. Voor de uitvoering van deze deeltaken is personeel uit de genoemde afdelingen geautoriseerd. Dit noemen we behandelaren. De deeltaak bevat een deel van de persoonsgegevens die in de aanvraag zijn ingetypt (contactgegevens, geboortedatum, BSN, IBAN), exclusief de bij de aanvraag gevoegde bijlagen (zoals kopie ID, kopie loonverklaring).

Datalek:

1. De behandelaren krijgen in de deeltaak te veel gevoelige persoonsgegevens (geboortedatum, BSN, IBAN) te zien, die ze niet nodig hebben voor de uitvoering van die taak.
2. Ook andere behandelaren (406 personen) die in Topdesk andere taken uitvoeren kunnen de deeltaken met daarin deze persoonsgegevens zien.
3. Voor alle behandelaren geldt bovendien dat ze vanuit de deeltaak met een enkele muisklik ook de volledige aanvraag kunnen zien, inclusief de daaraan gekoppelde bijlagen (kopie ID, etc.). Door een tekortkoming in de Topdesk software is het niet mogelijk om dit te voorkomen.

Stand van zaken

Het Privacyteam heeft de art 5 1-2e geadviseerd om dit datalek te melden bij de Autoriteit Persoonsgegevens én bij de betrokken statenleden en fractiemedewerkers. art 5 1-2e heeft conform besloten. De melding bij de Autoriteit Persoonsgegevens is inmiddels gedaan. Willy de Zoete heeft woensdag in de rondvraag in de GS-vergadering gemeld dat er een datalek is.

Vervolg

Voor het vervolg is het nodig een team te formeren om de boodschap te formuleren en ook mogelijke gevolgen te doordenken en waar mogelijk te bedenken welke vragen er kunnen komen en hoe (en door wie) beantwoord worden.

Door de omvang, type functionarissen en korte termijn waarop boodschap moet worden geformuleerd zal het lastig zijn om iedereen bij elkaar te krijgen. Lijkt mij wel goed om samen met deze samenstelling te starten, maar om het werkbaar te maken dan afspraken te maken om met een delegatie te werken aan de boodschap / deze zo snel mogelijk op te leveren.

Ik stel voor dat de coördinatie bij de P&O als proceseigenaar ligt en daarbij de volgende stakeholders te betrekken:

- Coördinatie: ….
- Bestuursadviseur van Willy de Zoete: art 5 1-2e
- Communicatie: art 5 1-2e
- Persvoorlichter art 5 1-2e
- De FG: art 5 1-2e
- Privacyjurist FJZ: art 5 1-2e
- Inhoudelijk: art 5 1-2e art 5 1-2e

- FZ? (is nog niet geïnformeerd)

Wat rest is:

- Het informeren van betrokkenen (vrijdag 20-9, uiterlijk maandag 23/9)
  - De afdeling Communicatie is bezig met het opstellen van een concept brief
  - Toon van de brief: PZH heeft veel aandacht voor veilige omgang met persoonsgegevens, medewerkers zijn in toenemende mate alert hierop, hierdoor is opgemerkt dat medewerkers van interne ondersteunende afdelingen meer persoonsgegevens konden zien dan nodig, hier is werk van gemaakt, situatie is opgelost, geen aanwijzing dat de gegevens op straat liggen
- De bestuurlijk-politieke communicatie,
  - Willy de Zoete heeft woensdag in de rondvraag in de GS-vergadering gemeld dat er een datalek is. Waarschijnlijk is het ook nodig dat GS PS hierover informeren.
  - Opstellen tekst voor GS-brief
  - Communicatie, inhoudelijk betrokkenen, Bestuursadviseur
- Zorgen dat vragen van de betrokkenen beantwoord worden (inclusief de afweging welke vragen op de casus betrekking hebben en welke vragen politiek van aard zijn)
  - P&O, Communicatie, inhoudelijk betrokkenen, Bestuursadviseur
    - art 5 1-2evordt bij ons (P&O) de contac tpersoon die betrokkenen kunnen bellen (ze bellen normaal gesproken ook met hem als ze vragen hebben rondom personeelssalarisadministratie).
- Anticiperen op externe vragen van journalisten en maatschappelijke organisaties.
  - Deze kunnen via verschillende kanalen binnenkomen (via de FG, via de website, journalist aan de balie, tv-ploeg)
  - Persvoorlichter, FG, jurist, inhoudelijk betrokkenen
- Anticiperen op statenvragen
  - Bestuursadviseur, FG, jurist, inhoudelijk betrokkenen
- Anticiperen op verscherpte aandacht van de AP: hoe kan dit en hoe zit dat bij jullie andere systemen?
  - FG, jurist, inhoudelijk betrokkenen

Aanpak berichtgeving datalek

Vertrouwelijk

art 5 1-2e 9-09-2019

Situatie

Er is een proces ingericht voor de aanmelding van statenleden en fractiemedewerkers tussen Statengriffie en P&O. Het gaat om tussentijdse wisselingen bij vertrek en vervanging.
Eigenaar van dit proces is de afdeling P&O. Er zijn twee procesbeschrijvingen: Indiensttreding PS-lid en Indiensttreding Fractiemedewerkers
De aanmeldingen worden geïnitieerd door de Statengriffie.
De aanmelding bevat veel persoonsgegevens; naast contactgegevens ook gevoelige informatie zoals kopie ID, financiële gegevens en BSN. Deze informatie gebruikt P&O voor de salarisadministratie en afhandeling van personeelszaken.

Het proces wordt ondersteund door een ICT-systeem (Topdesk). De Statengriffie vult in dit systeem de aanmelding met de bovenstaande persoonsgegevens in. P&O ontvangt en verwerkt deze informatie.
Via het systeem worden ook deeltaken uitgezet bij medewerkers van I&A en FZ. Dit is voor het aanmaken van werkplek gerelateerde zaken (account, tablet, telefoon) en het verzorgen van toegangspassen, OV-abonnement en dergelijke. Voor de uitvoering van deze deeltaken is personeel uit de genoemde afdelingen geautoriseerd. Dit noemen we behandelaren. De deeltaak bevat een deel van de persoonsgegevens die in de aanvraag zijn ingetypt (contactgegevens, geboortedatum, BSN, IBAN), exclusief de bij de aanvraag gevoegde bijlagen (zoals kopie ID, kopie loonverklaring).

Datalek:

1. De behandelaren krijgen in de deeltaak te veel gevoelige persoonsgegevens (geboortedatum, BSN, IBAN) te zien, die ze niet nodig hebben voor de uitvoering van die taak.
2. Ook andere behandelaren (406 personen) die in Topdesk andere taken uitvoeren kunnen de deeltaken met daarin deze persoonsgegevens zien.
3. Voor alle behandelaren geldt bovendien dat ze vanuit de deeltaak met een enkele muisklik ook de volledige aanvraag kunnen zien, inclusief de daaraan gekoppelde bijlagen (kopie ID, etc.). Door een tekortkoming in de Topdesk software is het niet mogelijk om dit te voorkomen.

Stand van zaken

Het Privacyteam heeft de art 5 1-2e geadviseerd om dit datalek te melden bij de Autoriteit Persoonsgegevens én bij de betrokken statenleden en fractiemedewerkers. art 5 1-2e heeft conform besloten. De melding bij de Autoriteit Persoonsgegevens is inmiddels gedaan. Willy de Zoete heeft woensdag in de rondvraag in de GS-vergadering gemeld dat er een datalek is.

Vervolg

Voor het vervolg is het nodig een team te formeren om de boodschap te formuleren en ook mogelijke gevolgen te doordenken en waar mogelijk te bedenken welke vragen er kunnen komen en hoe (en door wie) beantwoord worden.

Door de omvang, type functionarissen en korte termijn waarop boodschap moet worden geformuleerd zal het lastig zijn om iedereen bij elkaar te krijgen. Lijkt mij wel goed om samen met deze samenstelling te starten, maar om het werkbaar te maken dan afspraken te maken om met een delegatie te werken aan de boodschap / deze zo snel mogelijk op te leveren.

Ik stel voor dat de coördinatie bij de P&O als proceseigenaar ligt en daarbij de volgende stakeholders te betrekken:

- Coördinatie: ….
- Bestuursadviseur van Willy de Zoete: art 5 1-2e
- Communicatie: art 5 1-2e
- Persvoorlichter art 5 1-2e
- De FG: art 5 1-2e
- Privacyjurist FJZ: art 5 1-2e
- Inhoudelijk: art 5 1-2e art 5 1-2e

- FZ? (is nog niet geïnformeerd)

Wat rest is:

- Het informeren van betrokkenen (vrijdag 20-9, uiterlijk maandag 23/9)
  - De afdeling Communicatie is bezig met het opstellen van een concept brief
  - Toon van de brief: PZH heeft veel aandacht voor veilige omgang met persoonsgegevens, medewerkers zijn in toenemende mate alert hierop, hierdoor is opgemerkt dat medewerkers van interne ondersteunende afdelingen meer persoonsgegevens konden zien dan nodig, hier is werk van gemaakt, situatie is opgelost, geen aanwijzing dat de gegevens op straat liggen
- De bestuurlijk-politieke communicatie,
  - Willy de Zoete heeft woensdag in de rondvraag in de GS-vergadering gemeld dat er een datalek is. Waarschijnlijk is het ook nodig dat GS PS hierover informeren.
  - Opstellen tekst voor GS-brief
  - Communicatie, inhoudelijk betrokkenen, Bestuursadviseur
- Zorgen dat vragen van de betrokkenen beantwoord worden (inclusief de afweging welke vragen op de casus betrekking hebben en welke vragen politiek van aard zijn)
  - P&O, Communicatie, inhoudelijk betrokkenen, Bestuursadviseur
    - art 5 1-2e vordt bij ons (P&O) de contactpersoon die betrokkenen kunnen bellen (ze bellen normaal gesproken ook met hem als ze vragen hebben rondom personeelssalarisadministratie).
- Anticiperen op externe vragen van journalisten en maatschappelijke organisaties.
  - Deze kunnen via verschillende kanalen binnenkomen (via de FG, via de website, journalist aan de balie, tv-ploeg)
  - Persvoorlichter, FG, jurist, inhoudelijk betrokkenen
- Anticiperen op statenvragen
  - Bestuursadviseur, FG, jurist, inhoudelijk betrokkenen
- Anticiperen op verscherpte aandacht van de AP: hoe kan dit en hoe zit dat bij jullie andere systemen?
  - FG, jurist, inhoudelijk betrokkenen

De Autoriteit Persoonsgegevens (AP) veroorzaakte vrijdag 24 mei zelf een datalek. Een woordvoerder zette in een email naar journalisten, redacties en relaties 38 geadresseerden in het cc-veld. Daardoor kon iedere ontvanger zien wie het mailtje nog meer had gekregen (zie kader). Hoe gaat de privacytoezichthouder zelf om met zo'n incident?

Volgens AP is er in het eigen geval met de cc-knop sprake van een datalek. De interne procedures zijn gevolgd, maar of het incident officieel gemeld moet worden bij de AP is nog in overweging. De woordvoerder licht toe: 'We hebben uiteraard een procedure voor beveiligingsincidenten. Het incident moet eerst zo spoedig mogelijk intern gemeld worden - afdelingshoofd, directeur, beveiligingsambtenaar, functionaris gegevensbescherming - zodat is te beoordelen of er sprake is van een datalek dat ook gemeld moet worden bij de AP.'

Bij het publiceren van dit artikel is daar nog geen besluit over genomen, legt de woordvoerder uit. In die motivatie speelt bijvoorbeeld de omvang van het aantal gelekte mailadressen mee en is ook de inhoud van de gegevens van belang, licht ze toe, verwijzend naar de richtlijnen van de meldplicht datalekken waarin het onbedoeld of ongegrond delen van namen van geadresseerden in cc wordt beoordeeld als een datalek.

De woordvoerder: 'De volgende vraag is of een datalek ook bij de AP gemeld moet worden. Dat is afhankelijk van de (potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van betrokkenen. Het datalek moet worden gemeld als het leidt tot een risico voor de rechten en vrijheden van betrokkenen. Als er geen gevoelige gegevens zijn onthuld en als er slechts een klein aantal e-mailadressen is onthuld, hoeft een datalek niet altijd gemeld te worden.'

Cc-knop

Vrijdagochtend 24 mei jl verstuurt AP om 7.25 uur een mail naar 38 journalisten, redacties en relaties om hen te wijzen op een persbericht met de titel: 'Wat betekent de privacywet voor jou(w bedrijf)'. In het cc-veld staan 38 e-mailadressen.

De woordvoerder merkt kennelijk vrij snel dat er iets is misgegaan of wordt daarop gewezen. Om 7.46 volgt een nieuwe mail met een verzoek: 'Zojuist gepubliceerd: Start campagne 'Wat betekent de privacywet voor jou(w bedrijf)?' intrekken.'

Om 10.22 uur volgt nog een email: 'Ik heb vanochtend in een onoplettend moment per abuis een persbericht verstuurd naar een aantal e-mailadressen in de cc ipv de

bcc. Ik heb daarna de e-mail ingetrokken, maar mogelijkerwijs zijn alle e-mailadressen toch zichtbaar geweest voor alle of een deel van de adressanten. De fout is uiteraard gelijk intern gemeld en zal volgens de geldende procedures worden opgepakt. Mijn welgemeende excuses.'

'Datelek hoeft niet altijd extern gemeld te worden'

Het is dus afhankelijk van de omvang van het gelekte aantal mailadressen en de inhoud van het bericht of het incident ook bij de autoriteit gemeld moet worden. Incidenten met de cc-knop worden vaker gemeld bij de dienst. De woordvoerder: 'In de meeste gevallen betreft het datalek het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger. Hierbij gaat het met name om poststukken met gevoelige gegevens die bij de verkeerde persoon terechtkomen en geopend retour worden gestuurd (de onjuiste ontvanger heeft kennis genomen van de inhoud van de brief). Ook kan het gaan om een mail met daarin gevoelige persoonsgegevens die wordt verzonden naar de verkeerde ontvanger. Bijvoorbeeld door een typefout of omdat er in het mailprogramma een verkeerde geadresseerde wordt geselecteerd.'

Ze vervolgt: 'In het algemeen geldt: als iedereen toestemming heeft gegeven of als alle adressanten elkaar kennen en elkaars e-mailadressen kennen. De inbreuk op privacy is dan minimaal. Gebruik van cc moet wel een doel dienen. In een werkomgeving kan het functioneel zijn bijvoorbeeld omdat je elkaars reactie ziet.'

Risico

Organisaties bepalen dus grotendeels zelf op basis van welke motivatie ze besluiten om een datalek via de cc-knop wel of niet te melden bij de AP. Volgens de woordvoerder loopt een organisatie die niets meldt altijd het risico dat één van de ontvangers zich meldt bij de autoriteit. Ze verwacht dat het onder de pet houden van incidenten zich uiteindelijk tegen organisaties zal keren en boetes zullen volgens als achteraf blijkt dat ze op onrechtmatige gronden een incident hebben verzwegen.

Het blijft voor de dienst lastig om in algemene zin aan te geven wanneer een dergelijk incident moet worden gemeld. Het hangt van specifieke details af, meldt de woordvoerder. Zo wordt bij incidenten met persoonlijke mailadressen de gevolgen voor de privacy van de persoon vaak zwaarder gewogen dan bij zakelijke mailadressen.

De woordvoerder over het eigen datalek met de cc-knop: 'In dit specifieke geval gaat het om een verwijzing naar een algemeen persbericht op onze openbare website. Het gaat dus niet om bijvoorbeeld de salarisgegevens van onze medewerkers. Dat

zou het ook weer anders maken. Maar ik kan mezelf natuurlijk wel voor mijn kop slaan voor het aanvinken van die cc-knop.'

@
Op Privacy-web.nl las ik dat de Autoriteit Persoonsgegevens afgelopen vrijdag te maken had met een datalek: ze had per ongeluk e-mailadressen van relaties openbaar gemaakt. De privacywaakhond had in een e-mail naar de pers 38 e-mailadressen in de cc gezet. Daardoor konden alle ontvangers elkaars e-mailadressen inzien. Dit is een datalek. Voor de goede orde: De AP had deze adressen in de bcc moeten zetten, zodat de ontvangers niet elkaars e-mailadressen kunnen zien.

Moet de Autoriteit Persoonsgegevens dit datalek melden, en zo ja, bij wie dan? Immers, als er een datalek is kan het zo zijn dat deze gemeld moet worden… bij de Autoriteit Persoonsgegevens en in sommige gevallen bij de betrokkenen. Of dit incident gemeld moet worden hangt met name af van het aantal gelekte e-mailadressen en de inhoud van de betreffende e-mail.

meldplicht datalekken

Immers, de Autoriteit Persoonsgegevens moet als "verwerkingsverantwoordelijke" maatregelen nemen om de persoonsgegevens te beschermen tegen verlies en onrechtmatige verwerking. Een datalek moet dus voorkomen worden door daartegen maatregelen te nemen. De e-mailadressen moesten daarom op de bcc in plaats van op de cc. Nu persoonsgegevens toch onrechtmatig verwerkt worden is er sprake van een datalek.

Dit moet in principe gemeld worden, maar dat hoeft niet in alle gevallen: er moet sprake zijn van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Heeft het datalek ook waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene, dan moet ook deze persoon geïnformeerd worden over het datalek.

In dit geval zal het niet zoveel voeten in de aarde hebben. De betreffende e-mail bevatte een verwijzing naar een persbericht dat op de website van de toezichthouder was verschenen. Toch toont het maar aan hoe snel er al sprake kan zijn van een datalek. Ze zijn niet de eerste, en zullen ook zeker niet de laatste zijn.

"Van: art 5 1-2e
Verzonden: 2020-11-02 17:40:09+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e
"CC: art 5 1-2e voormedia.com'; art 5 1-2e art 5 1-2e
art 5 1-2e
Onderwerp: FW: Acties n.a.v. datalek Relevant
"
Beste art 5 1-2e art 5 1-2een art 5 1-2e

Sinds ons laatste gesprek zijn er verschillende overleggen geweest en acties uitgevoerd.

1. De acties door Voormedia om het potentiële datalek te dichten en verdere incidenten te voorkomen

www.relevant.nl <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.relevant.nl%2F&data=04%7C01% art 5 1-2e 40pzh.nl%7C6f4d540362bf4856835c08d87f4df6b7%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C637399320106612575%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=4AOTfRrXXwEDylKYbus%2BE%2BmmCN6QcI%2B1URqN8PisemA%3D&reserved=0> bestaat uit verschillende componenten.

* Voormedia heeft de onderliggende structuren van de relevant website geüpgraded naar de nieuwste versie. Hierbij zijn de scores van B naar A+ gegaan: https://www.ssllabs.com/ssltest/analyze.html?d=relevant.nl&hideResults=on <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ssllabs.com%2Fssltest%2Fanalyze.html%3Fd%3Drelevant.nl%26hideResults%3Don&data=04%7C01% art 5 1-2e 40pzh.nl%7C6f4d540362bf4856835c08d87f4df6b7%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C637399320106612575%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=2dwm94MXC9%2Btp3ktICL5etQ%2BVUezV79J0wo2hZ9k09M%3D&reserved=0> . Dit is conform de huidige stand van zaken.
* Bovenop de onderliggende structuren maakt Relevant voornamelijk gebruik van een applicatie (Confluence) deze versie is de laatst mogelijke versie die we hebben kunnen implementeren 5.1.5. Deze software dateert uit 2013. Nieuwe software is wel aangeraden door Voormedia maar de licentie is erg duur en er is nieuwbouw nodig (zie ook verderop), plus dat de hele website overgezet moet worden naar een nieuwe eigenaar. Dat is de reden geweest om hier eerder niet voor te beslissen. Ondertussen zijn we wel 2 jaar verder, wat veel langer is dan toentertijd vermoed werd. Achteraf had toch een nieuwe upgrade ons waarschijnlijk deze situatie bespaard.
* De wie-is-wie is offline
* De projectruimten zijn offline
* Er kunnen geen nieuwe accounts meer aangevraagd worden: enkel het openbare deel van de website draait nog. Dus ook bot software is verwijderd (e capcha, of hoe schrijf je dat?)

2. Bespreking van de routes mogelijke routes.

Er zijn 5 mogelijke routes, die hieronder staan vermeld en waar de reacties ook achter staan. Bij punt 3 staat de route die we volgen.

a. Relevant uitzetten. Deze situatie is a. ongewenst en b. onnodig. Ad a Die projectruimten worden erg gemist maar het openbare deel wordt dagelijks gebruikt door het netwerk. Met minder komt de informatievoorziening over EV in de knel. Ad b Er draait nu enkel nog een light versie van de website zonder persoonsgegevens, met enkel openbare informatie, dus zonder de projectruimten.

b. Het uitvoeren van minimale wijzigingen, zoals het verwijderen van de wie-is-wie en de inlog verbeteren, maar de projectruimten wel weer online zetten, met aanpassing van de procedure om een account aan te maken. De onderliggende structuur is dan up to date, maar Relevant blijft draaien op de verouderde versie van Confluence. De applicatie zal naar verwachting mankementen vertonen als er een P-test wordt uitgevoerd. Deze situatie is voor Relevant zelf wenselijk, want de projectruimten worden gemist. Echter, deze situatie is waarschijnlijk NIET acceptabel voor PZH. Als er een penetratietest wordt uitgevoerd, valt de oudere versie van confluence door de mand: die geeft resultaten die qua oplossing veel tijd en geld zal kosten én misschien lukt het niet eens. Beter dus optie c.
c. De content migreren naar een nieuwe omgeving, zonder gebruik te maken van confluence. Dit is wat Voormedia eerdere heeft voorgesteld (Relevant light) maar wat niet wenselijk werd geacht omdat het ten koste van de projectruimten gaat. Echter, dit is een stap die als je de content later wilt hergebruiken bij een nieuwe eigenaar altijd zou moeten uitvoeren. Het is kostenefficient om het nu te doen. De data zit nu in een confluence structuur, maar die is niet erg logisch, dus die wil je sowieso kwijt als je gaat migriteren naar een nieuwe eigenaar/structuur. Relevant light kan je vervolgens transformeren naar een tussenliggende structuur die bedacht moet worden. De database van Voormedia is platter is dan confluence nodig heeft. Vraag is of we de projectruimten op een andere manier kunnen faciliteren?
d. Upgraden van Relevant naar de laatste versie van Confluence (met incompatible plugins als gevolg). Achtergrond: er zijn 2 scaffolding plugins gebouwd omdat dit de enige manier was om met plugins van confluence te werken met behoud van de gewenste functionaliteiten. Dat geeft een afhankelijkheid aan de oude versie aan, want de nieuwe versie werkten niet meer met die plugins. Dus als je nu gaat upgraden is dat extra duur, omdat je én de duren licentie en die nieuwbouw. Voor de tijdelijkheid van onze situatie is deze optie niet aangeraden.
e. Nieuw bouwen van Relevant met de daarbij behorende gewenste functionaliteiten. Die is gewenst maar kan pas na bestuurlijke besluitvorming.

3. Besluitvorming over de te volgen route en acties

Zojuist heb ik gesproken met art 5 1-2e We zijn er allebei van overtuigd dat we het beste zonder Confluence verder kunnen en dus gaan voor de light versie van Relevant.

art 5 1-2e en ik hebben dus geopteerd voor keuze 2c

* We gaan verder zonder Confluence, de licentie wordt opgezegd door Voormedia.
* Zonder wie-is-wie (structureel)
* Helaas ook zonder de projectruimten. We onderzoeken op welke manier deze op een andere manier gefaciliteerd kunnen worden
* Enkel het openbare deel van de website draait nog.
* De omzetting van PZH naar een nieuwe eigenaar wordt voor 1-7-2021 verwacht.

Qua uit te voeren acties

* Voormedia voert de migratie uit.
* Voormedia of een andere partij voert hierna de p-test uit op de light versie. Kan PZH aangeven wat de voorkeur heeft? Het moet allemaal wel voor 31 december 2020 zijn afgerond, ivm de afronding van het programma IOV per die datum en dat kunnen de kosten niet meer geboekt worden op de IOV.
* We streven ernaar om Relevant op 1 juli 2021 over te hebben gezet naar een nieuwe eigenaar, maar dat dit kunnen we niet garanderen. Actie art 5 1-2e
* We gaan op zoek naar een mogelijkheid om projectruimten op een andere manier aan te bieden. Blijkbaar is Teams daar ook toe in staat, dat zou wel makkelijk zijn want iedereen gebruikt dat. Actie: via art 5 1-2e

* We gaan het communiceren naar de gebruikers. Actie via art 5 1-2e

Wordt vervolgd. Bedankt allemaal!

Vriendelijke groet,

art 5 1-2e
Landelijk coördinator Impuls Omgevingsveiligheid
Provincie Zuid-Holland
art 5 1-2e

"

Van: art 5 1-2e
Verzonden: 2023-09-27 14:51:18+00:00
Aan: art 5 1-2e
CC: art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: Acties TAB ivm dataonderzoek
"
Hoi art 5 1-2e

Ik heb twee meldingen in Topdesk gezet, enerzijds voor het aanleveren van logs, anderzijds voor het isoleren van stukken ivm privacy.

M23 09 03055 isoleren stukken (kopie paspoort + naam en curriculum vitae + naam)

M23 09 03059 auditlog 4 dossiers

Verzoek om auditlog van de te isoleren stukken volgt nog.

Dank je wel alvast Mark!

Met vriendelijke groet,

art 5 1-2e

Functioneel Beheer

art 5 1-2e

"

"Van: art 5 1-2e
Verzonden: 2020-05-08 18:16:28+00:00
"Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: Advies
"
Hi,

Graag jullie op- en aanmerkingen.

Ik heb dit ook naar art 5 1-2e gestuurd.

Helaas krijg ik foutmeldingen op Onedrive.

Ik wil het document ook niet via iDMS delen ,omdat de directe collega's van art 5 1-2e beheerrechten in iDMS hebben en onze privacyteam omgeving kunnen inkijken.

Daarom toch maar per e-mail.

Graag jullie reactie.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>
"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Concept

Melding gegevens

Naam melder	:	art 5 1-2e betrokkene)
Registratienummer van het incident	:	Volgt
Datum en tijdstip van de melding	:	Vrijdag 8 mei 2020 14:39
Route van de melding	:	E-mail

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 8 mei 2020 17:45
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e privacy jurist)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerker

Situatie

(*Korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*
Betrokkene voerde per telefoon een gesprek met haar teamleider.
Tegelijkertijd probeerde ze met deze leidinggevende een Teams chat te starten, zodat ze elkaar ook konden zien. Daar ging iets mis, want ze startte per ongeluk een vergadering met een Team waar ze deel van uit maakt. De microfoon van de laptop stond daarbij open.
Omdat ze elkaar niet te zien kregen hebben ze het gesprek verder telefonisch gedaan.

Een ander lid van dat Team zag dat er een vergadering werd geopend en kwam (op de laptop) in die chat en kon doordat de microfoon van de laptop open stond meeluisteren met het telefoongesprek. Betrokkene had dit niet in de gaten.
Een deel van het gesprek ging over persoonlijke aangelegenheden. Het meeluisterende teamlid heeft daar niet alleen in meegeluisterd maar daar ook in Teams een opname van gemaakt.
Hij heeft dat wel later per e-mail bij betrokkene gemeld.

Het opgenomen audio gesprek staat in de chat waar de andere teamleden ook bij kunnen.
Dit audio gesprek kan daar niet uit worden verwijderd. Automatisch gebeurt dit wel maar pas na 20 dagen.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Betreft een gesprek.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	1 persoon heeft meegeluisterd en een opname gemaakt. 8 collega's hebben potentieel toegang tot de opname.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen,	Luisteren

Vraag	Antwoord
veranderen, verwijderen)	
Welke persoonsgegevens betreft het?	Persoonlijk gesprek tussen betrokkene en teamleider, onder meer over de samenwerking met een collega.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja. Directe collega's.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Ja. Betreft het uitlekken van een persoonlijk gesprek. De samenwerking tussen collega's kan onder druk komen te staan. Betrokkene voelt zich aangetast in haar persoonlijke levenssfeer. Haar vertrouwen is geschaad.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja, in relatie tot de vertrouwelijkheid van de informatie.
Betreft het een datalek?	Ja. Deze informatie is bij de verkeerde persoon terecht gekomen.
Ondernomen beperkende maatregelen.	Het opgenomen audiogesprek staat in de chat waar de andere teamleden ook bij kunnen. Door de I&A Teams beheerder is gepoogd de opname uit de chat te verwijderen. Dit bleek niet mogelijk. Automatisch gebeurt dit wel maar pas na 20 dagen. De collega die de opname heeft gemaakt is Teamlid is hierop aangesproken door het bureauhoofd. Het bureauhoofd heeft in de chat een bericht geplaatst over het niet afluisteren van de opname.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	De I&A beheerder van Teams is op zoek naar een manier om het audio gesprek weg te halen, misschien door de hele chat te verwijderen als dat kan.

[1] Art.9 AVG: Gegevens over ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
	In de Teams training dient aandacht te worden besteed aan de gevaren van het ongemerkt openzetten van camera en microfoon. In de communicatiecampagne Data Donderdag zal aandacht worden besteed aan zorgvuldig gebruik van Teams en het maken van opnamen.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

Er is sprake van een datalek, omdat er persoonsgegevens in verkeerde handen zijn gekomen.

Gezien de vertrouwelijke aard van de informatie en omdat het de directe werkkring van betrokkene betreft, achten wij het hiermee verbonden risico voor aantasting van de persoonlijke levenssfeer van betrokkene hoog.

Conclusie en advies
Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. Dat is hier naar ons oordeel wel het geval. Het betreft informatie die de positie van betrokkene in de directe werksituatie kan schaden.

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert het Privacy team om:

- De datalek melding en beoordeling zoals gebruikelijk te administreren in het provinciale logboek.
- Het datalek te melden bij de Autoriteit Persoonsgegevens.

Het datalek is besproken met directbetrokkenen, zodat verdere actie hier niet nodig is.


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2020-01-10 10:36:50+00:00
"Aan: art 5 1-2e
"CC: Zoete - van der Hout, WH, de; art 5 1-2e
Onderwerp: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Beste art 5 1-2e

Bijgaand het advies van het privacyteam in het kader van een gemeld datalek.

De beoordeling is dat er sprake is van een datalek.

Er is sprake van een laag risico.

Het advies is niet te melden aan de AP en niet aan de betrokkenen.

De melding en het advies zijn afgestemd met onze FG en zoals gebruikelijk opgenomen in onze administratie.

Ik hoor graag of je akkoord bent met dit advies.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>
"


provincie
ZUID HOLLAND

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Definitief

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	M20 01 00799
Datum en tijdstip van de melding	:	Woensdag 8 januari 2020 12:31
Route van de melding	:	Datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 10 januari 2020
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e (privacy jurist)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerker, privacy officer van de afdeling Communicatie

Situatie

(*Korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*
Op 7 januari 2020 heeft de melder een e-mail gestuurd naar de PZH-collega's die zich hadden aangemeld voor de nieuwjaarsreceptie van de provincie. Met als doel dat de collega's zich op de bijeenkomst konden voorbereiden om er zo een optimaal resultaat uit te kunnen halen. Bij de mail was daarom een Excel-overzicht gevoegd van de externe relaties die zich ook hadden aangemeld (520 personen). Het overzicht bestond uit voornaam, achternaam, organisatie en functie.
Per ongeluk heeft de melder de mail met het overzicht ook gestuurd aan oud-Statenlid art 5 1-2e art 5 1-2e reageerde per e-mail (met smiley) dat het overzicht vast niet voor hem was bedoeld en heeft op verzoek van de melder de e-mail weggegooid.

Melder heeft de situatie besproken met de privacy officer van zijn afdeling en ter beoordeling voorgelegd aan het Privacyteam.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Van 520 provinciale relaties de voornaam, achternaam, organisatie en functie
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	1
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen
Welke persoonsgegevens betreft het?	Voornaam, achternaam, organisatie en functie

Vraag	Antwoord
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Nee. De gegevens zijn gestuurd aan een oud-Statenlid.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	De ontvanger is een oud-Statenlid, de gegevens zijn niet gevoelig, de inhoud van de e-mail is niet gevoelig en geeft geen aanleiding tot misbruik. De betreffende persoonsgegevens hebben geen vertrouwelijk karakter en zijn deels ook via internet op te zoeken. Gezien deze context achten wij het hiermee verbonden risico voor de betrokkenen laag.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja, in relatie tot de vertrouwelijkheid van de persoonsgegevens van de provinciale relaties.
Betreft het een datalek?	Ja. Onrechtmatige verwerking (misbruik van de persoonsgegevens) achten wij onwaarschijnlijk, maar kan niet uitgesloten worden, zodat er strikt genomen sprake is van een inbreuk in verband met persoonsgegevens (datalek) .
Ondernomen beperkende maatregelen.	art 5 1-2e eef t op verzoek van de melder de e-mail weggegooid.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Verdere maatregelen zijn niet nodig.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval
De persoonsgegevens zijn niet gevoelig, de inhoud van de e-mail is niet gevoelig en geeft geen aanleiding tot misbruik en de ontvanger is een oud-Statenlid van de provincie Zuid-Holland.
Gezien deze context achten wij het hiermee verbonden risico voor de betrokkenen laag.
Onrechtmatige verwerking is echter strikt genomen niet uit te sluiten, zodat er volgens de AVG wel sprake is van een inbreuk in verband met persoonsgegevens, beter bekend als: datalek.

Conclusie en advies
Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. Dat is hier naar ons oordeel niet het geval.

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert het Privacyteam om:

- Het datalek niet te melden bij de Autoriteit Persoonsgegevens.
- Het datalek niet te melden bij de betrokkenen.
- De melding en beoordeling zoals gebruikelijk te administreren in het provinciale logboek.

"Van: art 5 1-2e
Verzonden: 2020-05-29 10:28:04+00:00
"Aan: art 5 1-2e
"CC: Zoete - van der Hout, WH, de; art 5 1-2e art 5 1-2e
Onderwerp: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Beste art 5 1-2e

Bijgaand het aangekondigde advies over het datalek dat gisteren is gemeld.

Het advies is afgestemd met onze FG en met art 5 1-2e is bij de afhandeling betrokken als privacy officer van DBI.

Zoals gebruikelijk is het datalek geregistreerd in onze provinciale administratie.

Het advies is om dit datalek te melden aan de Autoriteit Persoonsgegevens.

Ik hoor graag of je hiermee instemt.

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e
Verzonden: donderdag 28 mei 2020 17:15
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
CC: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Datalek in behandeling

Hallo art 5 1-2e

Het Privacyteam heeft een datalek in behandeling.

Het betreft een vaststellingsbesluit met persoonsgegevens dat per ongeluk door GSO op de provinciale website is gepubliceerd.

Het besluit is inmiddels van de provinciale website verwijderd, maar is op dit moment nog zichtbaar in het webarchief van de provincie (https://zuidholland.archiefweb.eu) en enkele regels zijn nog zichtbaar in de zoekresultaten van Google.

Hier wordt actie op ondernomen.

Het adviesrapport volgt morgenochtend.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>
"


provincie
ZUID HOLLAND

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Definitief

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	M20 05 02572
Datum en tijdstip van de melding	:	Donderdag 28 mei 2020 15:32 uur
Route van de melding	:	Datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 29 mei 2020 10:00 uur
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e (privacy jurist)
Strekking advies ter kennisgeving gedeeld met	:	art 5 1-2e

Situatie

Publicatie op de website van de provincie Zuid-Holland van een (geheim) GS besluit met persoonsgegevens van de burger aan wie het geadresseerd is. Het besluit is gepubliceerd op 13 mei 2020 om 12:00 uur.
Het datalek is ontdekt op 27 mei 2020 om ca 23.00 uur. De advocaat van betrokkene heeft bij de provincie een verzoek tot depublicatie gedaan.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Van één persoon: Naam, adres, woonplaats, schadebedrag
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend. Het besluit was op het internet gepubliceerd. - De web statistieken van de provinciale website laten zien dat het document op 24 mei één keer is geopend. En op 28 mei (dag van de melding van het datalek) enkele keren; dat heeft waarschijnlijk mede te maken met het depubliceren van het document van de website. - De statistieken van Archiefweb zijn nog niet binnen. We verwachten daar ook geen grote aantallen bezoekers. - Hoe vaak de informatie is opgedoken in de Google zoekresultaten is niet bekend.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen, kopiëren, afdrukken, e-mailen
Welke persoonsgegevens betreft het?	Naam, adres, woonplaats, schadebedrag.
Betreft het bijzondere	Nee.

Vraag	Antwoord
persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Nee. De gegevens zijn gepubliceerd op het internet.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Het is niet uit te sluiten dat de publicatie een risico oplevert voor betrokkene. De advocaat van de betrokkene heeft de provincie op de publicatie van de persoonsgegevens gewezen en een verzoek tot verwijdering gedaan.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja, in relatie tot de vertrouwelijkheid van de betreffende persoonsgegevens.
Betreft het een datalek?	Ja. Persoonsgegevens zijn ten onrechte openbaar gemaakt.
Ondernomen beperkende maatregelen.	Het besluit is van de provinciale website verwijderd en ook uit het webarchief (https://zuidholland.archiefweb.eu) van de provincie.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Enkele regels zijn nog zichtbaar in de zoekresultaten van Google. Er wordt gewerkt aan een verwijderingsverzoek..

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

Het besluit bevat een aan betrokkene uit te keren schadebedrag. Het openbaar worden van deze informatie in combinatie met de genoemde persoonsgegevens kan een nadelig effect hebben op de persoonlijke levenssfeer van betrokkene. Het is daardoor te kenmerken als persoonsinformatie van gevoelige aard. Door de advocaat van betrokkene is gevraagd om deze gegevens te depubliceren.

Conclusie en advies

Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. Dat is hier naar ons oordeel het geval.

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert het Privacy team om:

- Het datalek te melden bij de Autoriteit Persoonsgegevens.
- De melding en beoordeling zoals gebruikelijk te administreren in het provinciale logboek.

"Van: art 5 1-2e
Verzonden: 2020-05-11 09:58:05+00:00
"Aan: art 5 1-2e
"CC: Zoete - van der Hout, WH, de; art 5 1-2e
Onderwerp: Advies datalek
"
Beste art 5 1-2e

Bijgaand het advies m.b.t. het datalek van vrijdag jl.

Het advies is afgestemd met onze FG en zoals gebruikelijk opgenomen in onze administratie.

Ik hoor graag of je hiermee instemt.

Na jouw besluit kunnen we de voorlopige melding die ik afgelopen vrijdag heb gedaan bij de AP intrekken, aanpassen of definitief maken.

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 8 mei 2020 18:45
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
CC: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: RE: Aankondiging datalek

Voorlopige melding bij AP gedaan:

Tijdstip ontvangst

08-05-2020 18:41:34

Uniek nummer

art 5 1-2e

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 8 mei 2020 17:16
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
CC: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Aankondiging datalek

Hallo art 5 1-2e

Na een melding te hebben ontvangen, heb ik in de loop van de middag de datalek procedure gestart.

Ik ben met het privacy team nog bezig aan het advies.

Je ontvangt dit uiterlijk maandagochtend, nadat het door betrokkene en privacy team is gezien.

Wij zullen je in het advies adviseren om het te beschouwen als een datalek en het datalek te melden aan de AP.

Om binnen de wettelijke termijn te blijven, zal ik vast een voorlopige melding bij de AP doen.

Na jouw besluit kunnen we deze melding intrekken, aanpassen of definitief maken.

Situatie:

Het betreft een interne zaak waarbij een collega in Microsoft Teams een opname heeft gemaakt van een telefoongesprek dat een andere collega met haar teamleider had.

In de opname komen persoonlijke zaken voor.

De opname is door 1 persoon gemaakt en potentieel door 8 collega’s af te luisteren.

Er wordt nog gezocht naar een manier om de opname uit Teams te verwijderen, maar dat blijkt niet eenvoudig.

Ik doe dit in het advies verder uit de doeken.

Mocht je op voorhand vragen hebben dan hoor ik het uiteraard graag.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>
"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Concept

Melding gegevens

Naam melder	:	art 5 1-2e (betrok kene)
Registratienummer van het incident	:	M20 05 00547
Datum en tijdstip van de melding	:	Vrijdag 8 mei 2020 14:39
Route van de melding	:	E-mail

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Maandag 11 mei 2020 09:30
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e (privacy jurist)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerker

Voorlopige melding gedaan bij de Autoriteit Persoonsgegevens:

Tijdstip ontvangst: 08-05-2020 18:41:34

Uniek nummer: art 5 1-2e

Situatie

(*Korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*

Betrokkene voerde per telefoon een gesprek met haar teamleider, waarin ook vertrouwelijke zaken werden besproken.

Tijdens het telefoongesprek probeerde betrokkene een Teams chat met deze teamleider te starten, zodat ze elkaar ook konden zien. Daar ging iets mis, want ze startte per ongeluk een vergadering met een Team waar ze deel van uit maakt. De microfoon van de laptop stond daarbij open.

Omdat betrokkene en teamleider elkaar niet te zien kregen hebben ze het gesprek verder telefonisch gedaan.

Een ander lid van dat Team zag dat er een vergadering werd geopend en kwam (op de laptop) in die chat. De collega kon - doordat de microfoon en camera van de laptop open stonden - meeluisteren met het telefoongesprek. Betrokkene had dit niet in de gaten.

Een deel van het gesprek ging over persoonlijke aangelegenheden. Het meeluisterende teamlid heeft daar niet alleen in meegeluisterd, maar daar ook in Teams een opname van gemaakt.

Hij heeft dat later per e-mail bij betrokkene gemeld.

Het opgenomen audio gesprek staat opgeslagen in de chat waar de andere teamleden ook bij kunnen. Dit audio gesprek kan daar niet uit worden verwijderd. Automatisch gebeurt dit wel maar pas na 20 dagen.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Betreft een gesprek.

Vraag	Antwoord
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	1 persoon heeft meegeluisterd en een opname gemaakt. 8 collega's hebben potentieel toegang tot de opname.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Luisteren en opname
Welke persoonsgegevens betreft het?	Persoonlijk gesprek tussen betrokkene en teamleider, onder meer over de samenwerking met een collega.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja. Directe collega's.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Ja. Betreft het uitlekken van een persoonlijk gesprek. De samenwerking tussen collega's kan onder druk komen te staan. Betrokkene voelt zich aangetast in haar persoonlijke levenssfeer. Haar vertrouwen is geschaad.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja, in relatie tot de vertrouwelijkheid van de informatie.
Betreft het een datalek?	Ja. Deze informatie is bij de verkeerde persoon terecht gekomen.
Ondernomen beperkende maatregelen.	Het opgenomen audiogesprek staat in de chat waar de andere teamleden ook bij kunnen. Door de I&A Teams beheerder is gepoogd de opname uit de chat te verwijderen. Dit bleek niet mogelijk. Automatisch gebeurt dit wel maar pas na 20 dagen. De collega die de opname heeft gemaakt is Teamlid is hierop aangesproken door het bureauhoofd.

[1] Art.9 AVG: Gegevens over ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
	Het bureauhoofd heeft in de chat een bericht geplaatst over het niet afluisteren van de opname.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	De I&A beheerder van Teams is op zoek naar een manier om het audio gesprek weg te halen, misschien door de hele chat te verwijderen als dat kan. I&A doet onderzoek naar de wenselijkheid en voorwaarden van het maken van opnamen in Teams, om te zorgen dat de privacy van de Teams gebruikers niet wordt geschaad. In de Teams training dient aandacht te worden besteed aan de gevaren van het ongemerkt openzetten van camera en microfoon. In de communicatiecampagne Data Donderdag zal aandacht worden besteed aan zorgvuldig gebruik van Teams en het maken van opnamen.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.

- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval
Er is sprake van een datalek, omdat er persoonsgegevens in verkeerde handen zijn gekomen.
Gezien de vertrouwelijke aard van de informatie en omdat het de directe werkkring van betrokkene betreft, achten wij het hiermee verbonden risico voor aantasting van de persoonlijke levenssfeer van betrokkene hoog.

Conclusie en advies
Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. Dat is hier naar ons oordeel wel het geval. Het betreft informatie die de positie van betrokkene in de directe werksituatie kan schaden.

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert het Privacy team om:

- De datalek melding en beoordeling zoals gebruikelijk te administreren in het provinciale logboek.
- Het datalek te melden bij de Autoriteit Persoonsgegevens.

Het datalek is besproken met direct betrokkenen, zodat verdere actie hier niet nodig is.


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2020-07-03 11:07:50.549000+00:00
"Aan: art 5 1-2e Zoete - van der Hout, WH, de"
CC:
Onderwerp: advies datalek
"
Dag art 5 1-2e

Bijgaand mijn advies over het datalek Bibob.

Ik adviseer om wel te melden bij AP, niet bij betrokkene.

Met vriendelijke groet,

art 5 1-2e

Functionaris voor Gegevensbescherming

M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>

-Wanneer u de provincie Zuid-Holland een e-mail stuurt, ontvangt u binnen 2 werkdagen een reactie en binnen twee weken een antwoord. Al uw informatie wordt vertrouwelijk behandeld. Persoons- of adresgegevens worden uitsluitend gebruikt waarvoor u ze heeft verstrekt. Uw e-mailbericht wordt op een goede en veilige manier gearchiveerd.

-Vragen kunt u stellen via het contactformulier <https://www.zuid-holland.nl/contact/contactinformatie/> .
"


provincie
ZUID HOLLAND

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: CONCEPT

Melding gegevens

Naam melder	:	art 5 1-2e art 5 1-2e
Registratienummer van het incident	:	DL_FG_20200630
Datum en tijdstip van de melding	:	30-06-2020 17:01
Route van de melding	:	Telefonische melding

Advies

Opgesteld door	:	art 5 1-2e (FG)
Datum en tijdstip advies	:	Vrijdag 3 juli 10:00 uur
Advies besproken met	:	-
Advies ter kennisgeving gedeeld met	:	art 5 1-2e art 5 1-2e

Situatie

(*Korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*
Geheime stukken uit een Bibob-procedure zijn ingezien door onbevoegden, ondanks nadrukkelijke instructies van de betrokken Bibob-ambtenaar. De stukken zijn in iBabs geplaatst door art 5 1-2e Op dat moment was enkel de gedeputeerde, die zich bezighoudt met Bibob-aangelegenheden, de enige die toegang had tot deze stukken. Dinsdag 30 juni werd duidelijk dat de bestuursadviseur van de betrokken gedeputeerde de stukken had ingezien ondanks nadrukkelijke instructies dat deze alleen bestemd zijn voor de gedeputeerde. Hiermee zijn zowel de regels uit de Wet Bibob, de Wet politiegegevens als de AVG geschonden.

Gelet op de aard van het datalek en de geheime status van de inhoud van de documenten, is het datalek behandeld door de FG. Dit is vooraf besproken met de concerndirecteur, zonder in te gaan op de inhoud van het dossier. Het onderzoek heeft plaatsgevonden in samenwerking met de behandelend Bibob-ambtenaar.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Zeer veel, het is een omvangrijk rapport met veel (gevoelige) persoonsgegevens en politiegegevens
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Tenminste 1
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen
Welke persoonsgegevens betreft het?	Zeer veel persoonsgegevens en politiegegevens
Betreft het bijzondere	In elk geval wel politiegegevens

Vraag	Antwoord
persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja, bestuursadviseur en secretaresse
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee
Betreft het een beveiligingsincident?	Ja
Betreft het een datalek?	Ja
Ondernomen beperkende maatregelen.	Geen, het is een incidenteel issue
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Totdat er technische maatregelen zijn getroffen, zullen de stukken in hardcopy ter beschikking worden gesteld aan leden van GS

Afweging

Kaders

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Conclusie
(*Korte beschrijving van de conclusie)*
De documenten die (mogelijk) zijn ingezien betreffen de resultaten van een onderzoek in het kader van de Wet Bibob. Vanuit wet- en regelgeving zijn er strikte eisen gesteld aan de personen die inzage mogen hebben in deze documenten. In het onderhavige geval heeft tenminste 1 onbevoegde inzage gehad en valt, althans technisch, niet al te sluiten dat nog 1 medewerker onbevoegd inzage heeft gehad.

Advies
Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. Dat is hier naar mijn oordeel het geval.

Ik adviseer, gezien de bovengenoemde afwegingskaders en analyse, om:
- Het datalek te melden bij de Autoriteit Persoonsgegevens.
- De melding en beoordeling te administreren in het provinciale logboek, zij het dat het ditmaal in een sterk afgeschermde omgeving.

art 5 1-2e
Functionaris voor Gegevensbescherming

Den Haag, 3 juli 2020

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Definitief

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	M20 10 02225
Datum en tijdstip van de melding	:	Vrijdag 23 oktober 10:16 uur
Route van de melding	:	Digitale Loket

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 30 oktober 09:00
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e (jurist), art 5 1-2e (privacy officier), art 5 1-2e (adviseur informatieveiligheid)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerkers

Situatie

Melding is als onderstaand binnengekomen:

- Melding datalek Wie-is-wie Relevant
Datum 23 oktober 2020
Door art 5 1-2e
Via het Loket van de provincie Zuid-Holland naar de Autoriteit Persoonsgegevens

De landelijke website www.relevant.nl bestaat uit twee delen, een informatief deel over externe veiligheid en een wie-is-wie. De wie-is-wie is alleen zichtbaar nadat je bent ingelogd maar deze lijkt lek voor bots. Gisteren aan het einde van de middag kreeg ik het volgende signaal via een van de gebruikers:
Op de eerste pagina van de wie-is-wie staat een aantal 'fake' namen en e-mail adressen. De gebruiker die het heeft gemeld heeft meteen een snelle analyse gemaakt: ruim 250 accounts zijn naar zijn idee toe te schrijven aan Bots, dat is meer dan 18% van het bestand.

Wat we direct hebben gedaan
- Voormedia, de host van Relevant, is gevraagd om de Wie-is-Wie direct offline te zetten;
- Voormedia, de host van Relevant, is gevraagd te onderzoeken waar er nog meer gelekt is,
- Voormedia zet zo nodig de hele website Relevant offline.
- We nemen ook contact op met METT, de host van de Wie-is-Wie. Maar het lek zit waarschijnlijk aan de Relevantkant, daar gaan we dan ook vanuit. Je moet namelijk opnieuw inloggen als je via METT in de wie-is-wie wilt en dat lukt de beheerder van Relevant zelf niet.
- We zullen alle email adressen handmatig doornemen en alle verdachte accounts verwijderen.
- Als er verdere lekken zijn, of meer bekend is wat er precies is gehackt (scraping) worden daar direct gerichte acties op genomen.
Wat we daarna doen
- De inlogprocedure moet veiliger. Er zit wél een robotcontrole op, maar er zijn geen eisen aan het wachtwoord of dat een gebruiker pas toegang krijgt wanneer het opgegeven emailadres is bevestigd enz.
- De AVG richtlijnen moeten beter worden ingericht. Dus een betere beveiliging (niet meer geautomatiseerd) van de inlogaanvragen, eerst een opt-in voordat je in de wie-is-wie wordt opgenomen enz.
- de gebruikers worden met een mail op de hoogte gesteld. (Zij zijn in het verleden gemaild of het akkoord is dat hun gegevens in de Wie-is-Wie staat, dat achter inlog zit. Mensen die niet akkoord waren moesten daar toen actie op ondernomen. Dat is toen (in 2017, dus te lang geleden) niet veel gedaan, maar dat komt ook omdat een Wie-is-Wie juist bedoeld is om elkaar te kunnen vinden, het is een netwerk. Nieuwe mensen krijgen geen apart bericht over de Wie-is-wie en moeten dit krijgen en ervoor kiezen dit niet te willen.)

Ter toelichting:
Relevant is een kennisportaal waar professionele informatie op gebied van externe veiligheid wordt uitgewisseld. Er staan geen bedrijfsgevoelige informatie en data op.
In de wie is wie staan naam, professioneel email adres en telefoonnummer, organisatie en functie. Geen andere gegevens. Er worden geen financiële transacties via de website uitgevoerd.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	De website www.relevant.nl heeft ongeveer 750 geregistreerde gebruikers.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Op de website www.releveant.nl vonden zich ongeveer 250 geautomatiseerde nepaccounts (zogenaamde Bots).
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Het is technisch onmogelijk om exact te achterhalen voor welk doel de nepaccounts zijn aangemaakt. De hostingspartij heeft bevestigd in het verleden last te hebben gehad van spambots. De aangetroffen bots zijn mogelijk spambots. Deze bots verzamelen e-mailadressen om mailinglijsten samen te stellen voor het verzenden van ongevraagde e-mail, ook wel spam genoemd. Dergelijke spambots verzamelen e-mailadressen van o.a. websites, nieuwsgroepen, online adressenboeken en chatrooms. Hostingspartij bevestigd, schriftelijk, onderstaande: *Als tweede klopt het dat er een aantal gebruikers is met een vreemde naam en emailadres. Het merendeel hiervan zal inderdaad aangemaakt zijn door bots. Dit hoeft niet direct te betekenen dat deze bots ook informatie hebben gescrapet van de website, dit kunnen ook spambots zijn (hier hebben we in het verleden zeker last van gehad). Omdat het onwenselijk is dat bezoekers of bots zich registreren met onjuiste informatie lijkt het ons goed om het registratieproces strakker te maken. Je kunt hierbij denken aan een emailbevestiging of een controle- en acceptatiestap aan de kant van Relevant.* Het is niet uit te sluiten dat de bots geen informatie hebben gescrapet van de website. Scraping is een techniek waarmee data van een websites kan worden gehaald. Deze data wordt geanalyseerd en kan gebruikt worden voor allerlei verschillende, wellicht kwaadaardige, doeleinden. Naast het adressenboek, bestaat de website www.relevant.nl ook uit een informatieve deel over externe veiligheid. Deze informatie is openbaar. **Conclusie:** De website www.relevant.nl bevat geen (gevoelige) bedrijfsinformatie. De bots hebben echter wel onbevoegd toegang verkregen tot het adressenboek behorend bij de

Vraag	Antwoord
	website waarbij mogelijk een kopie gemaakt is van de aanwezige persoonsgegevens.
Welke persoonsgegevens betreft het?	Zakelijk E-mailadres, voor- en achternaam en zakelijk telefoonnummer.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Nee.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. De persoonsgegevens zijn niet gevoelig van aard.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	De website www.relevant.nl voldoet, naar verwachting, niet volledig aan de eisen conform code voor informatiebeveiliging, de verplichte standaarden van het Forum voor Standaardisatie en de richtlijnen van het NCSC.
Betreft het een datalek?	De bots hebben onbevoegd toegang verkregen tot het adressenboek behorend bij de website www.relevant.nl, waarbij mogelijk een kopie gemaakt is van de aanwezige persoonsgegevens.
Ondernomen beperkende maatregelen.	- De Wie-is-wie is direct offline gezet en het registratieportaal voor de website is gesloten. - Het besloten gedeelte van Relevant (projectruimtes) is uit voorzorg offline gehaald, in afwachting van verder onderzoek. - Het openbare gedeelte van de website blijft online, omdat er op dit moment geen aanwijzingen zijn voor onwenselijke inmenging van derden. - De nepaccounts zijn verwijderd uit de gebruikerslijst (toegang is ontzegd). - Een voorlopige melding bij de Autoriteit Persoonsgegevens (AP). - Communicatie richting betrokkenen.

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	- Verdere kwetsbaarheden op de website www.relevant.nl worden onderzocht middels een pentest. Uitkomt van de pentest stelt ons in staat om inzicht te verkrijgen in de aanwezige risico's, waarna het mogelijk is om tot verdere maatregelen te komen. - Afsluiten verwerkersovereenkomst - Publiceren privacyverklaring - Beoordeling grondslag

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

De website www.relevant.nl bevat geen (gevoelige) bedrijfsinformatie. De bots hebben echter wel onbevoegd toegang verkregen tot het adressenboek, behorend bij de website, waarbij mogelijk een kopie gemaakt is van de aanwezige persoonsgegevens. Het adressenboek bestaat mogelijk uit de volgende persoonsgegevens:

- Naam
- Telefoonnummer
- E-mailadres

Bij het beoordelen of de inbreuk gemeld dient te worden zijn de aard en gevoeligheid van de persoonsgegevens een belangrijke factor. Hoe gevoeliger de gegevens, hoe groter het risico op schade voor de betrokkenen. Het is onwaarschijnlijk dat de bekendmaking van bovenstaande persoonsgegevens ernstige schade zal veroorzaken, wel bestaat de mogelijkheid dat eventuele buitgemaakte persoonsgegevens misbruikt zullen worden (denk bijvoorbeeld aan spam). Ondanks een inbreuk op vertrouwelijkheid verwachten wij niet dat het zal leiden tot identiteitsdiefstal of -fraude, lichamelijk letsel, psychisch leed, vernedering of reputatieschade. Echter betreft het hier een situatie waarbij:

- het om een landelijke website gaat die zich richt op **externe veiligheid** (nu blijkt de website zelf een kwetsbaarheid te bevatten)
- de website wordt gebruikt door alle provincies, waarbij provincie Zuid-Holland **verantwoordelijk** is voor de bescherming van persoonsgegevens
- de website niet beschikt over een privacyverklaring (wettelijk verplicht)
- onvoldoende zicht is op het doel waarvoor de persoonsgegevens mogelijk gekopieerd zijn door bots, oftewel er is een kans dat de persoonsgegevens misbruikt worden voor kwaadaardige doeleinden

Conclusie en advies

Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) nadelige gevolgen voor de betrokkenen. Dat is hier naar ons oordeel **mogelijk** het geval. De situatie wil dat wij niet goed in staat zijn om in te schatten in hoeverre de gevolgen daadwerkelijk nadelig kunnen zijn. Uit voorzorg adviseren wij om de voorlopige melding aan AP, om te zetten in een definitieve melding en betrokkenen verder te informeren (daar waar nodig).

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert het Privacyteam om:

• Het datalek te melden bij de Autoriteit Persoonsgegevens.
• Het datalek te melden bij de betrokkenen.
• De melding en beoordeling zoals gebruikelijk te administreren in het provinciale logboek.

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: DEFINITIEF

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	M19 09 01832
Datum en tijdstip van de melding	:	11-09-2019 12:26
Route van de melding	:	Op 11-09-2019 per e-mail. Op 16-09-2019 via het Datalekformulier

Advies

Opgesteld door	:	art 5 1-2e namens het Privacyteam)
Datum en tijdstip advies	:	16 september 2019
Advies besproken met	:	art 5 1-2e (concerndirecteur), Privacyteam: art 5 1-2e (P&O), art 5 1-2e (privacy jurist), art 5 1-2e (FG)
Strekking advies gedeeld met	:	art 5 1-2e (Statengriffie).

Situatie

(*Korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*
Een I&A-medewerker heeft gemeld dat hij in het digitale Loket (hierna: Topdesk) meer persoonsgegevens kan zien dan nodig is voor de uitvoering van zijn taak. Het betreft persoonsgegevens die gevoegd zijn bij de activiteit 'aanmaken telefoonnummer' die onderdeel uitmaakt van de aanmeldingsprocedure van nieuwe Statenleden en fractiemedewerkers.

Toelichting

De Statengriffie verzorgt sinds 16-02-2016 de aanmelding van nieuwe Statenleden en fractiemedewerkers bij de afdeling Personeel en Organisatie (P&O). Bij collegewisselingen gebeurt dit in bulk op papier. Voor de personele wisselingen die tussentijds plaatsvinden, maakt de Statengriffie gebruik van aanmelding via een workflow in de applicatie Topdesk. Naast contactgegevens bevat de aanvraag gevoelige persoonsgegevens, zoals: kopie identiteitsbewijs, burgerlijke staat, handtekening, Burgerservicenummer (BSN) en IBAN-nummer. Dit verschilt per aanvraag. Per aanvraag maakt Topdesk automatisch een aantal activiteiten (taken) aan in de takenlijst van behandelaars van verschillende ondersteunende afdelingen:

- Activiteit 1. P&O Salarisadministratie: Gegevens invoeren in Workforce
- Activiteit 2. P&O Personeelszaken: Brief, Workflow
- Activiteit 3. I&A Servicedesk: Account & Autorisaties
- Activiteit 4. FZ Beveiliging: Aanmaken toegangspas
- Activiteit 5. I&A Netwerk & telecom: Telefoonnummer aanmaken
- Activiteit 6. I&A Werkplekondersteuning: Tablet & Telefoon aanleveren aan Loket
- Activiteit 7. FZ Loket: OV-Abonnement
- Activiteit 8. FZ Loket: Tas klaarmaken

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens	Het betreft de verwerking van de aanmelding van 42 personen in de periode 16-02-2016 tot 27-08-2019. Dit zijn zowel Statenleden als fractiemedewerkers. Naast

Vraag	Antwoord
persoonsgegevens het betreft)	contactgegevens bevat de aanvraag gevoelige persoonsgegevens, zoals: kopie identiteitsbewijs, burgerlijke staat, handtekening, Burgerservicenummer (BSN) en IBAN-nummer. Het aantal persoonsgegevens verschilt per aanvraag.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Er is een groep van 406 provinciale medewerkers van ondersteunende afdelingen die via de applicatie Topdesk worden taken toebedeeld krijgen en de status van uitvoering daarvan in Topdesk registreren. Dit zijn Topdesk behandelaars. De taken en bijbehorende informatie (inclusief persoonsgegevens) worden binnen de applicatie Topdesk in de vorm van activiteiten geregistreerd en in takenlijsten geplaatst. Het betreft hier niet de 'gewone' Topdesk gebruikers, die via Het Loket op het Binnenplein bestellingen plaatsen of aanvragen doen. Hun systeemrechten zijn beperkt tot het kunnen zien van alleen hun eigen aanvragen.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen. Andere vormen van verwerking zijn bij gebrek aan logbestanden niet uit te sluiten.
Welke persoonsgegevens betreft het?	Naast contactgegevens bevat de aanvraag gevoelige persoonsgegevens, zoals: kopie identiteitsbewijs, burgerlijke staat, handtekening, Burgerservicenummer (BSN) en IBAN-nummer.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Ja. Kopie identiteitsbewijs kan iets zeggen over afkomst, ras of etniciteit. Een handtekening is ook een bijzonder persoonsgegeven, in het verlengde van het handschrift.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja. • Behandelaars van P&O, I&A, FZ die een rol hebben in de afhandeling van genoemde Topdesk activiteiten. • Behandelaars van andere dan bovengenoemde Topdesk activiteiten.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Ja. Er is sprake van persoonsgegevens die gebruikt kunnen worden voor (identiteits)fraude.
Betreft het een beveiligingsincident?	Ja. De vertrouwelijkheid van de persoonsgegevens bij de uitvoering van de genoemde activiteiten is onvoldoende geborgd.

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
Betreft het een datalek? *"inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;"*	Ja. Mogelijk is er sprake geweest van ongeoorloofde toegang tot persoonsgegevens.
Ondernomen beperkende maatregelen.	• Alle aanvragen zijn in het Topdesk systeem geblokkeerd en kunnen niet meer worden ingezien. • Er zijn procesafspraken gemaakt tussen P&O en de Statengriffie over de afhandeling van eventuele nog komende tussentijdse aanmeldingen. Tot er een oplossing is, zal dit tijdelijk niet via de Topdesk applicatie worden uitgevoerd.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	• Er dient een proces- en informatieanalyse plaats te vinden over de inrichting van het proces van aanmelden en verwerken van aanvragen en welke applicatie daarbij de beste ondersteuning biedt. • Ook dient de verwerking van persoonsgegevens gecontroleerd te worden van andere processen, die via Topdesk verlopen.

Afweging

Kaders

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens de Algemene verordening gegevensbescherming (AVG)[3], wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.

[3] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 – Groep Gegevensbescherming Artikel 29, versie 6 februari 2018

- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens waarschijnlijk een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse
Voor de betreffende behandelaars van P&O, I&A en FZ is het voor de uitvoering van hun activiteiten niet nodig de volledige aanvraag te zien inclusief bijlagen (zoals kopie identiteitsbewijs). Dat is in het Topdesk systeem voor een deel geregeld. In hun takenbak wordt alleen de uit te voeren activiteit geplaatst, maar daarin zijn zonder al te veel moeite toch persoonsgegevens (waaronder burgerlijke staat, handtekening, BSN en IBAN-nummer) van de betrokkene zichtbaar. Aanvullend is het door een fout in de Topdesk software mogelijk om via enkele handelingen in het systeem de volledige aanvraag inclusief bijlagen te openen. In 2016 is dit door I&A bij de softwareleverancier gemeld, maar het heeft nog niet tot aanpassing van de software geleid. Tot slot is het voor behandelaars die ándere dan bovengenoemde taken in Topdesk afhandelen, mogelijk om de genoemde activiteiten inclusief persoonsgegevens te vinden. Deze activiteiten verschijnen weliswaar niet direct in hun takenlijst, maar zijn wel te vinden door gericht in Topdesk op trefwoorden te zoeken en enkele systeemhandelingen uit te voeren.

Er is sprake van een beveiligingsincident, omdat:
- De vertrouwelijkheid van persoonsgegevens bij de uitvoering van de genoemde activiteiten onvoldoende is geborgd.

Er is sprake van een datalek in de zin van de AVG, omdat:
- Topdesk behandelaars van P&O[4], I&A en FZ voor de uitvoering van de genoemde activiteiten kennis konden nemen van meer persoonsgegevens dan nodig was voor de uitvoering van hun taak.
- Topdesk behandelaars van andere taken – weliswaar met meer moeite en kennis van het systeem - toegang tot de persoonsgegevens konden hebben.
- De Topdesk software een fout bevat die een achterdeur naar de persoonsgegevens in de aanvraag opent.

Melding aan de Autoriteit Persoonsgegevens is nodig, omdat:
- Het persoonsgegevens betreft van zowel algemene als gevoelige aard.
- Er geen logbestanden zijn op basis waarvan we kunnen uitsluiten dat daadwerkelijk behandelaars onterecht kennis hebben genomen van persoonsgegevens; we kunnen onrechtmatige verwerking daarom redelijkerwijs niet uitsluiten.

[4] P&O valt hier gedeelte buiten omdat de behandelgroep salarisadmistratie de gegevens nodig heeft.

Risico duiding

De Topdesk behandelaars die de persoonsgegevens potentieel hebben kunnen inzien zijn provinciale medewerkers. Sommigen hebben de persoonsgegevens bij de uitvoering van hun Topdesk activiteiten nodig. We hebben geen aanwijzing dat er behandelaars zijn die daadwerkelijk gebruik hebben gemaakt van de mogelijkheid om persoonsgegevens op te zoeken die ze niet nodig hebben. Ook hebben ons geen signalen bereikt dat er misbruik van de informatie is gemaakt.
Echter, we kunnen onrechtmatige verwerking niet traceren en daardoor niet uitsluiten. Zeker wanneer het kwalitatief ernstige gegevens betreft, zoals in dit geval, is er sprake van een hoog risico en moet dit worden gemeld aan de getroffen personen.

We zijn daarom van mening dat er sprake is van een hoog risico voor de betrokkenen, omdat:

- Het gevoelige persoonsgegevens betreft die gebruikt kunnen worden voor (identiteits)fraude.
- Er een ruime groep behandelaren is die op een relatief eenvoudige manier inzage in deze persoonsgegevens kon hebben.

Advies

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders, adviseert het Privacyteam om:

- Het datalek te melden bij de Autoriteit Persoonsgegevens.
- Het datalek te melden bij de betrokken Statenleden en fractiemedewerkers.

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: CONCEPT

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	
Datum en tijdstip van de melding	:	10 mei 2019 17:21
Route van de melding	:	Per e-mail aan de FG

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	9 juli 2019
Advies besproken met	:	art 5 1-2e (concerndirecteur), art 5 1-2e privacy jurist), art 5 1-2e FG)
Advies ter kennisgeving gedeeld met	:	art 5 1-2e (dossiereigenaren).

Situatie

(korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)

Het betreft een beperkt toegankelijk e-dossier DOS-2016-0009328 in het documentaire informatiesysteem, waarin zich toch documenten bevonden die door niet-geautoriseerde medewerkers gevonden en geopend konden worden. De rechtenbeperking op het e-dossier zorgde ervoor dat het betreffende e-dossier alleen zichtbaar was bij geautoriseerde medewerkers. Echter, door gericht via de zoekfunctionaliteit in het systeem gericht op trefwoorden te zoeken, kwamen de documenten voor in de lijst met zoekresultaten en konden ze op die manier toch door niet-geautoriseerde provinciaal ambtenaren worden geopend. Een aantal van deze documenten bevatten persoonsgegevens van algemene aard, zoals voornaam, achternaam en functie.

art 5 1-2e In hetzelfde dossier is ook een document ingezien met persoonsgegevens van gevoelige aard. Hierover is een apart advies uitgebracht.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Het betreft 15 documenten die in een beperkt toegankelijke omgeving stonden. De meeste ervan bevatten algemene persoonsgegevens als voornaam, achternaam, functie en organisatie. In totaal zijn dit 59 persoonsgegevens.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Acht provinciale collega's hebben daadwerkelijk toegang gehad tot één of meerdere van deze documenten, waarin zich algemene persoonsgegevens bevinden.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	De documenten zijn geopend.
Welke persoonsgegevens betreft het?	In de meeste documenten: Voornaam, achternaam en functie van provinciale ambtenaren.

Vraag	Antwoord
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja. Omdat het documenten betreft die in een beperkt toegankelijk dossier staan, hebben deze medewerkers hierover een gesprek gehad met hun bureauhoofd. Uit dit gesprek is niet gebleken dat informatie buiten de provinciale organisatie is verspreid.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Het betreft persoonsgegevens van algemene aard over provinciale collega's. Het risico op schade bij betrokken wordt daarom als beperkt ingeschat. Ook zijn na constatering van de situatie maatregelen getroffen om de toegangsrechten te corrigeren, waarbij de documenten ontoegankelijk zijn gemaakt.
Betreft het een beveiligingsincident?	Ja. De toegangsrechten stonden niet goed, waardoor niet-geautoriseerde toegang mogelijk werd.
Betreft het een datalek? *"inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;"*	Ja. Er is sprake geweest van ongeoorloofde toegang tot persoonsgegevens.
Ondernomen beperkende maatregelen.	• De toegangsrechten op het dossier en onderliggende documenten zijn direct na constateren van het beveiligingsincident gecorrigeerd. • De betrokken medewerkers zijn aangesproken door hun bureauhoofd. • De bewustwordingscampagne Up-to-data loopt op dit moment met specifieke aandacht voor AVG en persoonsgegevens.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	• Deze situatie is gecorrigeerd, maar er is onderzoek gestart of er soortgelijke gevallen zijn waar rechten mogelijk niet correct zijn aangebracht. Correcties op de rechten worden in overleg met de dossiereigenaren doorgevoerd.

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
	• De systeembeheerders zijn geïnstueerd over de correcte procedure rond beperken van toegangsrechten. • Periodieke controles op correcte rechtenstructuur zullen worden uitgevoerd.

Afweging

Kaders

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse en advies

- Omdat de toegangsrechten in het digitale dossier niet goed aangebracht waren, is er sprake van een beveiligingslek.
- Omdat er persoonsgegevens in de documenten voorkomen, is er sprake van een datalek in de zin van de AVG. Het betreft persoonsgegevens van algemene aard. Gezien de aard van de persoonsgegevens ligt melding aan de Autoriteit Persoonsgegevens niet voor de hand.
- Gezien de aard van de persoonsgegevens en de getroffen risicobeperkende maatregelen is het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor betrokkenen.

Gezien de afwegingscriteria in de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679[3], komen we tot het oordeel dat:

- het datalek niet gemeld dient te worden bij de Autoriteit Persoonsgegevens.
- er geen melding wordt gedaan bij betrokkenen.

[3] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 – Groep Gegevensbescherming Artikel 29, versie 6 februari 2018

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: CONCEPT

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	
Datum en tijdstip van de melding	:	10 mei 2019 17:21
Route van de melding	:	Per e-mail aan de FG

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	9 juli 2019
Advies besproken met	:	art 5 1-2e (concerndirecteur), art 5 1-2e privacy jurist), art 5 1-2e FG)
Advies ter kennisgeving gedeeld met	:	art 5 1-2e dossiereigenaren).

Situatie

(korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)

Het betreft een beperkt toegankelijk e-dossier DOS-2016-0009328 in het documentaire informatiesysteem, waarin zich toch een document bevond dat door niet-geautoriseerde medewerkers gevonden en geopend konden worden. De rechtenbeperking op het e-dossier zorgde er weliswaar voor dat het betreffende e-dossier alleen zichtbaar was bij geautoriseerde medewerkers, maar een document met persoonsgegevens is toch - door via de zoekfunctionaliteit in het systeem gericht op trefwoorden te zoeken - vanuit de zoekresultaten lijst door een niet-geautoriseerde medewerker gevonden en geopend. Een van deze documenten bevatten persoonsgegevens van gevoelige aard.

art 5 1-2e In hetzelfde dossier is ook een document ingezien met persoonsgegevens van algemene aard. Hierover is een apart advies uitgebracht.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Het betreft 1 document met daarin informatie (feiten, meningen) over het functioneren van 15 provinciale provinciale ambtenaren in het betreffende dossier.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	2 personen
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Het document is geopend en aan een provinciale collega gemaild.
Welke persoonsgegevens betreft het?	Informatie (feiten, meningen) over de rol van 15 provinciale provinciale ambtenaren in het betreffende dossier.
Betreft het bijzondere	Nee

Vraag	Antwoord
persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja. Leidinggevenden hebben de situatie met de medewerkers gesproken. Uit dit gesprek is niet gebleken dat informatie buiten de provinciale organisatie is verspreid.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Na het datalek zijn maatregelen getroffen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkenen. • De toegangsrechten zijn direct gecorrigeerd. • Het aantal personen dat toegang tot de persoonsgegevens heeft gehad, is beperkt (2). Ze zijn hierop aangesproken door hun leidinggevenden. • De verspreiding van de persoonsgegevens is beperkt.
Betreft het een beveiligingsincident?	Ja. De toegangsrechten stonden niet goed, waardoor niet-geautoriseerde toegang mogelijk werd.
Betreft het een datalek? *"inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;"*	Ja. Er is sprake geweest van ongeoorloofde toegang tot persoonsgegevens.
Ondernomen beperkende maatregelen.	• De toegangsrechten op het dossier en onderliggende documenten zijn direct na constateren van het beveiligingsincident gecorrigeerd. • De betrokken medewerkers (2) zijn aangesproken door hun bureauhoofd. • De bewustwordingscampagne Up-to-data loopt op dit moment met specifieke aandacht voor AVG en persoonsgegevens.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	• Deze situatie is gecorrigeerd, maar er is onderzoek gestart of er soortgelijke gevallen zijn waar rechten mogelijk niet correct zijn aangebracht. Correcties op de rechten worden in overleg met de dossiereigenaren doorgevoerd.

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
	• De systeembeheerders zijn geïnstueerd over de correcte procedure rond beperken van toegangsrechten. • Periodieke controles op correcte rechtenstructuur zullen worden uitgevoerd.

Afweging

Kaders

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse en advies

- Omdat de toegangsrechten in het digitale dossier niet goed aangebracht waren, is er sprake van een beveiligingslek.
- Omdat er persoonsgegevens in de documenten voorkomen, is er sprake van een datalek in de zin van de AVG. Het betreft persoonsgegevens van gevoelige aard. Gezien de aard van de persoonsgegevens ligt melding aan de Autoriteit Persoonsgegevens voor de hand.
- Na constatering van het datalek zijn direct risicobeperkende maatregelen getroffen in de vorm van ontoegankelijk maken van het document. Daarna zijn audit logs geanalyseerd en zijn de

medewerkers door hun leidinggegevenden aangesproken en bevraagd. Dit heeft geleid tot de conclusie dat de informatie niet verder is verspreid en dat de medewerkers dit ook in de toekomst niet zullen doen. Gezien de situatie en de na het datalek getroffen maatregelen wordt het niet waarschijnlijk geacht dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkenen.

Gezien de afwegingscriteria in de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679[3], komen we tot het advies dat:

- het datalek gemeld dient te worden bij de Autoriteit Persoonsgegevens.
    - De melding is uitgevoerd op 21-06-2019 (registratienummer: art 5 1-2e art 5 1-2e
- er geen melding wordt gedaan bij betrokkenen.

[3] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 – Groep Gegevensbescherming Artikel 29, versie 6 februari 2018

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: CONCEPT

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	
Datum en tijdstip van de melding	:	10 mei 2019 17:21
Route van de melding	:	Per e-mail aan de FG

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	22 mei 2019
Advies besproken met	:	art 5 1-2e privacyjurist)), art 5 1-2e FG), art 5 1-2e art 5 1-2e
Advies ter kennisgeving gedeeld met	:	

Situatie

(*korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*

De melding betreft een probleem met de afscherming van geheime documenten in een gevoelig dossier: WBR-dossier (DOS-2016-0009328, warmtebedrijf). Niet toegangsgerechtigde personen hebben delen van het genoemde dossier kunnen inzien.

- De toegangsrechten tot het iDMS-dossier *DOS-2016-0009328 Deelneming Warmtebedrijf Holding 2015- 2020* zijn in december 2018 beperkt tot slechts een kleine groep medewerkers.
- Daarbij is iets niet goed gegaan, waardoor het voor niet toegangsgerechtigde personen toch mogelijk is geweest om een aantal geheime documenten uit het genoemde dossier te vinden en in te zien.
- Door de rechtenbeperking was het dossier weliswaar niet zichtbaar, maar sommige documenten in het dossier konden via een (gerichte of ongerichte) zoekactie in iDMS toch worden gevonden en geopend. Of dit expres of per ongeluk gebeurd is, dat is uit de logging niet af te leiden.

Een deel van de documenten bevat persoonsgegevens. Omdat er ook sprake kan zijn van een datalek, zijn het privacyteam en de FG ingeschakeld.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Het betreft 15 geheime documenten. De meeste ervan bevatten algemene persoonsgegevens als voornaam, achternaam, functie en organisatie. In totaal zijn dit 59 persoonsgegevens. Daarnaast heeft 1 persoon inzage gehad in een geheim rapport (Barends en Krans). Dit rapport bevat feiten, meningen en beoordelingen over het functioneren van 15 provinciale medewerkers provinciale ambtenaren die betrokken zijn in het Warmtedossier.

Vraag	Antwoord
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	• 8 personen hebben toegang gehad tot documenten, waarin zich algemene persoonsgegevens bevinden. • Waarvan 1 persoon ook toegang heeft gehad tot een geheim rapport (Barends en Krans) met de hierboven genoemde gevoelige persoonsgegevens.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	De documenten zijn geopend. Eén van de documenten is aan een PZH collega gemaild.
Welke persoonsgegevens betreft het?	• In de meeste documenten: Voornaam, achternaam, functie en organisatie van provinciale ambtenaren • In het onderzoeksrapport van Barends en Krans: gevoelige persoonsgegevens.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja. Alle medewerkers hebben een gesprek gehad met hun bureauhoofd. Uit deze gesprekken is niet gebleken dat informatie buiten de provinciale organisatie is verspreid. Eén persoon heeft het geheime rapport (Barends en Krans) gemaild aan een provinciale collega.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. • Het aantal personen dat toegang tot de persoonsgegevens heeft gehad, is beperkt. • De verspreiding van de persoonsgegevens is beperkt. • Corrigerende maatregelen zijn getroffen. • De kans dat het bekend zijn van de persoonsgegevens leidt tot schade bij betrokkenen, wordt als beperkt ingeschat. • Rapport Barends/Krans: Twee personen hebben toegang gehad tot het rapport met de gevoelige persoonsgegevens. Deze medewerkers zijn hgierop aangesproken door hun bureauhoofden. De informatie is niet verder gedeeld. • Overige documenten: De persoonsgegevens in de overige documenten zijn niet van dien aard dat er een hoog risico mee gemoeid is.
Betreft het een beveiligingsincident?	Ja
Betreft het een datalek? *"inbreuk in verband met persoonsgegevens: een inbreuk op de*	Ja.

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;"	
Ondernomen beperkende maatregelen.	• De toegangsrechten op het dossier zijn direct na constateren van het beveiligingsincident gecorrigeerd. • Alle medewerkers hebben een gesprek gehad met hun bureauhoofd. • De bewustwordingscampagne Up-to-data loopt op dit moment met specifieke aandacht voor AVG en persoonsgegevens.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	• Onderzoek in iDMS naar mogelijk soortgelijke gevallen loopt. • Correcties op de rechten worden in overleg met de dossiereigenaren doorgevoerd. • De systeembeheerders zullen worden geïnstueerd over de correcte procedure rond beperken van toegangsrechten. • Periodieke controles op correcte rechtsnstructuur moeten worden uitgevoerd.

Afweging

Kaders

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen

betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Conclusie
(*korte beschrijving van de conclusie)*

Advies
De conclusie is dat er sprake is van een beveiligingslek en dat er ook sprake is van een datalek in de zin van de AVG.
Gezien de afwegingscriteria in de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679[3], komen we tot het oordeel dat:
- het datalek niet meldingsplichtig is bij de Autoriteit Persoonsgegevens.
- er geen melding wordt gedaan bij betrokkenen.

[3] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 – Groep Gegevensbescherming Artikel 29, versie 6 februari 2018

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e Afdeling Personeel en Organisatie - Bureau Interim Consult)
Registratienummer van het incident	:	A 91451
Datum en tijdstip van de melding	:	23 augustus 2022 om 12:52 uur
Route van de melding	:	Vermissing ICT-MIDDEL formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e (Eenheid Privacy)
Datum en tijdstip advies	:	23 augustus 2022 om 15:30 uur
Advies besproken met	:	
Strekking advies ter kennisgeving gedeeld met	:	
Besluit	:	Kwalificeren als datalek, maar geen melding AP nodig.

Situatie

Op 23 augustus 2022 is via Topdesk een melding datalek ontvangen van art 5 1-2e Zie bijgevoegde oorspronkelijke melding. Het betreft de vermissing van een SIM-kaart. De melder heeft voordat hij op vakantie ging de SIM-kaart van PZH uit de werktelefoon gehaald om te voorkomen dat hij per ongeluk data van de provincie in het buitenland zou verbruiken (kosten dataverkeer). Echter, bij terugkomst kon hij de SIM-kaart niet meer vinden. Naar aanleiding van de melding is – per mail - contact opgenomen met de melder en via het ICT-plein met een collega art 5 1-2e van de afdeling I&A. Hieruit is gebleken dat de SIM-kaart inmiddels is geblokkeerd. Het is niet bekend of er gegevens – zoals namen en telefoonnummers – op de SIM-kaart stonden opgeslagen. De melder geeft in ieder geval – per mail - aan geen gegevens op de SIM-kaart te hebben opgeslagen en dat de SIM-kaart waarschijnlijk – in de week van 13 juni - in huis is zoekgeraakt. Voor zover er gegevens op de SIM-kaart stonden opgeslagen heeft I&A aangegeven dat deze door het blokkeren van de SIM-kaart ook niet meer te raadplegen zijn.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Waarschijnlijk stonden er geen gegevens op de SIM-kaart opgeslagen, maar dit is niet helemaal met zekerheid te zeggen. De melder geeft aan dat er geen volgens hem geen gegevens stonden opgeslagen.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend. Er is in ieder geval geen informatie bekend dat er door derden van de SIM-kaart gebruik is gemaakt.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Onbekend. Het meest waarschijnlijke scenario is dat er sprake is geweest van een inbreuk op de vertrouwelijkheid, dat wil zeggen dat bijvoorbeeld telefoongegevens en namen op de SIM-kaart te raadplegen waren door derden. De SIM-kaart is vergrendeld,

Vraag	Antwoord
	maar meestal betreft dit een 'standaard' PIN-code.
Welke persoonsgegevens betreft het?	Onbekend. De melder geeft aan dat er geen volgens hem geen gegevens stonden opgeslagen.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Onbekend. De melder geeft aan dat er geen volgens hem geen gegevens stonden opgeslagen. *De AVG ziet deze persoonsgegevens als bijzondere persoonsgegevens:* - *persoonsgegevens waaruit ras of etnische afkomst blijkt;* - *persoonsgegevens waaruit politieke opvattingen blijken;* - *persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;* - *persoonsgegevens waaruit het lidmaatschap van een vakvereniging blijkt;* - *gegevens over iemands gezondheid;* - *gegevens over iemands seksueel gedrag of seksuele gerichtheid;* - *genetische gegevens;* - *biometrische gegevens met het oog op de unieke identificatie van een persoon.* Het lijkt onwaarschijnlijk dat er dergelijke gegevens op de SIM-kaart stonden opgeslagen.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Onbekend. Er is in ieder geval geen informatie bekend dat er door derden van de SIM-kaart gebruik is gemaakt. Waarschijnlijk is de SIM-kaart in huis zoekgeraakt.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Van een hoog risico is sprake indien de inbreuk kan leiden tot identiteitsfraude, discriminatie en reputatieschade. Dit lijkt onwaarschijnlijk.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	De SIM-kaart is beveiligd en met alleen het bezit van een SIM-kaart is er nog geen toegang tot verdere gegevens binnen de systemen van PZH.
Betreft het een datalek?	Hiervan is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
	anderszins verwerkte persoonsgegevens (artikel 4, punt 12, AVG). Het is mogelijk dat er persoonsgegevens op de SIM-kaart stonden en dat derden deze gegevens konden raadplegen. In dat licht bezien kwalificeer ik het als een datalek.
Ondernomen beperkende maatregelen.	De SIM-kaart is geblokkeerd. Voor zover er gegevens op de SIM-kaart stonden opgeslagen heeft I&A aangegeven dat deze door het blokkeren van de SIM-kaart ook niet meer te raadplegen zijn.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	NVT.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in

verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

De melder is de SIM-kaart waarschijnlijk in huis verloren. Er is in ieder geval geen informatie bekend dat er door derden van de SIM-kaart gebruik is gemaakt. De melder geeft aan geen gegevens op de SIM-kaart te hebben opgeslagen, maar dit kan niet volledig worden uitgesloten. Verder is een SIM-kaart middels een PIN-code vergrendeld. In de praktijk betreft dit vaak wel een eenvoudig te raden PIN-code. De SIM-kaart is inmiddels geblokkeerd en hierdoor zijn eventuele gegevens die hierop stonden opgeslagen ook niet meer te raadplegen. Ten aanzien van de vermissing van een ICT middel staat in de voorbeelden bij de Guidelines aangegeven dat dit – in beginsel - niet aan de AP hoeft te worden gemeld: *Zolang de gegevens met een geavanceerd algoritme zijn versleuteld, er back-ups van de gegevens bestaan, de unieke sleutel niet is gecompromitteerd en de gegevens tijdig kunnen worden hersteld, is het mogelijk dat deze inbreuk niet hoeft te worden gemeld. Vindt er later echter een compromittering plaats, moet de inbreuk wel worden gemeld.*

Conclusie en advies

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert het Privacy team als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt NIET gemeld bij de Autoriteit Persoonsgegevens of betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.

"Van: art 5 1-2e
Verzonden: 2019-07-25 15:08:27.705000+00:00
"Aan: art 5 1-2e
"CC: Baljeu, J.N."
Onderwerp: Advies_in_kader_van_meldplicht_datalekken_05_06_2019
"
Dag art 5 1-2e

Bijgaand mijn advies omtrent de situatie van de betaalautomaat in het Y-gebouw.

Met vriendelijke groet,

art 5 1-2e

Functionaris voor Gegevensbescherming

M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>

-Wanneer u de provincie Zuid-Holland een e-mail stuurt, ontvangt u binnen 2 werkdagen een reactie en binnen twee weken een antwoord. Al uw informatie wordt vertrouwelijk behandeld. Persoons- of adresgegevens worden uitsluitend gebruikt waarvoor u ze heeft verstrekt. Uw e-mailbericht wordt op een goede en veilige manier gearchiveerd.

-Vragen kunt u stellen via het contactformulier <https://www.zuid-holland.nl/contact/contactinformatie/> .
"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: DEFINITIEF

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	
Datum en tijdstip van de melding	:	5 juni 2019
Route van de melding	:	

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	25 juli 2019, 15.00 uur
Advies besproken met	:	
Advies ter kennisgeving gedeeld met	:	

Situatie

(*korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*
In het Y-gebouw is een kleine voorziening gerealiseerd waar medewerkers broodjes en dergelijke kunnen kopen.
Het afrekenen daarvan gebeurt bij een soort betaalautomaat. Deze automaat voorziet er in dat medewerkers een account kunnen aanmaken waarbij ze geld kunnen storten op hun account waarmee afgerekend kan worden. Identificatie voor dit account kan geschieden middels een vingerafdruk.

De AVG stelt dat vingerafdrukken biometrische gegevens zijn, waarmee zij behoren tot de categorie bijzondere persoonsgegevens. Bijzondere persoonsgegevens vallen onder een zwaarder regime en mogen niet zomaar worden verwerkt door de provincie of door een derde partij in opdracht van de provincie. Hoewel het in dit geval een derde partij betreft die de biometrische gegevens niet als directe opdracht van de provincie verwerkt, kan bij medewerkers al snel de indruk ontstaan dat dit wel een voorziening is van de provincie.
In de Algemene Verordening Gegevensbescherming en de Uitvoeringswet AVG wordt ingegaan op het gebruik van biometrische gegevens. Daarin is bepaald dat biometrische gegevens vallen onder de categorie bijzondere persoonsgegevens. In beginsel is het niet toegestaan om bijzondere persoonsgegevens te verwerken tenzij daar een uitzondering voor geldt.
Uitzonderingen gelden echter niet in het geval van de betaalmogelijkheid in het Y-gebouw.
Toestemming zou normaal gesproken een uitzondering kunnen zijn. In dit geval echter niet, omdat in een werkgevers – werknemersrelatie ervan wordt uitgegaan dat toestemming niet in vrijheid gegeven kan worden. Daarbij komt dat de werknemer wordt opgezadeld met een omvangrijk en complex document inzake het geven van toestemming voor het gebruik van zijn vingerafdruk.
Verder bepaalt de Uitvoeringswet dat het verbod om biometrische gegevens, met het oog op de unieke identificatie van een persoon te verwerken, niet van toepassing is, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.
Ook deze uitzondering: noodzakelijk voor authenticatie of beveiligingsdoeleinden doet zich hier niet voor. Er kan moeilijk worden gezegd dat het voor een dergelijke betaalautomaat noodzakelijk is om vingerafdrukken te verwerken.
Er valt dan ook geen wettelijke grondslag te vinden voor het gebruik van biometrische gegevens.

Daarnaast speelt nog het volgende.
De partij die deze oplossing levert en waar de gegevens worden verwerkt, is gevestigd in de Verenigde Staten en dus buiten de EU. Zij is niet aangesloten bij het Privacy Shield én zij geeft aan dat de gebruiker

er mee in moet stemmen om bij geschillen uitsluitend in te zullen stemmen met arbitrage en zich daarbij te onttrekken aan een mogelijke gang naar de rechter.

Concluderend kan worden gesteld dat er voor de PZH geen enkele wettelijke grondslag is om gebruik te maken, of door een leverancier in opdracht van de PZH te laten maken van biometrische gegevens voor een betaalautomaat.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Waarschijnlijk betreft het een beperkte groep weknemers
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Niet bekend
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Opslaan, lezen, veranderen
Welke persoonsgegevens betreft het?	Biometrische gegevens, gekoppeld aan een account waarin naam en financiële gegevens worden verwerkt
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Ja, biometrische gegevens
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Nee, de gegevens worden verwerkt door een derde partij
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Waarschijnlijk niet, het betreft hier een verwerkingsactiviteit die behoort tot de kernactiviteit van de aanbieder
Betreft het een beveiligingsincident?	Waarschijnlijk niet, het betreft hier een verwerkingsactiviteit die behoort tot de kernactiviteit van de aanbieder
Betreft het een datalek?	Waarschijnlijk niet, het betreft hier een verwerkingsactiviteit die behoort tot de kernactiviteit van de aanbieder
Ondernomen beperkende maatregelen.	De afdeling FZ is door de FG verzocht de aangeboden dienst per direct te beëindigen. FZ heeft aangegeven dat dit zal geschieden, waar nog enige tijd overheen zal gaan eer de door

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
	medewerkers reeds gestorte bedragen zijn opgenomen.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	De leverancier moet de aangeboden dienst beëindigen.

Afweging

Kaders

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse en advies

- Er is in dit geval waarschijnlijk niet zozeer sprake een beveiligingsincident, en derhalve ook niet van een datalek.
- Het is wel in strijd met het privacy statement van de provincie waarin wordt gesteld dat persoonsgegevens niet buiten de EU mogen worden verwerkt.

- Er is wel sprake van een overtreding van de AVG door de leverancier, die biometrische gegevens verwerkt, hoewel dat in strijd is met de AVG
- Daarnaast is het bedenkelijk dat de provincie haar werknemers een dienst aanbiedt door een derde partij die zich niet wenst te onderwerpen aan het Europees recht

Gezien de afwegingscriteria in de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679[3], komen we tot het oordeel dat:

- Er geen sprake is van een datalek, en derhalve ook niet gemeld dient te worden bij de Autoriteit Persoonsgegevens.
- er geen melding wordt gedaan bij betrokkenen.

[3] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 – Groep Gegevensbescherming Artikel 29, versie 6 februari 2018


provincie
ZUID HOLLAND

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e *Afdeling I&A*)
Registratienummer van het incident	:	A 91213
Datum en tijdstip van de melding	:	8 augustus 2022 om 13:15 uur (ontvangst melding)
Route van de melding	:	Vermissing ICT-MIDDEL formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e art 5 1-2e
Datum en tijdstip advies	:	8 augustus 2022 om 15:06 uur
Advies besproken met	:	art 5 1-2e (FG)

Strekking advies ter kennisgeving gedeeld met	:	Eenheid privacy

Situatie

Op 8 augustus 2022 om 13:05 uur is via Topdesk melding van een PZH-medewerker ontvangen. Hij geeft aan op de nacht van vrijdag op zaterdag 6 augustus 2022 omstreeks 03:00 uur zijn smartphone (CI nummer CI350110412013057) te hebben verloren bij Tijdens een bezoek aan een festival te Malosewaver, Geel te Belgie is mijn telefoon kwijtgeraakt.
De smartphone stond vergrendeld en kan alleen ontgrendeld worden met een wachtwoord.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Onbekend.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend. Smartphone stond vergrendeld en is beveiligd met een wachtwoord. Persoonsgegevens waren om die reden niet eenvoudig raadpleegbaar.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Onbekend.
Welke persoonsgegevens betreft het?	Onbekend.
	Lijkt onwaarschijnlijk, maar kan niet worden uitgesloten.

Vraag	Antwoord
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Onbekend.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Onwaarschijnlijk.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Onwaarschijnlijk.
Betreft het een datalek?	Ja. De mogelijkheid bestaat dat een kwaadwillende zich door middel van een hack toegang heeft verschaft tot opgeslagen persoonsgegevens op de smartphone.
Ondernomen beperkende maatregelen.	De simkaart is vergrendeld.. Smartphone is na de verliesmelding op afstand leeggemaakt (Gewiped). Wachtwoord is ook gewijzigd door melder.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Niet van toepassing

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt?
  Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu?
  Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval
De kans dat een kwaadwillende zich toegang heeft verschaft tot (persoonsgegevens op) de smartphone lijkt klein. De smartphone is beveiligd met een wachtwoord. Na de melding is de Simkaart geblokkeerd.
Direct na de melding is de smartphone op afstand leeg gemaakt. (Gewiped).
Zolang niet bekend is geworden dat iemand zich daadwerkelijk toegang heeft verschaft tot de inhoud van de laptop volgt uit de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 dat er weliswaar sprake is van een datalek maar dat dit niet hoeft te worden gemeld.

Conclusie en advies
De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt NIET gemeld bij de Autoriteit Persoonsgegevens of betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e Projecten & Programma's)
Registratienummer van het incident	:	A 91224
Datum en tijdstip van de melding	:	8 augustus 2022 om 15:39 uur (ontvangst melding)
Route van de melding	:	Vermissing ICT-MIDDEL formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	9 augustus 2022 om 10:00 uur
Advies besproken met	:	art 5 1-2e (FG)

Strekking advies ter kennisgeving gedeeld met	:	Eenheid privacy

Situatie

Op 8 augustus 2022 om 15:39 uur is via Topdesk melding van een PZH-medewerker ontvangen.
Zij geeft aan tijdens haar vakantie, op 12 juli, haar smartphone te hebben verloren en de vermissing pas bij terugkomst te hebben doorgegeven.
De smartphone stond vergrendeld en kan alleen ontgrendeld worden met een wachtwoord.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Onbekend.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend. Smartphone stond vergrendeld en is beveiligd met een wachtwoord. Persoonsgegevens waren om die reden niet eenvoudig raadpleegbaar.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Onbekend.
Welke persoonsgegevens betreft het?	Onbekend.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in	Lijkt onwaarschijnlijk, maar kan niet worden uitgesloten.

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen,

Vraag	Antwoord
artikel 9 AVG?	
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Onbekend.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Onwaarschijnlijk.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Onwaarschijnlijk.
Betreft het een datalek?	Ja. De mogelijkheid bestaat dat een kwaadwillende zich door middel van een hack toegang heeft verschaft tot opgeslagen persoonsgegevens op de smartphone.
Ondernomen beperkende maatregelen.	De simkaart is vergrendeld.. Smartphone is na de verliesmelding op afstand leeggemaakt (Gewiped). Wachtwoord is ook gewijzigd door melder.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Niet van toepassing

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt?

godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.

[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.

- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu?
  Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

De kans dat een kwaadwillende zich toegang heeft verschaft tot (persoonsgegevens op) de smartphone lijkt klein. De smartphone is beveiligd met een wachtwoord. Na de melding is de Simkaart geblokkeerd.
Direct na de melding is de smartphone op afstand leeg gemaakt. (Gewiped).
Zolang niet bekend is geworden dat iemand zich daadwerkelijk toegang heeft verschaft tot de inhoud van de laptop volgt uit de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 dat er weliswaar sprake is van een datalek maar dat dit niet hoeft te worden gemeld.

Conclusie en advies

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt NIET gemeld bij de Autoriteit Persoonsgegevens of betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e Bureau Cultuur en Vrije Tijd)
Registratienummer van het incident	:	A 92300 / W22 09 00230
Datum en tijdstip van de melding	:	16 september 2022 om 13:21 uur (ontvangst melding)
Route van de melding	:	Vermissing ICT-MIDDEL formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	19 september 2022 om 10:11 uur
Advies besproken met	:	art 5 1-2e

Strekking advies ter kennisgeving gedeeld met	:	Eenheid privacy

Situatie

Op 16 september 2022 om 13:21 uur is via Topdesk een melding van een PZH-medewerker ontvangen. Zij meldt vermissing van haar laptop vanuit B4 teamszone stilte werkplek naast kamer massagestoel op donderdag 15 september na 17.00. De laptop was afgesloten voordat de collega de stilteruimte heeft verlaten. Collega art 5 1-2es vervolgens rond 19:00 uur nog terug geweest in de betreffende ruimte en heeft haar spullen meegenomen, echter zonder de laptop in haar tas te stoppen.

Vandaag heeft zij de beveiliging benaderd, die de laptop vervolgens in de betreffende ruimte heeft aangetroffen, waarbij de beveiligingsmedewerker heeft vastgesteld dat de laptop was uitgeschakeld. De laptop is door de beveiligingsmedewerker zeker gesteld en zal maandag door art 5 1-2e daar worden opgehaald.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Hoogstwaarschijnlijk geen.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Hoogstwaarschijnlijk geen. Laptop stond uitgeschakeld en is beveiligd met een wachtwoord. Persoonsgegevens waren om die reden niet eenvoudig raadpleegbaar.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Hoogstwaarschijnlijk geen.

Vraag	Antwoord
Welke persoonsgegevens betreft het?	Onbekend
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Lijkt onwaarschijnlijk.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Onbekend.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Hoogst onwaarschijnlijk.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Onwaarschijnlijk.
Betreft het een datalek?	Ja. De mogelijkheid bestaat dat een kwaadwillende zich door middel van een hack toegang heeft verschaft tot lokaal opgeslagen persoonsgegevens op de laptop
Ondernomen beperkende maatregelen.	De laptop is door de beveiliging zeker gesteld en zal maandag door melder aldaar worden opgehaald.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Niet van toepassing

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt?
  Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu?
  Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

<u>Analyse van dit specifieke geval</u>
Zolang niet bekend is geworden dat iemand zich daadwerkelijk toegang heeft verschaft tot de inhoud van de laptop volgt uit de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 dat er weliswaar sprake is van een datalek maar dat dit niet hoeft te worden gemeld.

Conclusie en advies
De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt NIET gemeld bij de Autoriteit Persoonsgegevens of betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e (bureau subsidies)
Registratienummer van het incident	:	(M22 07 02449)
Datum en tijdstip van de melding	:	28 juli 2022 11:43 (ontvangst melding)
Route van de melding	:	Datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e en art 5 1-2e
Datum en tijdstip advies	:	3 augustus 2022 om 11:49 uur
Advies besproken met	:	art 5 1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Eenheid privacy

Situatie

Het betreft hier een incident waarbij een brief waarin de provincie mededeelt aan een burger aangifte te doen van strafbare feiten aan twee gemeenten is verstrekt. De naam van de burger is daarbij ook aan de gemeenten verstrekt. Er is daarnaast ook telefonisch bij de gemeenten geïnformeerd of zij ook aangifte wilden doen jegens deze persoon vanwege het gebruik in privé van briefpapier van de gemeenten,

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Eén. De naam van een burger
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend. Ambtenaren bij de gemeente Halderberge en gemeente Gorinchem.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Persoonsgegevens zijn ingezien door onbevoegden.
Welke persoonsgegevens betreft het?	De naam van een burger
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.

Vraag	Antwoord
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Nee. Ambtenaren bij de gemeente Halderberge en gemeente Gorinchem konden een naam van een burger lezen op een bijlage.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	ja, het betreft een aankondiging dat de provincie aangifte doet vanwege strafbare feiten bij de politie jegens deze persoon. Aangezien deze persoon werkzaam is geweest bij die gemeenten is hij geïdentificeerd door die gemeenten.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Nee.
Betreft het een datalek?	Ja.
Ondernomen beperkende maatregelen.	De beide gemeente zijn ingelicht. Verzocht is om de betreffende bijlage te wissen/vernietigen.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Collega's bij bureau subsidies worden geïnstrueerd over de AVG en het beperken van het delen van namen van burgers aan collega overheden.

Afweging

<u>Toelichting op het wettelijke kader *(standaard tekst)*</u>

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt?
  Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.

[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu?
  Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

Het betreft hier een incident waarbij een brief waarin de provincie mededeelt aan een burger aangifte te doen van strafbare feiten aan twee gemeenten is verstrekt. De naam van de burger is daarbij ook aan de gemeenten verstrekt. Er is daarnaast ook telefonisch bij de gemeenten geïnformeerd of zij aangifte wilden doen jegens deze persoon vanwege het gebruik in privé van briefpapier van de gemeenten, Er is derhalve sprake van een hoog risico voor betrokkene. Er bestond voor de provincie geen wettelijke grondslag om deze informatie met de gemeente te delen. Bovendien kunnen er naar de opinie van de eenheid Privacy vraagtekens gezet worden bij de stelling van de provincie dat deze persoon een strafbaar feit jegens die gemeenten heeft gepleegd. Betrokkene dient daarom geïnformeerd te worden over dit datalek.

Het betreft hier een datalek dat gemeld dient te worden aan de Autoriteit Persoonsgegevens.

Conclusie en advies

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt WEL gemeld bij de Autoriteit Persoonsgegevens en betrokkene.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.

art 5 1-2e

Van: art 5 1-2e
Verzonden: maandag 6 februari 2023 14:00
Aan: Servicedesk ICT-Plein
CC: art 5 1-2e
Onderwerp: TOPdesk M22 10 03600Virus of vermoeden /malware/spyware/adware/ ransomware/etc.

Beste collega's,

In deze melding staat rechts onderin (zie onderstaand) het advies om een (extra) TOPdesk melding te maken voor de Eenheid Privacy. Dit is zo te zien niet gebeurd, en ook niet (meer) nodig. Ik heb contact gehad met melder Jort Verhulst, die verklaarde dat er geen inbreuk op persoonsgegevens heeft plaatsgevonden. Daarom hoeft deze melding niet verder te worden gemeld als Datalek.

Dit ticket kan daarom worden afgesloten.

Hartelijk dank,
art 5 1-2e

art 5 1-2e art 5 1-2e **onzichtbaar voor aanmelder**

Acties uitgevoerd door de Servicedesk en de gebruiker: pop up notificaties geblokkeerd en de wi
Linkjes geopend in spam mail of iets anders aan geklikt/doorgegeven: nee
Data gelekt en/of data versleuteld?: nee
Wat is zichtbaar (foutmeldingen/eventuele printscreens): zie screenshots
Wanneer dit incident is voorgevallen: 10:30 - 31-10-2022
Waar dit incident is voorgevallen (PZH locatie, thuis, onderweg): PZH
Was de telefoon/tablet/laptopvergrendeld op moment van incident:

Kennisbank: KI 0168

Deze procedure uitvoeren::

1. Wachtwoord reset uitvoeren (KI 0076)

2. Deze melding doorzetten Serverbeheer: BIS - Serverbeheer
Ter technische beoordeling over dit incident

3. En een (extra) Topdesk melding maken en doorzetten naar Eenheid Privacy: Bestuur - Eenheid
Ter informatie over dit incident

4. Betreffende laptop/telefoon/tablet zekerheidshalve omwisselen (KI 0507)

Met vriendelijke groet,

art 5 1-2e

Privacy Officer

provincie Zuid-Holland

Eenheid Privacy
T art 5 1-2e | **Mail** art 5 1-2e @pzh.nl

Provincie Zuid-Holland | Zuid-Hollandplein 1
Postbus 90602 | 2509 LP Den Haag
www.zuid-holland.nl

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e
Verzonden: 2023-05-24 08:23:18+00:00
Aan: art 5 1-2e
CC: art 5 1-2e
Onderwerp: Re: Definitief RE: Conceptadvies datalek A99581
"
Akkoord.

<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAAb9ysg&data=05%7C01%7 art 5 1-2e art 5 1-2e 40pzh.nl%7C824cc1ab188e4856a9e008db5c1f5d3d%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015609209%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=TxqLnDfXYRAovX9tfWEt6PwnBkdcFWTWdQ%2BOdbwHQlw%3D&reserved=0>

Met vriendelijke groet,

art 5 1-2e art 5 1-2e

Functionaris voor Gegevensbescherming

Gerechtelijk Deskundige

<olm://attachment/AQADAAAAyQAAAAAAAAAAM74HAAAAAAAA1AAAAAAABD9sAAAAAAAHvjMAAAAAAAQ_bAMAAIAAAAAAJW5lLmJvbnNAcHpoLm5sX0FjdGl2ZVN5bmNFeGNoYW5nZV9IeFM%3D/AQADAAABagAAAAAAAAAAPL4HAAAAAAABZwAAAAAABD1TAAAAAAAHvjwAAAAAAAQ9UwMAAIAAAAAAJW5lLmJvbnNAcHpoLm5sX0FjdGl2ZVN5bmNFeGNoYW5nZV9IeFM%3D>

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl%7C824cc1ab188e4856a9e008db5c1f5d3d%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015609209%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=akyvDHFfWTEqGof3VvwEUTJhU6tJPjSCgWEa8Ls0Afk%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Outlook voor Android <https://eur03.saf ks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAAb9ysg&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl%7C824cc1ab188e4856a9e008db5c1f5d3d%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015609209%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=TxqLnDfXYRAovX9tfWEt6PwnBkdcFWTWdQ%2BOdbwHQlw%3D&reserved=0> downloaden

---

From: art 5 1-2e < art 5 1-2e pzh.nl>
Sent: Wednesday, May 24, 2023 8:21:14 AM

To: art 5 1-2e < art 5 1-2e pzh.nl>
Cc: art 5 1-2e < art 5 1-2e pzh.nl>
Subject: FW: Definitief RE: Conceptadvies datalek A99581

Akkoord?

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7C824cc1ab188e4856a9e008db5c1f5d3d
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015765475%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=U39IC7m1rce8rWPx00tDV3LE0%2BjDXxY%2FraqBX1nE27o
%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: dinsdag 23 mei 2023 17:26
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Definitief RE: Conceptadvies datalek A99581

Dit is ‘m.

Met vriendelijke groet,

art 5 1-2e

Privacy Officer

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protect outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art 5 1-2e art 5 1-2e 40pzh.nl
%7C824cc1ab188e4856a9e008db5c1f5d3d
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015765475%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=U39IC7m1rce8rWPx00tDV3LE0%2BjDXxY%2FraqBX1nE27o
%3D&reserved=0>

Werkdagen: ma, di, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 23 mei 2023 16:12
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: Conceptadvies datalek A99581

Hi art 5 1-2e

Check nog even de slotparagraaf. Dat loopt niet helemaal lekker mbt tot de
wipeactie van de servicedesk.

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protect outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art 5 1-2e art 5 1-2e 40pzh.nl

Van: art 5 1-2e
Verzonden: 2023-09-14 11:40:34+00:00
Aan: art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e
CC: art 5 1-2e
Onderwerp: Akkoord iDMS-datalekonderzoek ihkv AP-melding
"
Goedemorgen art 5 1-2e art 5 1-2e& art 5 1-2e

Zoals zojuist besproken in onze Teams-meeting (dd 14-9-2023, 11:00) hierbij ons (mede namens art 5 1-2e akkoord om verder onderzoek te verrichten in iDMS in het kader van datalekonderzoek voor de Autoriteit Persoonsgegevens.

Dit onderzoek zal zich richten op openbaar toegankelijke (kopieën van) paspoorten, curriculum vitae's en Bibob-documenten in iDMS.

Met vriendelijke groet,

art 5 1-2e

Privacy Officer

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7 art 5 1-2e %40pzh.nl
%7Cb9f1dba5135847dbfa6a08dbb506a531%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638302812365484859%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C
%7C&sdata=vAxGEcso9ZQNscJNZeKi5yjFJtfSHlTSQJZBbDcepW8%3D&reserved=0>

Werkdagen: ma, di, wo, do

Elke dag beter. Zuid-Holland.

"


provincie
Zuid-Holland

Uitleg Azure en de portal

Azure is het cloud computing platform van Microsoft. De provincie gebruikt dit platform als gedistribueerd datacenter voor het hosten van diverse applicaties. Ook biest Azure aan beheerders en ontwikkelaars diverse tools en ontwikkelplatforms, zoals voor de BI omgeving. Technisch beheerders van Azure en ontwikkelaars van applicaties binnen I&A maken gebruik van deze omgeving. Zij hebben binnen Azure via speciale rechten voor toegang tot de tools om hun werkzaamheden uit te voeren. Om het makkelijk te maken biedt Microsoft standaard voor iedere Azure omgeving een web-pagina genaamd de Azure Portal. Dit is een soort dashboard, wat gebruikers een overzicht biedt van programma's, ontwikkeltools en informatie over de Azure omgeving.

Gewone gebruiker hoeven niet in te loggen op de portal, omdat zij de applicaties en data die zij van Azure nodig hebben, via het startmenu op hun laptop beschikbaar hebben. I&A biedt gewone gebruikers dan ook geen linkjes of verwijzingen naar de portal en je kunt je afvragen of men weet van het bestaan van deze portal.

De melding

De melder van het datalek kwam per toeval op de Azure Portal terecht, naar aanleiding van de Microsoft Security Training die hij volgde n.a.v. de phishing-campagne die door I&A is uitgevoerd.

Hij heeft aan art 5 1-2e gemeld dat hij naar de webpagina van de portal kon gaan en daar informatie kon zien over alle op Azure geregistreerde gebruikers, waaronder persoonsgegevens. De informatie betrof zowel PZH medewerkers als derden die van PZH toegang hebben gekregen tot bepaalde applicaties of gedeelde samenwerkingsomgevingen.

De volgende persoonsgegevens waren voor de melder in te zien:

- Van PZH-medewerkers: dezelfde informatie die ook in het smoelenboek op het Binnenplein staat aangevuld met het PZH personeelsnummer. Het personeelsnummer is herleidbaar naar een individu en dus een persoonsgegeven.

- Van derden: een door PZH gegenereerde gebruikersnaam en een geregistreerd e-mailadres. Ook deze gegevens zijn herleidbaar naar individuen.

Analyse van de melding

De toegangsrechten binnen de Azure omgeving zijn gesynchroniseerd met de Citrix omgeving, waardoor het inloggen op de portal gebeurt via single sign on. Als je rechten binnen Citrix hebt, hoef je op de portal geen username en wachtwoord meer in te vullen.

De melder is een gewone gebruiker; hij heeft geen speciale toegangsrechten binnen Azure om (via de portal) toegang te hebben tot beheer- of ontwikkeltools. Wel kon hij informatie inzien over gebruikers. Dit is veroorzaakt doordat de toegangsrechten op

deze informatie niet dichtgezet zijn voor gewone gebruikers. Dit is te classificeren als een informatiebeveiligingsincident.

Het informatiebeveiligingsincident is te kwalificeren als een datalek als het heeft geleid tot ongeoorloofde toegang tot deze informatie. Dit is hier het geval.

Genomen maatregelen:

I&A heeft op 4 augustus 2021 een beperking aangebracht in de toegangsrechten tot de Azure Portal, waardoor gewone gebruikers geen toegang meer hebben tot de portal.

Duiding van het risico

Het risico hangt af van de aard van de gegevens en de hoeveelheid mensen die kennis heeft genomen van de persoonsgegevens.

Het personeelsnummer van PZH medewerkers kwalificeert niet als een gevoelig persoonsgegeven. Het risico van kennis van dit gegeven door onbevoegden wordt als laag ingeschat.

De audit log is geanalyseerd van de aanmeldingen van de laatste maand voorafgaand aan de melding (periode 08-07-2021 t/m 04-08-2021) op de Azure Portal. Dit betreft aanmeldingen op de beginpagina van de portal. Het is (nog niet) mogelijk gebleken om de log te versmalllen naar alleen toegang tot de gebruikersgegevens. Uit de log blijkt dat - naast degene die de melding heeft gedaan – alleen geautoriseerd I&A personeel de portal heeft bezocht. De onbevoegde toegang in deze periode is beperkt gebleven tot één PZH medewerker.

Daarmee wordt het risico van dit datalek als laag ingeschat.

Conclusie

Er is sprake van een datalek van beperkte omvang en met een laag risico. Maatregelen zijn getroffen om herhaling te voorkomen.

Het is niet nodig dit datalek te melden aan de AP. Het datalek wordt geregistreerd in het logboek.

art 5 1-2e

Van: art 5 1-2e
Verzonden: donderdag 2 februari 2023 16:36
Aan: art 5 1-2e
Onderwerp: RE: Virusmelding 31-10-2022

Beste art 5 1-2e

Zie hieronder.

Groeten art 5 1-2e

Van: art 5 1-2e < art 5 1-2e @pzh.nl>
Verzonden: donderdag 2 februari 2023 11:32
Aan: art 5 1-2e o zh.nl>
Onderwerp: Virusmelding 31-10-2022

Beste art 5 1-2e

Graag kom ik namens de eenheid Privacy nog even terug op je melding van een mogelijk virus bij het openen van pop-up notificaties op https://rijnengouwewiericke.nl/. Deze melding heb ik destijds gemist doordat die niet in mijn mailbox is terechtgekomen.

Om te kunnen beoordelen of hier sprake is geweest van een inbreuk op persoonsgegevens (datalek) heb ik nog een paar vragen:

1. Heeft I&A naar jouw mening dit incident afdoende afgehandeld? Ja, heel serieus; meteen digitale check gedaan. En ik moest mn wachtwoord aanpassen. En de week erna heb ik mn computer omgewisseld.
2. Heb je de indruk dat onbevoegden toegang hebben gehad tot jouw computer? Nee. Ik heb een of twee keer een pop-up gekregen en toen heb ik meteen I&A gebeld en is er digitaal meegekeken door I&A op mn pc en hetgeen de pop-up veroorzaakte is gevonden en verwijderd.
3. Heb je de indruk dat er persoonsgegevens (*informatie over een geïdentificeerde of identificeerbare natuurlijke persoon*) verloren zijn gegaan, bewerkt zijn door onbevoegden of “buit zijn gemaakt”? Nee, ik ben niks geks tegengekomen.
4. Heb je nadien nog “last” gehad van de gevolgen van dit incident? Nee, niks meer van gemerkt.

Ik verneem graag per e-mail of telefoon je reactie. Bij voorbaat dank.

Met vriendelijke groet,

art 5 1-2e
Privacy Officer

provincie Zuid-Holland

Eenheid Privacy
M art 5 1-2e **Mail** art 5 1-2e @pzh.nl

Provincie Zuid-Holland | Zuid-Hollandplein 1
Postbus 90602 | 2509 LP Den Haag
www.zuid-holland.nl

Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	23-10-2020 15:47:52
Uniek nummer	art 5 1-2e

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Naam van het bedrijf of de organisatie	Provincie Zuid-holland
Adres	Zuid-Hollandplein 1
Postcode	2596AW
Plaats	Den Haag
In welke sector is de organisatie of het bedrijf actief?	Openbaar bestuur - Provincie

Wie meldt het datalek?

Naam	art 5 1-2e
Functie	Tactisch Specialist Informatieveiligheid
E-mailadres	art 5 1-2e Op zh.nl
Telefoonnummer	art 5 1-2e

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Ja

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Ja, namelijk:
Naam van de andere organisatie die betrokken was bij de inbreuk	Voormedia

In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?

Hostingpartij

2. Tijdlijn

Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	23-10-2020

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Hacking, malware (bijv. ransomware) en/of phishing

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest
aanwezigheid van bots. Onderzoek naar impact loopt.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Nee
Burgerservicenummer (BSN)	Nee
Contactgegevens	Ja
Toegangs- of identificatiegegevens	Nee
Financiële gegevens	Nee
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee

Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	750

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja
Klanten (huidig en potentieel)	Nee
Leerlingen of studenten	Nee
Patiënten	Nee
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
Relevant is bedoeld voor professionals die in hun werk te maken hebben met Externe Veiligheid. De website richt zich met name op medewerkers van gemeenten, provincies en (regionale) samenwerkingsverbanden.

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	1
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	750

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere	Nee

manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Nee
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Nee
Financiële verliezen	Nee
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde	Nee

persoonsgegevens	
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Ja
Wanneer heeft u het datalek gemeld aan de betrokkenen?	23-10-2020

Wat is de inhoud van de melding aan de betrokkenen?
Informatie over het vermoedelijke datalek.

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	750
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	mail

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
Website is offline gehaald tot nader onderzoek

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende	Nee

gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?	Nee

9. Overig

Is naar uw mening deze melding compleet?	Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

Terug

Een datalek! Wat nu?

Een datalek binnen de provincie Zuid-Holland? Meld dit dan zo snel mogelijk via het Loket.

Wat is een datalek?

We spreken van een datalek als persoonsgegevens onrechtmatig verwerkt of verloren gegaan zijn. Bijvoorbeeld als persoonsgegevens in handen vallen van derden, die geen toegang tot die gegevens mogen hebben. Persoonsgegevens onbedoeld vernietigen of onbruikbaar maken is ook een datalek.

Een datalek! Wat nu?

Het team van de eenheid Privacy behandelt datalekken. Het team (of de Functionaris voor Gegevensbescherming zelf) kan daarna nog contact opnemen voor meer details. Maak je geen zorgen: het kan iedereen overkomen en het is niet strafbaar! Datalekken komen in iedere organisatie voor en elk datalek is een leermomentje. Wij kunnen als organisatie overigens wel een boete krijgen van de Autoriteit Persoonsgegevens, als wij datalekken niet of niet op tijd melden.

Waarom is het zo belangrijk om een datalek onmiddellijk te melden?

Wij moeten als provincie binnen 72 uur een datalek bij de Autoriteit Persoonsgegevens melden. Er moet dan wel een grote kans op ernstige nadelige gevolgen voor de (bescherming van) persoonsgegevens van de betrokkene(n).

Daarom is het belangrijk om een datalek meteen te melden via Het Loket, zodat we nog tijd hebben om te onderzoeken hoe groot het datalek is en hoe groot de mogelijke gevolgen kunnen zijn van het datalek.

Denk na over hoe je met persoonsgegevens omgaat

Het is eigenlijk een heel eng idee dat iemand met minder goede bedoelingen aan allerlei persoonsgegevens kan komen én deze kan verspreiden. Daarom besteden we veel aandacht aan informatieveiligheid en hoe we omgaan met persoonsgegevens. Eén goede richtlijn is:
Ga om met de persoonsgegevens van een ander zoals je met je eigen gegevens omgaat!

Dus: vermoed of constateer je een datalek? Meld het!

Voorbeelden van mogelijke datalekken:

- Gevoelige persoonsgegevens sturen naar een onjuist e-mailadres, dus naar iemand waar de gegevens niet voor bedoeld zijn.
- Documenten waarin persoonsgegevens staan sturen naar een organisatie die de persoonsgegevens niet nodig heeft voor de uitvoering van haar taak.
- Een brief met daarop persoonsgegevens naar de verkeerde persoon sturen.
- Zonder noodzaak op internet documenten met persoonsgegevens publiceren.
- Vermiste of gestolen gegevensdragers met persoonsgegevens (bijvoorbeeld telefoon, laptop, tablet, documenten, USB stick).
- Als je toegang hebt tot persoonsgegevens waar je geen toegang toe zou moeten hebben.
- Inbraak in een computer met onversleutelde persoonsgegevens.
- Anonieme enquêteresultaten die toch herleidbaar blijken te zijn tot respondenten.
- Afgedrukte documenten met persoonsgegevens die onbeheerd bij een kopieerapparaat liggen.

In de groep AVG vind je onder 'Procedures, modellen en regelingen' de procedure om datalekken af te handelen. Neem bij twijfel of vragen contact op met de eenheid Privacy via privacy@pzh.nl.

Bekijk ook de animatie 'Wat doe je bij een datalek?'

Ontvangstbevestiging van melding inbreuk

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596 AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

AUTORITEIT
PERSOONSGEGEVENS

[✓] Provincie

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	art 5 1-2e
Functie	Adviseur Informatieveiligheid
E-mailadres	art 5 1-2e @pzh.nl
Telefoonnummer	art 5 1-2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	1-1-2019
(Mogelijke) einddatum van de inbreuk	27-9-2021
4.2 Wanneer is het incident ontdekt?	23-9-2021
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Betrokkenen kwam een Pdf-bestand met persoonsgegevens tegen op het internet. Helaas waren de persoonsgegevens in dit bestand niet goed afgelakt.
4.4 Is dit het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

AUTORITEIT
PERSOONSGEGEVENS

Beschrijf hieronder waarom u de inbreuk later dan 72 uur na ontdekking meldt:	Tijd voor onderzoek nodig gehad om exact te achterhalen hoe complex het datalek is.

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Persoonsgegevens per ongeluk gepubliceerd

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Publicatie van een Pdf-bestand waarbij persoonsgegevens onjuist zijn afgelakt. Door de tekst te kopiëren en te plakken in een ander bestand zijn de persoonsgegevens zichtbaar te maken.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Contactgegevens

[✓] E-mailadres

[✓] Telefoonnummer

[✓] Locatiegegevens

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

AUTORITEIT PERSOONSGEGEVENS

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("**-gegevensregisters**") zijn getroffen door het datalek	100
Geef een toelichting op bovengenoemd aantal:	Wij schatten in dat het om meer dan 100 betrokkenen gaat.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Inwoners Provincie Zuid-Holland
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1
Het maximum aantal betrokkenen is:	200

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

AUTORITEIT PERSOONSGEGEVENS

Meerdere opties zijn mogelijk.

[✓] Ongeoorloofde ongedaanmaking van pseudonimisering

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Persoonsgegevens zijn afgelakt, echter kon men deze vooralsnog inzien door simpel de tekst te selecteren en elders te plakken. In eerste instantie zat er dus degelijk een vorm van bescherming, echter was deze gemakkelijk ongedaan te maken. Wij schatten in dat het grote publiek geen inzage heeft gehad in de persoonsgegevens, tenzij een kwaadwillende bewust inzage wilde hebben in de afgelakte gegevens. Dat is niet uit te sluiten. In combinatie met locatiegegevens kan er een beperkt risico optreden voor de betrokkenen.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Ja
Aan hoeveel personen wilt u de inbreuk gaan melden?	200
Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?	15-10-2021
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Uitleg over het datalek en ondernomen maatregelen.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

AUTORITEIT
PERSOONSGEGEVENS

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	mogelijk via de website, anders mail

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Alle bestanden van het internet verwijderd.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Onderzoek naar hoe wel juist gegevens af te lakken.

Privacyverklaring

Van: art 5 1-2e
Verzonden: 2023-09-22 16:18:08+00:00
Aan: art 5 1-2e
CC: art 5 1-2e art 5 1-2e
Onderwerp: Bevestiging m.b.t. onderzoekrsresultaten
"
Hoi art 5 1-2e

Wellicht ten overvloede maar voor de volledigheid bevestig ik bij deze dat in de eerste rapportage gegevens bescherming ook treffers zitten die voldoende zijn afgeschermd en is gemaakt met systeembeheersrechten.

Met vriendelijke groet,

art 5 1-2e

Functioneel Beheer

art 5 1-2e

"

Van: art 5 1-2e art 5 1-2e
Verzonden: 2021-03-10 13:18:55+00:00
Aan: art 5 1-2e art 5 1-2e art 5 1-2e
CC: art 5 1-2e ; art 5 1-2e
art 5 1-2e art 5 1-2e ; art 5 1-2e
Onderwerp: Bevinding audit rapport tbv onderzoek datalek
"
Collega's,

Hier onze bevindingen n.a.v. audit onderzoek:

Er is een rapport gemaakt door Technisch Applicatiebeheer art 5 1-2e om audit gegevens te achterhalen van 3 mappen in het archief. (M21 03 00910 WR voor auditgegevens dossiers archief)

Op 10 maart 2021 hebben Functioneel beheer art 5 1-2e n art 5 1-2e en Record Management (art 5 1-2e e art 5 1-2e het audit rapport geanalyseerd. Dit rapport bevat meer van 200.000 items.

In het rapport komt vaak de naam van art 5 1-2e voor, omdat zij afgelopen vrijdag 5 maart veel dossiers heeft verplaatst (aktie Move). Er waren 269 personeelsdossiers / verwerven en aannemen in het archief verplaatst. Daarnaast zijn ook de 702 personeelsdossiers / in stand houden bedrijfskapitaal (oud) in het archief verplaatst.

In de audit gegevens zagen we nog andere namen die 'iets' gedaan hadden (bijv. openen, wijzigen, printen, downloaden). Dit is gecontroleerd en het zijn medewerkers van RM, DIV, P&O, van WOB art 5 1-2e en art 5 1-2e

Eén rapport is in de loop van de ochtend nog nader uitgezocht, maar ook hier zijn geen acties te vinden door onbevoegden.

Conclusie: er heeft geen ongeoorloofde toegang plaats gevonden.

@art 5 1-2e art 5 1-2e<mailto : art 5 1-2e pzh.nl> Mocht je het rapport willen zien, laat het ons weten. Na 1 week wordt dit rapportje vernietigd.

Met vriendelijke groeten,

art 5 1-2e art 5 1-2e

Record management en Functioneel beheer iDMS

Van: art 5 1-2e art 5 1-2e
Verzonden: woensdag 10 maart 2021 10:35
Aan: art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl>
CC: art 5 1-2e < art 5 1-2e pzh.nl> ; art 5 1-2e
art 5 1-2e pzh.nl> ; art 5 1-2e pzh.nl>
Onderwerp: controle rapport tbv onderzoek datalek : status bevinding

art 5 1-2e

Vanmorgen met Functioneel beheer en Record Management het audit rapport geanalyseerd. Dit rapport bevat meer van 200.000 items.

In het rapport komt vaak de naam van art 5 1-2e voor, omdat zij afgelopen vrijdag veel dossiers heeft verplaatst (aktie Move). Er waren 269 personeelsdossiers / verwerven en aannemen in het archief verplaatst. Daarnaast zijn ook de 702 personeelsdossiers / in stand houden bedrijfskapitaal (oud) in het archief verplaatst.

In de audit gegevens zagen we nog andere namen die 'iets' gedaan hadden (bijv. openen, wijzigen, printen, downloaden). Dit is gecontroleerd en het zijn medewerkers van RM, DIV, P&O, van WOB art 5 1-2e en art 5 1-2e

Op één rapport heb ik nog een vraag gesteld aan Technisch applicatiebeheer om voor de zekerheid na te gaan of het rapportje wel klopt omdat er weinig auditgegevens hierop staan. (Het kan waarschijnlijk wel kloppen, want er waren ook in een bepaald folder slechts een paar dossiers). Als art 5 1-2eit kan bevestigen, dan gaan wij ervan uit dat er geen ongeoorloofde gebruikers hebben gekeken in de dossiers.

Dit is de status even tussendoor. Ik wacht af op reactie van art 5 1-2e

Groet, art 5 1-2e

Van: art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: woensdag 10 maart 2021 09:37
Aan: art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: controle rapport tbv onderzoek datalek

Dankjewel, ik ben benieuwd

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 9 maart 2021 14:50
Aan: art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Re: controle rapport tbv onderzoek datalek

Rapport is gemaakt. Morgen gaan we analyseren en uitzoeken

Groet, art 5 1-2e

Outlook for Android <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2Fghei36&data=04%7C01%7art 5 1-2e art 5 1-2e 40pzh.nl%7Cd184984906cd4388a0fa08d8e3beacd2%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C637509755366456449%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=Wnl2rfr7ZRPXjczq%2Bck1aUuH9ykq1gimkPRrw4bHgrI%3D&reserved=0>
downloaden

From: art 5 1-2e art 5 1-2e
Sent: Tuesday, March 9, 2021 10:33:12 AM
To: art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Subject: RE: controle rapport tbv onderzoek datalek

art 5 1-2e art 5 1-2e moet het nog bespreken me t art 5 1-2e Ik laat je weten.

Groet, art 5 1-2e

Van: art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 9 maart 2021 09:40
Aan: art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: controle rapport tbv onderzoek datalek

Hoi art 5 1-2e

Dankjewel. Enig idee wanneer het rapport gedraaid zal zijn?

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: rt 2021 14:15
Aan: art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: controle rapport tbv onderzoek datalek

Heren,

Ik heb een melding uitgezet bij Technisch Applicatiebeheer voor een controle rapport. Met dit rapport kunnen we nagaan wie in een bepaalde map (en tijd) een item heeft geopend.

Er wordt aan gewerkt. Ik heb geen oude rapport kunnen achterhalen, vandaar dat ik een verzoek heb ingediend voor een nieuw rapport.

Groet,

art 5 1-2e art 5 1-2e

Functioneel Beheer iDMS

Afdeling I&A

M art 5 1-2e

E art 5 1-2e PZH.nl <mailto : art 5 1-2e PZH.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=04%7C01% art 5 1-2e art 5 1-2e %40pzh.nl
%7Cd184984906cd4388a0fa08d8e3beacd2%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C637509755366466442%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=nhy2Uh%2FCw8sqYPnbEdrT0er5NJHCjUrbuHIFY4ZaqCQ%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

(09.00-14.00)

Elke dag beter. Zuid-Holland.
"


provincie
Zuid-Holland

provincie ZUID-HOLLAND

Gedeputeerde Staten

Postadres Provinciehuis
Postbus 90602
2509 LP Den Haag
T 070 - 441 66 11
www.zuid-holland.nl

Datum
24-9-2019

Mandaatnummer
-
Ons kenmerk
DOS-2018-0006727

Bijlagen
-

«naam»

Onderwerp
Melding datalek

Geachte heer/mevrouw,

O
nlangs is een datalek geconstateerd in één van onze systemen. Door dit lek zijn persoonlijke gegevens van u tijdelijk onvoldoende beschermd geweest. Met deze brief informeer ik u graag verder.

Melding datalek
Sinds vorig jaar mei is de Algemene Verordening Gegevensbescherming (AVG) van kracht. Deze verordening voorziet in een versterking van de privacyrechten en bescherming van persoonsgegevens. We hebben naar aanleiding van deze verordening onder meer een functionaris voor gegevensbescherming aangesteld en het toezicht op de verwerking van persoonsgegevens verder aangescherpt. Doordat wij onze bestaande werkwijzen en processen nu meer dan vroeger kritisch tegen het licht houden komen zwakke plekken sneller in beeld en kunnen we snel gepaste maatregelen nemen. Dat is ook nu het geval. Een alerte medewerker heeft op 11 september opgemerkt dat hij meer gegevens kon inzien dan hij nodig heeft voor het uitoefenen van zijn functie en heeft daar melding van gemaakt.

Toelichting aard en omvang
Voor het aanmelden van nieuwe statenleden en fractiemedewerkers maakt de provincie gebruik van een IT-systeem. Hierin worden de persoonsgegevens geregistreerd die u de provincie heeft verstrekt met oog op de salarisverwerking en het verstrekken van toegangspassen en IT-middelen. Dit gebeurt door daartoe aangewezen medewerkers van ondersteunende afdelingen. Een van deze medewerkers wees er op dat hij in dit IT-systeem meer van uw persoonsgegevens kon inzien dan strikt noodzakelijk voor de uitvoering van zijn taak. Daarnaast is na onderzoek gebleken dat een andere groep behandelaren (406 personen) – zij het met wat meer moeite – deze persoonsgegevens ook zou kunnen inzien. We hebben geen aanwijzing dat dit daadwerkelijk is gebeurd, maar kunnen dit helaas niet uitsluiten. Bovenstaand proces betreft alleen de incidentele tussentijdse personele wijzigingen en niet de aanmelding van meerdere personen bij de installatie van PS na de verkiezingen.

Bezoekadres
Zuid-Hollandplein 1
2596 AW Den Haag

Tram 9 en de buslijnen 90, 385 en 386 stoppen dichtbij het provinciehuis. Vanaf station Den Haag CS is het tien minuten lopen. De parkeerruimte voor auto's is beperkt.

v

provincie ZUID HOLLAND

Afhandeling en maatregelen
Na constatering zijn uw persoonsgegevens uit het bewuste systeem verwijderd en de werkwijze is direct aangepast, zodat dit niet opnieuw kan gebeuren. De functionaris voor gegevensbescherming, de concerndirectie en Gedeputeerde Staten zijn op de hoogte gesteld. Er is ook een officiële melding gedaan bij de Autoriteit Persoonsgegevens.

Wat betekent dit voor u?
Ik begrijp het als u zich mogelijk zorgen maakt over dit datalek. Het betreft immers uw persoonlijke gegevens. Echter: het feit dat de *mogelijkheid* bestond om uw gegevens in te zien, wil niet zeggen dat dit ook daadwerkelijk is gebeurd, laat staan dat er misbruik van is gemaakt. Helaas hebben we in dit geval niet kunnen uitsluiten dat te veel provinciale medewerkers mogelijk uw gegevens hebben kunnen inzien. Al onze collega's leggen een ambtseed af en wij verwachten integer gedrag van ze. Niettemin raden wij u aan om alert te zijn op signalen van identiteitsfraude of ander misbruik van uw persoonsgegevens. Daarom vind ik het van belang u dit bericht te sturen.

Vragen?
Ik kan me voorstellen dat er bij u nog vragen leven als het gaat om uw persoonlijke situatie. U kunt hiervoor contact opnemen met art 5 1-2e personeels- en salarisadministrateur via art 5 1-2e@pzh.nl of art 5 1-2e Ook is onze functionaris gegevensbescherming, de heer art 5 1-2e art 5 1-2e beschikbaar voor om uw vragen te beantwoorden. U kunt hem bereiken per e-mail via fg@pzh.nl of telefonisch op art 5 1-2e

Hoogachtend,

art 5 1-2e

provincie ZUID-HOLLAND

Concerndirecteur

art 5 1-2e

Contact
privacy@pzh.nl
Postadres provinciehuis
Postbus 90602
2509 LP Den Haag
T 070 - 441 66 11
www.zuid-holland.nl

Datum
Zie verzenddatum linksonder
Ons kenmerk

Uw kenmerk

Bijlagen

art 5 1-2e

Onderwerp
Informatie over datalek

Geachte art 5 1-2e

W
ij hebben u per brief van 22 juli jl. geïnformeerd dat de provincie Zuid-Holland aangifte tegen u gaat doen, omdat u na opheffing van uw bedrijf een subsidieaanvraag heeft ingediend bij de provincie Zuid-Holland. In die brief schreven wij ook dat wij de gemeente Gorinchem en de gemeente Halderberge zouden adviseren ook aangifte tegen u te doen, onder meer omdat u het briefpapier van die gemeenten gebruikt heeft.

Uit intern juridisch onderzoek bleek dat wij uit privacy oogpunt uw persoonsgegevens niet aan die gemeenten mochten verstrekken. Op grond van artikel 34 AVG informeren wij u over deze gang van zaken. Wij zien dit als een datalek en hebben dit ook volgens artikel 33 AVG gemeld aan de Autoriteit Persoonsgegevens.

Wij bieden u onze excuses aan voor de gemaakte vergissing.

Hoogachtend,

art 5 1-2e

Deze brief is digitaal vastgesteld, hierdoor staat er geen fysieke handtekening in de brief.

Bezoekadres
Zuid-Hollandplein 1
2596 AW Den Haag

Tram 9 en de buslijnen 90, 385 en 386 stoppen dichtbij het provinciehuis. Vanaf station Den Haag CS is het tien minuten lopen. De parkeerruimte voor auto's is beperkt.

provincie Zuid-Holland

GEGEVENSBESCHERMING EN (WET) MELDPLICHT DATALEKKEN

Input	Proces	Output	Verantwoordelijke en toelichting
Data-verwerkingen	**1. Beheren register van verwerkingen**	Register van verwerkingen	**1. Data verantwoordelijke:** ○ Bepaald aanwezige gegevensbewerking waarvoor we als organisatie verantwoordelijke zijn; ○ Stelt wanneer vereist een register van verwerkingen op (conform de geldende wet- en regelgeving); ○ Overweegt/kan aantonen bij deze gegevensverwerking: • De bekendheid van deze gegevensverwerking bij c.q. toestemming door de betrokkene; • De bepaalde en gerechtvaardigde doeleinden voor verzameling van deze gegevens.
Register van verwerkingen	**2. Beheren risico-management**	Risico-management DPIA	**2. Data verantwoordelijke:** ○ Werkt risicomanagement uit n.a.v. het register van verwerkingen; ○ Voert passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking en neemt deze op in het uitgewerkte risicomanagement; ○ Voert een DPIA uit wanneer dit vereist is.
Register van verwerkingen	**3. Invullen bewustwording en verwerkers-overeen-komsten**	Verwerkers-overeenkomst Bewustwording	**3. Data verantwoordelijke / IT-manager:** ○ Zorgt voor AVG-bewustwording bij de medewerkers; ○ Ziet toe, bij betrokkenheid van een verwerker, op de naleving van de maatregelen bij de verwerker; ○ Legt dit vast in een contract / verwerkersovereenkomst.
Verzoek betrokkene	**4. Reageren op verzoek**	Reactie en registratie	**4. Data verantwoordelijke / organisatie:** ○ Reageert, uiterlijk binnen 1 maand, op een verzoek van een betrokkene; ○ Volgt het verzoek op of geeft motivatie van de weigering en wijst betrokkene op zijn/haar klachtrecht.
Melding beveiligings-issue	**5. Melden datalek**	Registratie van incidenten Informeren betrokkenen Melden AP	**5. Data verantwoordelijke:** ○ Documenteert alle inbreuken, dus ook niet-meldingsplichtige; ○ Stelt de AP of verwerkersverantwoordelijke onverwijld (zo mogelijk binnen 72uur) in kennis van een datalek “tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen” (AVG art. 33 lid1)*; ○ Meldt een succesvolle mailware aanval altijd; ○ Stelt de betrokkene onverwijld in kennis indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer; ○ Registreert bij deze beveiligingsincidenten en datalekken de omstandigheden van het incident en bewaart deze gedurende een periode van 3 jaar; ○ Volgt communicatie met AP en betrokkene op.
Register van verwerkingen en risico-management Melding beveiligings-issue	**6. Opvolgen en verbeteren**	Registratie van incidenten Management review	**6. Directie / data verantwoordelijke:** ○ Heroverweegt risicomanagement en voert maatregelen door; ○ Beoordeelt periodiek de actualiteit van de van toepassing zijnde wet- en regelgeving en bijbehorende implementatie; ○ Neemt wat nodig op in de management review.

** Beoordeel een groter datalek altijd middels de officiële AVG wettekst en relevante jurisprudentie.*

N.B. Dit proces heeft betrekking op de AVG (Europese GDPR) en de wet meldplicht datalekken.

Van: art 5 1-2e
Verzonden: 2023-10-03 17:57:31+00:00
Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: concept advies aan art 5 1-2e omtrent melden aan AP en melden aan betrokkenen
"
Dag art 5 1-2e en art 5 1-2e

Het was een worsteling om er een beetje een verhaal van te maken op zo korte termijn.

Mijn conclusie is in elk geval om wel in één keer te melden aan de AP, maar voorlopig nog niet te melden aan betrokkenen. Daarvoor heb ik een juridische onderbouwing gevonden die wel moet worden afgestemd met en goedgekeurd door de AP.

Ik hoop dat jullie nog tijd vinden om ernaar te kijken voordat ik het naar art 5 1-2e stuur. Mijn deadline voor he versturen heb ik op 22.00 uur vanavond gezet .

Met vriendelijke groet,

art 5 1-2e art 5 1-2e

Functionaris voor Gegevensbescherming

Gerechtelijk Deskundige

M art 5 1-2e

E art 5 1-2e pzh.nl

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7art 5 1-2e art 5 1-2e 40pzh.nl%7Cf5e9200e148548126f4708dbc42973de%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638319454677185451%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=mSIQhcJVY12zO7aXcadsLT0k7QcENnRnVuD7ObJ5kZ0%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Krachtig Zuid-Holland.
"

Advies aan concerndirecteur omtrent melding datalek aan AP en betrokkenen

Vraagstelling
In dit memo wordt getracht een antwoord te geven op de vraag van de concerndirecteur wat wijsheid is ten aanzien van het melden van de verschillende geconstateerde datalekken aan de Autoriteit Persoonsgegevens. Dit advies is met name juridisch ingestoken, een bestuurlijke afweging zal gemaakt moeten worden door het DT.

Er zijn meerdere datalekken geconstateerd in iDMS. Eén datalek, met drie zoektermen, is aan de Autoriteit Persoonsgegevens (AP) gemeld op 8 september 2023. Daarnaast zijn er meerdere inbreuken geconstateerd zowel met handmatige acties door de FG en de Eenheid Privacy als bij geautomatiseerde zoekslagen door de functioneel beheerders van iDMS in samenwerking met het BI-team van I&A.
De vraag die voorligt is of deze datalekken separaat gemeld moeten worden aan de AP of dat dit in één 'container'-melding kan worden gevangen.

Advies FG
Advies FG omtrent melden AP: Gelet op het onderstaande juridische kaders (ook gelezen in samenhang met hetgeen in het laatste overleg in de stuurgroep is besproken) is de FG van mening dat er geen valide grondslag is en geen gegronde redenen zijn om de geconstateerde overtredingen van de AVG niet komende donderdag in één keer te melden aan de AP.

Advies FG omtrent melden aan betrokkenen: de uitleg in de overweging 86 AVG[1] geeft PZH enige ruimte om de melding aan betrokkenen mogelijk op een later tijdstip te informeren. Hierover dient wel op zeer korte termijn contact te worden opgenomen met de AP. Contactpersoon voor de AP is bij wet geregeld, zijnde de FG van PZH.

Situatiebeschrijving
Op 7 september jl. ontvingen de FG en de eenheid Privacy (EP) van PZH een melding van de CISO dat hij waarschijnlijk ongeoorloofd toegang heeft gehad tot persoonsgegevens in het IDMS. De CISO had middels de zoektermen "curriculum vitae", "kopie paspoort" en "Bibob" toegang tot documenten waar hij uit hoofde van zijn functie geen toegang toe behoeft.

[1] (86) De verwerkingsverantwoordelijke moet de betrokkene zonder onredelijke vertraging in kennis stellen van de inbreuk in verband met persoonsgegevens wanneer die inbreuk in verband met persoonsgegevens grote risico's voor de rechten en vrijheden van de natuurlijke persoon met zich kan brengen, zodat hij de nodige voorzorgsmaatregelen kan treffen.

De kennisgeving dient zowel de aard van de inbreuk in verband met persoonsgegevens te vermelden als aanbevelingen over hoe de natuurlijke persoon in kwestie mogelijke negatieve gevolgen kan beperken.

Dergelijke kennisgevingen aan betrokkenen dienen zo snel als redelijkerwijs mogelijk te worden gedaan, in nauwe samenwerking met de toezichthoudende autoriteit en met inachtneming van de door haarzelf of door andere relevante autoriteiten, zoals rechtshandhavingsautoriteiten, aangereikte richtsnoeren.

Zo zouden betrokkenen bijvoorbeeld onverwijld in kennis moeten worden gesteld wanneer een onmiddellijk risico op schade moet worden beperkt, terwijl een langere kennisgevingstermijn gerechtvaardigd kan zijn wanneer er passende maatregelen moeten worden genomen tegen aanhoudende of soortgelijke inbreuken in verband met persoonsgegevens.

De FG heeft de concerndirecteur per brief van 21 september jl. geïnformeerd over de resultaten van een onderzoek dat hij heeft laten doen naar de toegankelijkheid van persoonsgegevens en bijzondere persoonsgegevens voor medewerkers die deze gegevens niet nodig hebben voor de uitoefening van hun functie. Uit dit onderzoek bleek dat er naar alle waarschijnlijkheid een groot aantal documenten toegankelijk is voor onbevoegde medewerkers.

Juridisch kader melden aan betrokkenen
Melden aan betrokkenen
Artikel 34 AVG: Mededeling van een inbreuk in verband met de persoonsgegevens aan de betrokkene
lid 1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkenen de inbreuk in verband met persoonsgegevens onverwijld mee.
a. inbreuk in verband met persoonsgegevens: de AVG kent de term datalek niet, de juiste juridische terminologie hiervoor is inbreuk in verband met persoonsgegevens;
b. hoog risico: in het datalek van 7 september zijn een groot aantal identiteitsbewijzen naar boven gekomen, waaronder paspoorten, maar ook creditcardgegevens. Identiteitsbewijzen worden gezien als een hoog risico, gelet op de mogelijkheden om hiermee identiteitsfraude te plegen;
c. onverwijld: de melding moet onverwijld, althans zonder onnodige vertraging, worden gedaan, dat wil zeggen: zo snel als redelijk mogelijk. Zo zouden betrokkenen bijvoorbeeld onverwijld in kennis moeten worden gesteld wanneer een onmiddellijk risico op schade moet worden beperkt, terwijl een langere kennisgevingstermijn gerechtvaardigd kan zijn wanneer passende maatregelen moeten worden genomen tegen aanhoudende of soortgelijke inbreuken in verband met persoonsgegevens)….
Dergelijke kennisgevingen aan betrokkenen dienen zo snel als redelijkerwijs mogelijk te worden gedaan, in nauwe samenwerking met de toezichthoudende autoriteit…(overweging 86 AVG

Juridisch kader melden aan AP
Artikel 33 AVG: Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit
lid 1. Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.
……..
5. De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

Definitie datalek:
Artikel 4 AVG: Definities
12) „inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
De hierboven beschreven scenario's zien met name op de ongeoorloofde verstrekking of ongeoorloofde toegang tot (n de oorspronkelijke wettekst unauthorised disclosure of, or access to) persoonsgegevens.

De European Data Protection Board, het overkoepelend orgaan van alle nationale Europes toezichthouders, heeft een Richtlijn uitgebracht waarin nadere uitleg wordt verstrekt over het begrip datalek[2]. Helaas is er nog geen Nederlandse vertaling beschikbaar, dus ik beperk mij tot de originele tekst.
Hoofdstuk II onder A sub 62 t/m 64:
3. Delayed notifications
62. Article 33(1) GDPR makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This, along with the concept of notification in phases, recognises that a controller may not always be able to notify a breach within that time period, and that a delayed notification may be permissible.

63. Such a scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to establish the extent of the breaches and, rather
than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches.

64. Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a "bundled" notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time. If a series of breaches take place that concern different types of personal data, breached in different ways, then notification should proceed in the normal way, with each breach being reported in accordance with Article 33.

Onder 62 wordt aangegeven dat er omstandigheden kunnen zijn dat een datalekmelding niet binnen 72 uur wordt gedaan en dat dit toelaatbaar kan zijn. Bijvoorbeeld in het geval dat er meerdere, vergelijkbare datalekken zijn binnen een korte tijdspanne waarbij de rechten en vrijheden van veel betrokkenen aan de orde zijn (zie 63).
Normaliter dient ieder datalek separaat gemeld te worden, maar om de belasting voor de verwerkingsverantwoordelijke (PZH) en de toezichthouder (AP) niet onnodig groot te laten zijn, mag gekozen worden voor het gebundeld aanbieden van een datalekmelding (64).

[2] Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, Adopted 28 March 2023


provincie
Zuid-Holland

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Definitief

Melding gegevens

Naam melder	:	art 5 1-2e (FG), namens art 5 1-2e (concerndirecteur)
Registratienummer van het incident	:	M20 07 01126
Datum en tijdstip van de melding	:	Maandag 13 juli 2020 13:20
Route van de melding	:	Digitale Loket

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Dinsdag 28 juli 2020 13:00
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e jurist), art 5 1-2e (privacy officier), art 5 1-2e (adviseur informatieveiligheid)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerkers

Situatie

Melding is als onderstaand binnengekomen:

art 5 1-2e 13 juli 2020 13:18

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan

- Namens de concerndirecteur meld ik een datalek in iDMS. De toegang tot zeer geheime documenten in iDMS is toegankelijk voor een veel te grote groep beheerders (in dit geval van het team Bibob en de FG). Daarnaast is de logging van deze groep niet op voldoende niveau geregeld.

Let wel: in het kader van het onderzoek mag NIET worden gekeken in de mappen van het team Bibob of de FG!

Wat voor soort incident heeft er plaats gevonden?
- Iemand kan bestanden inzien zonder de juiste rechten

Wanneer vond de inbreuk plaats? Indien bekend
-

Wanneer vond de inbreuk plaats? Indien niet bekend
- sinds 25 mei 2018

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Er is geen sprake van een datalek.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Er is geen sprake van een datalek.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Er is geen sprake van een datalek.

Vraag	Antwoord
Welke persoonsgegevens betreft het?	Er is geen sprake van een datalek.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Er is geen sprake van een datalek.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Er is geen sprake van een datalek.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Er is geen sprake van een datalek.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Er is geen sprake van een datalek.
Betreft het een datalek?	Er is geen sprake van een datalek. .
Ondernomen beperkende maatregelen.	Er is geen sprake van een datalek.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Er is geen sprake van een datalek.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

Maandag 20 juli heeft een gesprek met betrokkenen plaats gevonden waarbij de aanleiding van het datalek als onderstaand is besproken:

Aanleiding voor het melden van een datalek is de onrust bij het Bibob-team over de toegang tot hun vertrouwelijke iDMS-mappen en in het bijzonder de mappen over C-quential. art 5 1-2e (coördinator Bibob) is, op maandag 20 juli, voorzien van informatie over het verkrijgen van inzicht in wie, welke documenten heeft geraadpleegd. Uit een eerste controle, onder mijn toezicht, is gebleken dat er geen sprak is van onbevoegde toegang of onjuist rechtenstructuur. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. In dit specifieke geval is er geen sprake van een beveiligingsincident of datalek. Er is geen aanwijzing dat er persoonsgegevens verloren zijn gegaan of dat er “onrechtmatige verwerking” van persoonsgegevens heeft plaats gevonden. Indien uit een tweede controleslag (uitvoering door art 5 1-2e toch blijkt dat er onbevoegd toegang is verkregen tot de mappen van Bibob dan neemt art 5 1-2e ontact op met FG en team informatieveiligheid.

Verder is gebleken uit de audittrial dat enkel bevoegde beheerders toegang hebben verkregen tot de mappen van het Bibob-team (ter uitvoering van hun werkzaamheden). Binnen het team van beheerders zijn dan ook onderling afspraken gemaakt over de beheertaken met betrekking tot de mappenstructuur van het Bibob-team. De stelling dat bestand bekeken kunnen worden zonder de juiste rechten is niet aan de orde. Het functioneel beheer wordt uitgevoerd as designed. Er is geen sprake dat er ongeautoriseerd personeel toegang heeft tot persoonsgegevens.

Omdat er behoefte is aan extra beveiligingsmaatregelen heeft art 5 1-2e art 5 1-2e (beheer iDMS) aangeboden om verdere uitleg te geven over de technische beveiligingsmogelijkheden van iDMS. art 5 1-2e krijgt een beheerdersrol toegewezen, zodat zij o.a. zelf de toegangsrechten kan aanmaken en intrekken. art 5 1-2e en art 5 1-2e stemmen verdere procedurele- en technische maatregelen met elkaar af.

Conclusie en advies

Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. In dit geval is er geen sprake van een datalek.

art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 16 september 2022 09:23
Aan: art 5 1-2e
Onderwerp: RE: Datalek - Advies niet melden, alleen registreren

Ja, ik zal alles in de bijbehorende map in iDMS zetten.

Met vriendelijke groet,

art 5 1-2e
Privacy Officer

provincie Zuid-Holland

M art 5 1-2e
E art 5 1-2e @pzh.nl
www.zuid-holland.nl/contact

Werkdagen: ma, di, wo, do

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e @p zh.nl>
Verzonden: vrijdag 16 september 2022 09:08
Aan: art 5 1-2e < art 5 1-2e @pzh.nl>
Onderwerp: FW: Datalek - Advies niet melden, alleen registreren

Archiveer jij de mails etc?

Met vriendelijke groet

art 5 1-2e
Privacy jurist / Plaatsvervangend Functionaris voor Gegevensbescherming
Eenheid Privacy

provincie Zuid-Holland

M art 5 1-2e
E art 5 1-2e @pzh.nl
www.zuid-holland.nl/contact

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e @p zh.nl>
Verzonden: vrijdag 16 september 2022 09:07
Aan: art 5 1-2e < art 5 1-2e @pzh.nl>
CC: Willy de Zoete - van der Hout <wh.de.zoete@pzh.nl>; art 5 1-2e < art 5 1-2e @ pzh.nl>
Onderwerp: FW: Datalek - Advies niet melden, alleen registreren

Ha art 5 1-2e, ik volg je advies! Hartelijke groet, art 5 1-2e

---

Van: art 5 1-2e < art 5 1-2e @p zh.nl>
Verzonden: vrijdag 16 september 2022 08:37
Aan: art 5 1-2e < art 5 1-2e @p zh.nl>
CC: Willy de Zoete - van der Hout <wh.de.zoete@pzh.nl>; privacy <privacy@pzh.nl>; art 5 1-2e < art 5 1-2e @ pzh.nl>
Onderwerp: Datalek - Advies niet melden, alleen registreren

Beste art 5 1-2e;

Er is een datalek opgetreden. Er is per abuis een e-mail verstuurd met de geadresseerden in de CC in plaats van de BCC. De eenheid Privacy adviseert geen melding te doen bij de AP en het datalek alleen intern te registreren. Graag hoor ik of jij het advies opvolgt.

Met vriendelijke groet

art 5 1-2e
Privacy jurist / Plaatsvervangend Functionaris voor Gegevensbescherming
Eenheid Privacy

provincie Zuid-Holland

M art 5 1-2e
E art 5 1-2e @pzh.nl
www.zuid-holland.nl/contact

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e
Verzonden: 2023-09-24 22:18:39+00:00
Aan: art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e
CC: art 5 1-2e
Onderwerp: Data IDMS
"

Beste collega's,

Ter nadere onderbouwing van de constatering dat er een hoop gevoelige en bijzondere persoonsgegevens in IDMS vrij toegankelijk zijn, hebben wij (art 5 1-2een ik) aanvullend onderstaande zoektermen ingevoerd in IDMS met het account van ondergetekende. Voor zover ik weet, wijkt dat account niet af van een 'normaal' account. Onder iedere zoekterm hebben we een voorbeeld van een (ongewenst) zoekresultaat geplaatst.

Handtekening

https://idms/otcs/llisapi.dll?func=ll&objId=804540185&objAction=Open&nexturl=
%2Fotcs%2Fllisapi%2Edll%3Ffunc%3Dsrch%2ESearchCache%26cacheId
%3D1939548641&logStopConditionID=28987295_278994874_10_open

Bankpas

https://idms/otcs/llisapi.dll/fetch/
2000/16705/347675070/347679572/347684675/369679035/233780030/611086818/764457500
/789913495/-/scan_bankpas_S000148917_139609.pdf?nodeid=789913698&vernum=-2

Bezetting

https://idms/otcs/llisapi.dll?func=ll&objId=825742447&objAction=Open&nexturl=
%2Fotcs%2Fllisapi%2Edll%3Ffunc%3Dsrch%2ESearchCache%26cacheId
%3D1399122062&logStopConditionID=28970442_2009189331_1_open

Creditcard

https://idms/otcs/llisapi.dll/fetch/
2000/16719/16723/31212814/698284027/718540302/730673030/737522835/737530919/7375
38619/764021527/769988633/-/De_Zoete_2020-12_Creditcard_kosten_2020-06_
%28F005102249%29.pdf?nodeid=770256912&vernum=-2
<https://idms/otcs/llisapi.dll/fetch/2000/16719/16723/31212814/698284027/7185403
02/730673030/737522835/737530919/737538619/764021527/769988633/-/De_Zoete_2020-
12_Creditcard_kosten_2020-06_%28F005102249%29.pdf?nodeid=770256912&vernum=-2>

Invalidenkaart

https://idms/otcs/llisapi.dll?func=otemail.ViewAttachments&objid=579193112

Ziek

https://idms/otcs/llisapi.dll/fetch/
2000/16719/16722/180917029/180924809/180917865/180980408/792224067/-/
Medewerkers_ziek.pdf?nodeid=792216227&vernum=-2

Ziekte

https://idms/otcs/llisapi.dll/fetch/
2000/16734/489118871/554342254/583906598/584481070/569766334/-/Ziekte_-
_duur_per_medewerker_01-10-15_tm_30-09-16_pdf.pdf?nodeid=569764832&vernum=-2

Immateriele

https://idms/otcs/llisapi.dll?func=ll&objId=644745522&objAction=browse

VOG

https://idms/otcs/llisapi.dll?func=ll&objId=289606151&objAction=Open&nexturl=
%2Fotcs%2Fllisapi%2Edll%3Ffunc%3Dsrch%2ESearchCache%26cacheId
%3D1328404247&logStopConditionID=28987264_369646525_9_open

Vonnis

https://idms/otcs/llisapi.dll/fetch/
2000/16719/474855/163745404/164402687/813070870/286789640/-/2017-09-
28_Vonnis_rechtbank_inzake_SP_raadslid_Noordoostpolder_van_Ministerie_van_Binnen
landse_Zaken_en_Koninkrijksrelaties_%28AV00204022%29.pdf?
nodeid=614509817&vernum=-2

Wij vermoeden dat er bij een nieuwe query met bovengenoemde en andere zoektermen nog een groot aantal datalekken naar boven komt. Deze email dient louter ter illustratie dat de query die nu is/wordt uitgevoerd nog niet representatief is en de omvang van het probleem nog niet duidelijk is. Hetgeen complicerend is, is dat er bij een handmatige zoektocht zoals door ons is uitgevoerd een hoop ‘bijvangst’ in de zin van beleidsstukken wordt gevonden. Wij stellen voor om op korte termijn met het BI-team in overleg te gaan om tot een juiste en voor zover mogelijk zo volledig mogelijke query te komen.

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e
%40pzh.nl
%7C9808d2c0f8634a278c3108dbbd3b70b7%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638311835217558718%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=8wowp3r6NWrfpMBk3Ynpn%2FZlD8dXofZJPCru1%2FtIDYQ
%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

"


provincie
Zuid-Holland

Melden datalek

Aanmelder

Naam	art 5 1-2e
Telefoonnummer	
E-mail	art 5 1-2e @pzh.nl
Organisatie-eenheid	Kenniscluster Integrale Projectbeheersing-APP
Kostenplaatscode	354

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Mijn persoonlijke gegevens (privé-nummer en mailadres) staan vindbaar in iDMS. Dit hoort hier niet opgeslagen te zijn.
Wat voor soort incident heeft er plaats gevonden?	Anders
Anders? Graag toelichten	Er zijn privégegevens opgeslagen in een openbare database
Wanneer vond de inbreuk plaats? Indien bekend	1 mei 2023 12:00
Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☐

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☑
Telefoonnummers	☐

E-mailadressen of andere adressen voor digitale communicatie	☑
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☐
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	werknemer, mijzelf
Schatting van het aantal personen betrokken bij het datalek: minimaal	1
Schatting van het aantal personen betrokken bij het datalek: maximaal	onbekend

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art 5 1-2e
Telefoonnummer	
E-mail	art 5 1-2e @pzh.nl
Organisatie-eenheid	Bureau Mobiliteit en Milieu III
Kostenplaatscode	136

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	350330057252576
Bij een smartphone van de PZH. Wat is het 06 nummer?	art 5 1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	241123 rond 19.30-21.00 Utrecht Beatrix theater of buiten daarvoor
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Nee
Zijn de gegevens versleuteld?	Nee
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	zie bovenstaande situatie, ik had een verrassingsuitje met mn dochter en kwam er ineens achter dat ik mn telefoon niet meer had, hij zat in mn tasje

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art 5 1-2e
Telefoonnummer	art 5 1-2e
E-mail	art 5 1-2e @pzh.nl
Organisatie-eenheid	Afdeling Samenleving en Economie
Kostenplaatscode	393

Benodigde gegevens

Is dit een diefstal of vermissing?	Diefstal
Is er al aangifte gedaan?	Ja
Gelieve de aangifte te uploaden:	
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Laptop
Bij een apparaat van de PZH. Wat is het CI nummer?	HDZY2
Bij een smartphone van de PZH. Wat is het 06 nummer?	
Locatie, datum en tijdstip van vermissing, indien bekend?	Hilton hotel garage zeestraat tussen 18 - 21.35 uur.
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja

Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Nee
Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Onbekend
Zijn de gegevens versleuteld?	Ja
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Ja
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Achterruit van auto ingeslagen en laptop van verborgen plek uit kofferbak gehaald. Er zijn foto's van mijn terugkomst. Politie nog verzekeringsmaatschappij willen de beelden opvragen.

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art 5 1-2e
Telefoonnummer	
E-mail	art 5 1-2e @pzh.nl
Organisatie-eenheid	Bureau Infrastructuur en Support
Kostenplaatscode	279

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH. Wat is het 06 nummer?	
Locatie, datum en tijdstip van vermissing, indien bekend?	27-10-2022
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Onbekend
Zijn de gegevens versleuteld?	Ja
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Vanochtend was de telefoon niet in mijn tas meer.

art 5 1-2e

Van: Politie <noreply@politie.nl>
Verzonden: maandag 21 augustus 2023 17:27
Aan: art 5 1-2e
Onderwerp: Uw aangifte bij de politie art 5 1-2e

Geachte art 5 1-2e

U heeft aangifte gedaan via internet. Bedankt voor uw aangifte.

Het voorlopige nummer van uw aangifte is art 5 1-2e Als de aangifte administratief verwerkt is krijgt deze een definitief nummer. Hiervan ontvangt u bericht.

Op Mijn Politie kunt u zien hoe het ervoor staat met uw aangifte. Hiervoor moet u inloggen met uw DigiD.

Met vriendelijke groet,

Politie

« waakzaam en dienstbaar »

Deze e-mail is automatisch gemaakt. Daarom kunt u deze e-mail niet beantwoorden.

Van: art 5 1-2e
Verzonden: 2022-08-03 11:55:02.820000+00:00
Aan: art 5 1-2e
CC: art 5 1-2e Willy de Zoete - van der Hout
Onderwerp: Datalek dat gemeld moet worden bij AP en betrokkene
"
Beste art 5 1-2e

Bijgaand het advies om een datalek te melden bij de AP en betrokkene. Als jij het daarmee eens bent, informeer ik het bureauhoofd Subsidies en stel ik in samenspraak met de afdeling Communicatie een bericht op voor betrokkene. Als je meer informatie over deze casus wilt, kan ik je die uiteraard verstrekken.

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <http://www.zuid-holland.nl/contact>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e (bureau subsidies)
Registratienummer van het incident	:	(M22 07 02449)
Datum en tijdstip van de melding	:	28 juli 2022 11:43 (ontvangst melding)
Route van de melding	:	Datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e en art 5 1-2e
Datum en tijdstip advies	:	3 augustus 2022 om 11:49 uur
Advies besproken met	:	art 5 1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Eenheid privacy

Situatie

Het betreft hier een incident waarbij een brief waarin de provincie mededeelt aan een burger aangifte te doen van strafbare feiten aan twee gemeenten is verstrekt. De naam van de burger is daarbij ook aan de gemeenten verstrekt. Er is daarnaast ook telefonisch bij de gemeenten geïnformeerd of zij ook aangifte wilden doen jegens deze persoon vanwege het gebruik in privé van briefpapier van de gemeenten,

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Eén. De naam van een burger
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend. Ambtenaren bij de gemeente Halderberge en gemeente Gorinchem.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Persoonsgegevens zijn ingezien door onbevoegden.
Welke persoonsgegevens betreft het?	De naam van een burger
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.

Vraag	Antwoord
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Nee. Ambtenaren bij de gemeente Halderberge en gemeente Gorinchem konden een naam van een burger lezen op een bijlage.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	ja, het betreft een aankondiging dat de provincie aangifte doet vanwege strafbare feiten bij de politie jegens deze persoon. Aangezien deze persoon werkzaam is geweest bij die gemeenten is hij geïdentificeerd door die gemeenten.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Nee.
Betreft het een datalek?	Ja.
Ondernomen beperkende maatregelen.	De beide gemeente zijn ingelicht. Verzocht is om de betreffende bijlage te wissen/vernietigen.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Collega's bij bureau subsidies worden geïnstrueerd over de AVG en het beperken van het delen van namen van burgers aan collega overheden.

Afweging

<u>Toelichting op het wettelijke kader *(standaard tekst)*</u>

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt?
  Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.

[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu?
  Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

Het betreft hier een incident waarbij een brief waarin de provincie mededeelt aan een burger aangifte te doen van strafbare feiten aan twee gemeenten is verstrekt. De naam van de burger is daarbij ook aan de gemeenten verstrekt. Er is daarnaast ook telefonisch bij de gemeenten geïnformeerd of zij aangifte wilden doen jegens deze persoon vanwege het gebruik in privé van briefpapier van de gemeenten, Er is derhalve sprake van een hoog risico voor betrokkene. Er bestond voor de provincie geen wettelijke grondslag om deze informatie met de gemeente te delen. Bovendien kunnen er naar de opinie van de eenheid Privacy vraagtekens gezet worden bij de stelling van de provincie dat deze persoon een strafbaar feit jegens die gemeenten heeft gepleegd. Betrokkene dient daarom geïnformeerd te worden over dit datalek.

Het betreft hier een datalek dat gemeld dient te worden aan de Autoriteit Persoonsgegevens.

Conclusie en advies

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt WEL gemeld bij de Autoriteit Persoonsgegevens en betrokkene.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.


provincie
Zuid-Holland

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e
Registratienummer van het incident	:	M23 09 00678
Datum en tijdstip van de melding	:	5 september 2023 16:55
Route van de melding	:	Digitale Loket op Binnenplein

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	7 september 2023 11:33
Advies besproken met	:	Besproken met art 5 1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Gedeeld met eenheid Privacy

Situatie

Op 5 september 2023 om 16:55 kwam bij art 5 1-2e via de mail een melding binnen van art 5 1-2e art 5 1-2emet de vraag of het zichtbaar zijn van het BSN in de applicatie Easyfunders een datalek betreft. art 5 1-2e n ad deze vraag ontvangen van art 5 1-2e s enior subsidieadviseur.

Na een mailwisseling heeft art 5 1-2e p 6 september om 15:23 officieel melding gemaakt van een mogelijk datalek in Easyfunders via het TopDesk datalek-formulier.

art 5 1-2e g eeft aan dat hij in zijn rol als senior subsidieadviseur het BSN op de initiële pagina's in Easyfunders enkel ziet in de vorm van de laatste 3 cijfers. Als hij echter doorklikt naar de volgende pagina is het volledige BSN zichtbaar.

art 5 1-2e g eeft zelf aan dat de laatste 3 cijfers van het BSN volstaan in het uitoefenen van zijn functie. De Wet algemene bepalingen burgerservicenummer schrijft voor dat overheidsorganisaties het BSN mogen gebruiken als dat noodzakelijk is om hun publieke taak uit te voeren. Zoals art 5 1-2e a angeeft hebben hij en zijn collega's het volledige BSN niet nodig voor de uitoefening van hun functie.

art 5 1-2e P roject Manager bij Subsidies geeft in de mailwisseling aan dat de autorisatiematrix (veldrechten) van Easyfunders (welke zijn opgesteld en goedgekeurd door art 5 1-2e) laat zien dat het hoofd Subsidies en de rol Subsidieadviseur het BSN als enige mogen inzien. Andere rollen zijn afgeschermd. Of de rol van functioneel beheerder recht geeft op inzage in het BSN is niet duidelijk.

In de DPIA welke momenteel in uitvoering is, staat hierover echter het volgende:

Aanvullende maatregelen?	Het risico is gering. Als aanvullende maatregel is het BSN-nummer afgeschermd voor rollen in het systeem die dit nummer niet nodig hebben. Dit wordt al gedaan bij het binnenkomen van de aanvraag via de e-formulieren. Via de veldrechten autorisatie is de toegang tot de ingediende BSN heel erg beperkt tot alleen de beheerders. Verder zijn er geen aanvullende maatregelen nodig.

Dit komt niet overeen met de eerdergenoemde autorisatiematrix. Als het zichtbaar zijn van het BSN voor de bedrijfsvoering Subsidies voor Hoofd Subsidies en de rol subsidieadviseur nodig is, dan dient dit aangegeven en onderbouwd te worden in de DPIA.

Additioneel blijkt bij verdere navraag bij art 5 1-2e d e functioneel beheerders van Easyfunders, dat niet duidelijk kan worden aangegeven welke andere rollen mogelijk nog toegang hebben tot het zien van het volledige BSN.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Onduidelijk
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onduidelijk
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Mogelijk lezen, kopiëren, afdrukken, e-mailen,.
Welke persoonsgegevens betreft het?	BSN
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja, medewerkers van Subsidies
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee tgv geheimhoudingsverklaring
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja.
Betreft het een datalek?	Ja.

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
Ondernomen beperkende maatregelen.	De herinrichting van het systeem en het zorgen voor het gelijkstellen van de autorisatiematrix en de in de DPIA beschreven normen zal bij de verdere uitvoer van de DPIA worden meegenomen.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	N.v.t.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

art 5 1-2e s enior subsidieadviseur bij Subsidies, heeft de mogelijkheid om volledige BSN's te zien. Hij geeft echter aan dat de laatste 3 cijfers van het BSN volstaan in het uitoefenen van zijn functie. Zoals art 5 1-2e art 5 1-2e a angeeft hebben hij en zijn collega's het volledige BSN niet nodig voor de uitoefening van hun functie.

De autorisatiematrix (veldrechten) van Easyfunders zoals opgesteld door de medewerkers van Subsidies laat zien dat het hoofd Subsidies en de rol Subsidieadviseur het BSN als enige mogen inzien. Andere rollen zijn afgeschermd. Of de rol van functioneel beheerder recht geeft op inzage in het BSN is niet duidelijk. Deze autorisatiematrix komt niet overeen met de rechten zoals beschreven in de DPIA.

Conclusie en advies
De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt NIET gemeld bij de Autoriteit Persoonsgegevens en NIET aan betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.

Van: art 5 1-2e
Verzonden: 2023-09-28 11:49:53+00:00
Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: Datalek en Informatietransitie
"
Hoi art 5 1-2e en art 5 1-2e

Hier een eerste opzet.

Datalek Informatietransitie.docx
<https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?url=https%3A%2F%2Fpzh-my.sharepoint.com%2F%3Aw%3A%2Fr%2Fpersonal%2art 5 1-2e%2FDocuments%2FOneDrive%2520-%2520Provincie%2520Zuid-Holland_1%2F000%2520informatiebeheer%2F000%2520Record%2520management%2FMT-DI%2FDatalek%2520Informatietransitie%2FDatalek%2520Informatietransitie.docx%3Fd%3Dwf4621d6faca440c6be7ab14f%26csf%3D1%26web%3D1%26e%3DfheE4T&data=05%7C01%art 5 1-2e art 5 1-2e 40pzh.nl%7C509a745f3c984c55932c08dbc0084421%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638314913954503618%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=phT8zAIsAsEMMJt1Cj5PVZwv3bnPvAhnePQtmaqIJLI%3D&reserved=0>

Met vriendelijke groet,

art 5 1-2e

Strategisch adviseur Duurzaam Digitaal Informatiebeheer

P-team: Informatietransitie/ Kaders, Coaching en Advies

Domein: Informatisering & Automatisering

M art 5 1-2e

E art 5 1-2epzh.nl <mailto :art 5 1-2epzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%art 5 1-2e art 5 1-2e %40pzh.nl%7C509a745f3c984c55932c08dbc0084421%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638314913954503618%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=OduEeVoQKJ%2BKKvlx4jyJ1J6yq%2F%2FwkYvYmHaJQ3hOl1I%3D&reserved=0>

Werkdagen: ma, di, wo-ochtend, do, vr

Krachtig Zuid-Holland.


provincie
Zuid-Holland

Melden datalek

Aanmelder

Naam	art 5 1-2e
Telefoonnummer	
E-mail	art 5 1-2e ɔzh.nl
Organisatie-eenheid	Bureau Subsidies
Kostenplaatscode	413

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Ik ben subsidieverlener bij bureau Subsidies. Regelmatig hebben we te maken met frauduleuze subsidieaanvragen/ verleningen. Tijdens de behandeling van één van deze frauduleuze zaken heb ik per ongeluk een datalek veroorzaakt. Om inzichtelijk te maken hoe dit is gekomen beschrijf ik het voortraject. Er is aan een client in 2019 een MIT subsidie verleend. Omdat client niet tijdig een aanvraag tot vaststelling heeft ingediend zijn enkele bedrijfsgegevens via openbare bronnen gecontroleerd. Op basis van deze informatie is gebleken dat client op frauduleuze gronden subsidie heeft verkregen. Vervolgens is in overleg met juristen en leidinggevende de subsidie ambtshalve op nihil vastgesteld en trachten we via een vordering het reeds betaalde voorschot terug te vorderen. Dit is overigens inmiddels een ingebrekestelling geworden. Sinds de vordering is verzonden communiceert client met de provincie. Daarbij maakt client onder andere gebruik van briefpapier van de gemeente Gorinchem en de gemeente Halderberge. In overleg met leidinggevende is besloten om de gemeenten over het gebruik van hun briefpapier te informeren. Vorige week heb ik de gemeente Halderberge telefonisch geïnformeerd over het gebruik van hun briefpapier door client. De gemeente Halderberge was geïnteresseerd in een voorbeeld, deze heb ik gemaild. Tot mijn grote schrik kwam ik er later achter dat ik abusievelijk het adres van deze client niet heb verwijderd in het verzonden voorbeeld. Via een jurist heb ik gisteren vernomen dat ik hiermee een datalek hebt veroorzaakt. Ik ben enorm geschrokken door dit en heb dit vanmorgen direct gemeld bij mijn leidinggevende. Ik bied oprecht mijn verontschuldiging aan en hoop dat het niet tot problemen leidt. Overigens wordt na het zomerreces namens GS aangifte gedaan tegen deze client wegens fraude.
Wat voor soort incident heeft er plaats gevonden?	Anders
Anders? Graag toelichten	Mail gestuurd over een client naar de gemeente Halderberge waarbij de adresgegevens van client niet zijn verwijderd
Wanneer vond de inbreuk plaats? Indien bekend	26 juli 2022 11:38

Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☐

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☑
Telefoonnummers	☐
E-mailadressen of andere adressen voor digitale communicatie	☐
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☐

Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	persoonsgegevens van een burger
Schatting van het aantal personen betrokken bij het datalek: minimaal	1
Schatting van het aantal personen betrokken bij het datalek: maximaal	1

"Van: art 5 1-2e
Verzonden: 2020-07-30 13:02:17+00:00
"Aan: art 5 1-2e Zoete - van der Hout, WH, de"
"CC: art 5 1-2e
Onderwerp: Datalek iDMS
"

Beste art 5 1-2e Willy,

Naar aanleiding van een melding van een datalek in iDMS heb ik afgelopen 2 weken onderzoek verricht. Ik kom tot de conclusie dat hier geen sprake is van een datalek en wel om onderstaande redenen:

Aanleiding voor het melden van een datalek is de onrust bij het Bibob-team over de toegang tot hun vertrouwelijke iDMS-mappen en in het bijzonder de mappen over C-quential. art 5 1-2e (coördinator Bibob) is, op maandag 20 juli, voorzien van informatie over het verkrijgen van inzicht in wie, welke documenten heeft geraadpleegd. Uit een eerste controle, onder mijn toezicht, is gebleken dat er geen sprak is van onbevoegde toegang of onjuist rechtenstructuur. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. In dit specifieke geval is er geen sprake van een beveiligingsincident of datalek. Er is geen aanwijzing dat er persoonsgegevens verloren zijn gegaan of dat er “onrechtmatige verwerking” van persoonsgegevens heeft plaats gevonden. Indien uit een tweede controleslag (uitvoering door art 5 1-2e toch blijkt dat er onbevoegd toegang is verkregen tot de mappen van Bibob dan neemt art 5 1-2e contact op met FG en team informatieveiligheid.

Verder is gebleken uit de audittrial dat enkel bevoegde beheerders toegang hebben verkregen tot de mappen van het Bibob-team (ter uitvoering van hun werkzaamheden). Binnen het team van beheerders zijn dan ook onderling afspraken gemaakt over de beheertaken met betrekking tot de mappenstructuur van het Bibob-team. De stelling dat bestand bekeken kunnen worden zonder de juiste rechten is niet aan de orde. Het functioneel beheer wordt uitgevoerd as designed. Er is geen sprake dat er ongeautoriseerd personeel toegang heeft tot persoonsgegevens. Omdat er behoefte is aan extra beveiligingsmaatregelen heeft art 5 1-2e art 5 1-2e (beheer iDMS) aangeboden om verdere uitleg te geven over de technische beveiligingsmogelijkheden van iDMS. art 5 1-2e krijgt een beheerdersrol toegewezen, zodat zij o.a. zelf de toegangsrechten kan aanmaken en intrekken. art 5 1-2e en art 5 1-2e stemmen verdere procedurele- en technische maatregelen met elkaar af.

art 5 1-2e (FG) heeft een andere mening over deze kwestie.

Ik hoop jullie zo voldoende te hebben geïnformeerd, indien er vragen zijn dan verneem ik die graag.

Een prettige middag gewenst en hartelijke groet,

art 5 1-2e
"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Definitief

Melding gegevens

Naam melder	:	art 5 1-2e (FG), namens art 5 1-2e (concerndirecteur)
Registratienummer van het incident	:	M20 07 01126
Datum en tijdstip van de melding	:	Maandag 13 juli 2020 13:20
Route van de melding	:	Digitale Loket

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Dinsdag 28 juli 2020 13:00
Advies besproken met	:	art 5 1-2e (FG) art 5 1-2e (jurist), art 5 1-2e (privacy officier), art 5 1-2e (adviseur informatieveiligheid)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerkers

Situatie

Melding is als onderstaand binnengekomen:

art 5 1-2e 13 juli 2020 13:18

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan

- Namens de concerndirecteur meld ik een datalek in iDMS. De toegang tot zeer geheime documenten in iDMS is toegankelijk voor een veel te grote groep beheerders (in dit geval van het team Bibob en de FG). Daarnaast is de logging van deze groep niet op voldoende niveau geregeld.

Let wel: in het kader van het onderzoek mag NIET worden gekeken in de mappen van het team Bibob of de FG!

Wat voor soort incident heeft er plaats gevonden?
- Iemand kan bestanden inzien zonder de juiste rechten

Wanneer vond de inbreuk plaats? Indien bekend
-

Wanneer vond de inbreuk plaats? Indien niet bekend
- sinds 25 mei 2018

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Er is geen sprake van een datalek.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Er is geen sprake van een datalek.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Er is geen sprake van een datalek.

Vraag	Antwoord
Welke persoonsgegevens betreft het?	Er is geen sprake van een datalek.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Er is geen sprake van een datalek.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Er is geen sprake van een datalek.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Er is geen sprake van een datalek.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Er is geen sprake van een datalek.
Betreft het een datalek?	Er is geen sprake van een datalek. .
Ondernomen beperkende maatregelen.	Er is geen sprake van een datalek.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Er is geen sprake van een datalek.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

Maandag 20 juli heeft een gesprek met betrokkenen plaats gevonden waarbij de aanleiding van het datalek als onderstaand is besproken:

Aanleiding voor het melden van een datalek is de onrust bij het Bibob-team over de toegang tot hun vertrouwelijke iDMS-mappen en in het bijzonder de mappen over C-quential. art 5 1-2e (coördinator Bibob) is, op maandag 20 juli, voorzien van informatie over het verkrijgen van inzicht in wie, welke documenten heeft geraadpleegd. Uit een eerste controle, onder mijn toezicht, is gebleken dat er geen sprak is van onbevoegde toegang of onjuist rechtenstructuur. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. In dit specifieke geval is er geen sprake van een beveiligingsincident of datalek. Er is geen aanwijzing dat er persoonsgegevens verloren zijn gegaan of dat er “onrechtmatige verwerking” van persoonsgegevens heeft plaats gevonden. Indien uit een tweede controleslag (uitvoering door art 5 1-2e toch blijkt dat er onbevoegd toegang is verkregen tot de mappen van Bibob dan neemt art 5 1-2e ontact op met FG en team informatieveiligheid.

Verder is gebleken uit de audittrial dat enkel bevoegde beheerders toegang hebben verkregen tot de mappen van het Bibob-team (ter uitvoering van hun werkzaamheden). Binnen het team van beheerders zijn dan ook onderling afspraken gemaakt over de beheertaken met betrekking tot de mappenstructuur van het Bibob-team. De stelling dat bestand bekeken kunnen worden zonder de juiste rechten is niet aan de orde. Het functioneel beheer wordt uitgevoerd as designed. Er is geen sprake dat er ongeautoriseerd personeel toegang heeft tot persoonsgegevens.

Omdat er behoefte is aan extra beveiligingsmaatregelen heeft art 5 1-2e art 5 1-2e (beheer iDMS) aangeboden om verdere uitleg te geven over de technische beveiligingsmogelijkheden van iDMS. art 5 1-2e krijgt een beheerdersrol toegewezen, zodat zij o.a. zelf de toegangsrechten kan aanmaken en intrekken. art 5 1-2e en art 5 1-2e stemmen verdere procedurele- en technische maatregelen met elkaar af.

Conclusie en advies

Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. In dit geval is er geen sprake van een datalek.

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: art 5 1-2e

Melddatum: 06 juli 2023

Meldtijdstip: 15:55

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

AUTORITEIT
PERSOONSGEGEVENS

KvK-nummer (indien van toepassing)	27375169
Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Provincie

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	art 5 1-2e
Functie	Privacy officer
E-mailadres	art 5 1-2e @pzh.nl
Telefoonnummer	art 5 1-2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Ja

Geef aan welke andere organisaties betrokken waren bij de inbreuk?

AUTORITEIT
PERSOONSGEGEVENS

Naam	Op welke wijze betrokken	Toelichting (optioneel)
IV-Groep	aannemer (uitvoerend)	in opdracht van Provincie Zuid-Holland
ICT-leverancier van IV-Groep	(sub)verwerker van IV-Groep	

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	1-12-2022
(Mogelijke) einddatum van de inbreuk	31-12-2022
4.2 Wanneer is het incident ontdekt?	4-7-2023
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	De IV-Groep heeft dinsdag 4 juli een melding gedaan aan de Provincie Zuid-Holland. De IV-Groep geeft aan dat door hun deze leverancier het volgende is geconstateerd: - het Azure Storage account waarmee de backups van onze Ftp-server werden gemaakt, was niet voldoende beveiligd, waardoor deze benaderbaar was vanaf internet. Deze back-up service is eind 2022 beëindigd. Dit is door een externe beveiligingsonderzoeker (ethische hacker) , aangesloten bij DIVD, geconstateerd.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

AUTORITEIT
PERSOONSGEGEVENS

[✓] Hacking, malware (bijv. ransomware) en/of phishing

Meerdere opties zijn mogelijk binnen het gearceerde deel.

[✓] Ander type hacking en/of malware

Heeft u (digitaal forensisch) onderzoek uitgevoerd of laten uitvoeren naar de aard en de omvang van het datalek?	Ja, het onderzoek is afgerond

Optioneel: upload hier de rapportage van het onderzoek naar de inbreuk.

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Iv-Groep is een Nederlands ingenieurs bureau en is werkzaam in diverse marktsegmenten (water, infra, industrie, offshore & energy, bouw). Via één van haar werkmaatschappen zijn er werkzaamheden verricht voor de Provincie Zuid-Holland. Voor het uitwisselen van grote hoeveelheid bestanden is er gebruik gemaakt van een zogenaamde Ftp-server. Deze Ftp server wordt beheerd door één van de ICT-dienstverleners van Iv-Groep. Hierop kan via een toegekende gebruikersnaam en wachtwoord toegang tot deze informatie verkregen worden, zowel door Iv-medewerkers als door Provincie Zuid-Holland als opdrachtgever. Door deze ICT-dienstverlener is geconstateerd dat het Azure Storage account waarmee de backups van de Ftp-server werden gemaakt, niet voldoende was beveiligd, waardoor deze benaderbaar was vanaf internet. Dit is geconstateerd door een externe beveiligingsonderzoeker (ethische hacker), aangesloten bij DIVD. Deze back-up service is eind 2022 beëindigd. Er is geen aanwijzing dat er onbevoegde toegang is geweest (anders dan de ethisch hacker). Er is onvoldoende logging beschikbaar om dit met zekerheid vast te stellen.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

AUTORITEIT
PERSOONSGEGEVENS

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Contactgegevens

[✓] Adres en woonplaats

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	700
Geef een toelichting op bovengenoemd aantal:	Het betreft een adressenlijst met 700 NAW gegeven van bewoners, waarschijnlijk gebruikt voor etikettering van een standaard brief.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	aanwonenden van een provinciale weg
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	aanwonenden van een provinciale weg aan wie een brief moest worden gestuurd.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	700

8 Maatregelen vooraf

AUTORITEIT
PERSOONSGEGEVENS

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Betrokkenen kunnen ongewenst worden aangeschreven.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Het betreft NAW gegevens die met minimale inspanning ook op andere manieren verkregen kunnen worden.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Ja

AUTORITEIT
PERSOONSGEGEVENS

Aan hoeveel personen wilt u de inbreuk gaan melden?	700
Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?	7-8-2023
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Nog niet bekend

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per brief

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nog niet bekend
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nog niet bekend

11 Verzenden

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

AUTORITEIT
PERSOONSGEGEVENS

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	6-9-2023
Toelichting	Nader onderzoek waarbij wij afhankelijk zijn van informatie afkomstig van een derde partij (en de ICT-leverancier van die derde partij) in een vakantieperiode.

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

Melden datalek

Aanmelder

Naam	art 5 1-2e
Telefoonnummer	
E-mail	art 5 1-2e @pzh.nl
Organisatie-eenheid	Bureau Infrastructuur en Support
Kostenplaatscode	279

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Naar aanleiding van melding M23 03 03260 Op de nacht van zaterdag op zondag is er een pak papier uit de printer gekomen. Hierin staat allerlei mogelijk vertrouwelijk informatie. art 5 1-2e Xerox) heeft al me t art 5 1-2e serverteam) de oorzaak al proberen te achterhalen. Het voorval heeft zich voor gedaan op het moment dat de tijd voor uitgezet is vanwege zomertijd
Wat voor soort incident heeft er plaats gevonden?	Anders
Anders? Graag toelichten	Documenten op de printer achtergelaten(meer dan 200 vel)
Wanneer vond de inbreuk plaats? Indien bekend	26 maart 2023 3:00
Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☑

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☑

Telefoonnummers	☑
E-mailadressen of andere adressen voor digitale communicatie	☑
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☑
Anders, namelijk	onduidelijk wat de inhoud is.
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	diverse
Schatting van het aantal personen betrokken bij het datalek: minimaal	
Schatting van het aantal personen betrokken bij het datalek: maximaal	

art 5 1-2e

Van: art 5 1-2e
Verzonden: dinsdag 22 augustus 2023 09:32
Aan: art 5 1-2e
CC: art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: RE: Afspraak werkgroep

Hi allen,

art 5 1-2e an twoord zojuist dat zij de e-mail meteen na verzenden heeft vernietigd en de 'verkeerde' art 5 1-2e eeft benaderd om hetzelfde te doen.

Met vriendelijke groet,

art 5 1-2e
e ring en Automatisering
Directiesecretaresse Bedrijfsvoering

provincie Zuid-Holland

T art 5 1-2e
E art 5 1-2e p zh.nl
Werkdagen: ma, di, wo, vr

Provincie Zuid-Holland | Zuid-Hollandplein 1
Postbus 90602 | 2509 LP Den Haag
www.zuid-holland.nl

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e @pzh.nl>
Verzonden: dinsdag 22 augustus 2023 09:10
Aan: art 5 1-2e @pzh.nl>
CC: art 5 1-2e < art 5 1-2e @pzh.nl>; art 5 1-2e < art 5 1-2e p zh.nl> art 5 1-2e @pzh.nl>
Onderwerp: RE: Afspraak werkgroep

Hallo art 5 1-2e

Ik heb deze week 'datalekkendienst' dus ik pak het op.

Even een vraag aan jou: heb jij de afzender art 5 1-2e t gevraagd of zij aan de 'verkeerde art 5 1-2e eeft gevraagd om de per abuis aan haar verzonden email te vernietigen? Zo ja, mooi, zo nee, zou je dat dan a w illen doen?

Dank je wel alvast!

Groeten,

art 5 1-2e

Privacy Officer
Eenheid Privacy

provincie Zuid-Holland

T art 5 1-2e

E art 5 1-2e @pzh.nl
www.zuid-holland.nl/contact

Werkdagen: ma, di, wo, do, vr

Krachtig Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e @pzh.nl>
Verzonden: maandag 21 augustus 2023 15:39
Aan: art 5 1-2e < art 5 1-2e @pzh.nl>
Onderwerp: FW: Afspraak werkgroep

Van: art 5 1-2e @pzh.nl>
Verzonden: maandag 21 augustus 2023 15:17
Aan: art 5 1-2e < art 5 1-2e @p zh.nl>; art 5 1-2e < art 5 1-2e @pzh.nl>
CC art 5 1-2e @pzh.nl>
Onderwerp: FW: Afspraak werkgroep

Hallo heren,

Zojuist hebben wij art 5 1-2e n ikzelf, deze mails ontvangen van art 5 1-2e Zij heeft in haar eerste mailing per abuis de verkeerd art 5 1-2e eselecteerd bij het verzenden, waardoor de namen van deze collega's naar een voor ons onbekende externe zijn gestuurd. Van één collega art 5 1-2e is een privé -emailadres meegestuurd.
Nu staat er niet bijzonder veel gevoelige informatie in het bericht, maar na overleg met art 5 1-2e maak ik toch melding om in ieder geval de juiste stappen te volgen zodat ons niets te verwijten valt.

Met vriendelijke groet,

art 5 1-2e
Secretariaat Informatisering en Automatisering
Directiesecretaresse Bedrijfsvoering

provincie Zuid-Holland

T art 5 1-2e
art 5 1-2e @p zh.nl

Werkdagen: ma, di, wo, vr

Provincie Zuid-Holland | Zuid-Hollandplein 1
Postbus 90602 | 2509 LP Den Haag
www.zuid-holland.nl

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e @ghocommunicatie.nl>
Verzonden: maandag 21 augustus 2023 14:52
Aan: art 5 1-2e @pzh.nl>; art 5 1-2e zh.nl>
Onderwerp: Re: Afspraak werkgroep

Sorry, ik ben toe aan vakantie denk ik.
Nu zie ik dat mijn mail naar de verkeerde art 5 1-2e g egaan.

Groeten art 5 1-2e

Van: art 5 1-2e @ghocommunicatie.nl>
Datum: maandag, 21 augustus 2023 om 14:34
Aan: art 5 1-2e p zh.nl>, art 5 1-2e @k ollektiv-media.com>
Onderwerp: Afspraak werkgroep

Goedemiddag art 5 1-2e

Ben even kwijt wie er nog op vakantie is dus even naar jullie allebei.

1 september staat de eerste presentatie ingepland met art 5 1-2e en art 5 1-2e. Daar moet een vervolg op komen met de hele werkgroep. Hieronder de lijst met namen.
Kunnen jullie kijken wanneer dit zou kunnen? Voor keur voor woensdag of vrijdag in de ochtend.
Mag weer een teams call van max 1,5uur.

art 5 1-2e

Met vriendelijke groet,

art 5 1-2e

Projectleider

Ik ben bereikbaar op art 5 1-2e
Aanwezig op ma | di | do | vrij (ochtend)

Van 31 juli t/m 21 augustus heeft GH+O haar eigen bouwvak: 'makersverlof'. In deze periode zijn veel makers op vakantie en is onze capaciteit beperkt. Natuurlijk zijn we voor dringende vragen bereikbaar. En heb je een nieuwe opdracht? Bel gerust. We pakken de planning en uitvoering dan na het makersverlof op. Is jouw project al ingepland? Dan gaan we daar uiteraard volgens afspraak mee aan de slag.

Fijne vakantie! Team GH+O

Leiden
Nieuwstraat 31a
2312 KA Leiden
071 203 21 23

Leeuwarden
Zuidergrachtswal 3
8933 AD Leeuwarden
058 299 11 55

art 5 1-2e

Van: art 5 1-2e
Verzonden: maandag 21 augustus 2023 15:39
Aan: art 5 1-2e
Onderwerp: FW: Afspraak werkgroep

Van: art 5 1-2e @p zh.nl>
Verzonden: maandag 21 augustus 2023 15:17
Aan: art 5 1-2e < art 5 1-2e @p zh.nl>; art 5 1-2e < art 5 1-2e @pzh.nl>
C art 5 1-2e @pzh.nl>
Onderwerp: FW: Afspraak werkgroep

Hallo heren,

Zojuist hebben wij, art 5 1-2e n ikzelf, deze mails ontvangen van art 5 1-2e . Zij heeft in haar eerste mailing per abuis de verkeerde art 5 1-2e geselecteerd bij het verzenden, waardoor de namen van deze collega's naar een voor ons onbekende externe zijn gestuurd. Van één collega, art 5 1-2e is een privé -emailadres meegestuurd.
Nu staat er niet bijzonder veel gevoelige informatie in het bericht, maar na overleg met art 5 1-2e maak ik toch melding om in ieder geval de juiste stappen te volgen zodat ons niets te verwijten valt.

Met vriendelijke groet,

art 5 1-2e
Secretariaat Informatisering en Automatisering
Directiesecretaresse Bedrijfsvoering

provincie Zuid-Holland

T art 5 1-2e
E art 5 1-2e
Werkdagen: ma, di, wo, vr

Provincie Zuid-Holland | Zuid-Hollandplein 1
Postbus 90602 | 2509 LP Den Haag
www.zuid-holland.nl

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e g hocommunicatie.nl>
Verzonden: maandag 21 augustus 2023 14:52
Aan: art 5 1-2e @pzh.nl> art 5 1-2e o zh.nl>
Onderwerp: Re: Afspraak werkgroep

Sorry, ik ben toe aan vakantie denk ik.
Nu zie ik dat mijn mail naar de verkeerde art 5 1-2e s gegaan.

Groeten art 5 1-2e

Van: art 5 1-2e @ghocommunicatie.nl>
Datum: maandag, 21 augustus 2023 om 14:34
Aan: art 5 1-2e @p zh.nl>, art 5 1-2e @k ollektiv-media.com>
Onderwerp: Afspraak werkgroep

Goedemiddag art 5 1-2e

Ben even kwijt wie er nog op vakantie is dus even naar jullie allebei.

1 september staat de eerste presentatie ingepland met art 5 1-2e en art 5 1-2e. Daar moet een vervolg op komen met de hele werkgroep. Hieronder de lijst met namen.
Kunnen jullie kijken wanneer dit zou kunnen? Voor keur voor woensdag of vrijdag in de ochtend.
Mag weer een teams call van max 1,5uur.

art 5 1-2e

Met vriendelijke groet,

art 5 1-2e

Projectleider

Ik ben bereikbaar op art 5 1-2e
Aanwezig op ma | di | do | vrij (ochtend)

Van 31 juli t/m 21 augustus heeft GH+O haar eigen bouwvak: 'makersverlof'. In deze periode zijn veel makers op vakantie en is onze capaciteit beperkt. Natuurlijk zijn we voor dringende vragen bereikbaar. En heb je een nieuwe opdracht? Bel gerust. We pakken de planning en uitvoering dan na het makersverlof op. Is jouw project al ingepland? Dan gaan we daar uiteraard volgens afspraak mee aan de slag.

Fijne vakantie! Team GH+O

art 5 1-2e

Van: art 5 1-2e
Verzonden: dinsdag 22 augustus 2023 09:14
Aan: art 5 1-2e
CC: art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: RE: Afspraak werkgroep

Hallo art 5 1-2e

Ik heb art 5 1-2e zojuist gevraagd om de e-mail te vernietigen.

Met vriendelijke groet,

art 5 1-2e
Secretariaat Informatisering en Automatisering
Directiesecretaresse Bedrijfsvoering

provincie Zuid-Holland

T art 5 1-2e
E art 5 1-2e @p zh.nl
Werkdagen: ma, di, wo, vr

Provincie Zuid-Holland | Zuid-Hollandplein 1
Postbus 90602 | 2509 LP Den Haag
www.zuid-holland.nl

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e @pzh.nl>
Verzonden: dinsdag 22 augustus 2023 09:10
Aan art 5 1-2e @pzh.nl>
CC: art 5 1-2e < art 5 1-2e @pzh.nl>; art 5 1-2e < art 5 1-2e @p zh.nl>; art 5 1-2e zh.nl>
Onderwerp: RE: Afspraak werkgroep

Hallo art 5 1-2e

Ik heb deze week 'datalekkendienst' dus ik pak het op.

Even een vraag aan jou: heb jij de afzender art 5 1-2e gevraagd of zij aan de 'verkeerde' art 5 1-2e heeft gevraagd om de per abuis aan haar verzonden email te vernietigen? Zo ja, mooi, zo nee, zou je dat dan alsnog willen doen?

Dank je wel alvast!

Groeten,

art 5 1-2e
Privacy Officer

Eenheid Privacy

provincie Zuid-Holland

T art 5 1-2e
M
E art 5 1-2e @pzh.nl
www.zuid-holland.nl/contact

Werkdagen: ma, di, wo, do, vr

Krachtig Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e @pzh.nl>
Verzonden: maandag 21 augustus 2023 15:39
Aan: art 5 1-2e < art 5 1-2e @pzh.nl>
Onderwerp: FW: Afspraak werkgroep

Van art 5 1-2e @pzh.nl>
Verzonden: maandag 21 augustus 2023 15:17
Aan: art 5 1-2e < art 5 1-2e @p zh.nl>; art 5 1-2e < art 5 1-2e @pzh.nl>
CC: art 5 1-2e o zh.nl>
Onderwerp: FW: Afspraak werkgroep

Hallo heren,

Zojuist hebben wij, art 5 1-2en ikzelf, deze mails ontvangen van art 5 1-2e Zij heeft in haar eerste mailing per abuis de verkeerde art 5 1-2e eselecteerd bij het verzenden, waardoor de namen van deze collega's naar een voor ons onbekende externe zijn gestuurd. Van één collega art 5 1-2e i s een privé -emailadres meegestuurd.
Nu staat er niet bijzonder veel gevoelige informatie in het bericht, maar na overleg met art 5 1-2e maak ik toch melding om in ieder geval de juiste stappen te volgen zodat ons niets te verwijten valt.

Met vriendelijke groet,

art 5 1-2e
Secretariaat Informatisering en Automatisering
Directiesecretaresse Bedrijfsvoering

provincie Zuid-Holland

T art 5 1-2e
E art 5 1-2e @p zh.nl
Werkdagen: ma, di, wo, vr

Provincie Zuid-Holland | Zuid-Hollandplein 1
Postbus 90602 | 2509 LP Den Haag
www.zuid-holland.nl

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e hocommunicatie.nl>
Verzonden: maandag 21 augustus 2023 14:52
Aan: art 5 1-2e zh.nl>; art 5 1-2e @pzh.nl>
Onderwerp: Re: Afspraak werkgroep

Sorry, ik ben toe aan vakantie denk ik.
Nu zie ik dat mijn mail naar de verkeerde art 5 1-2e s gegaan.

Groete art 5 1-2e

Van: art 5 1-2e hocommunicatie.nl>
Datum: maandag, 21 augustus 2023 om 14:34
Aan: art 5 1-2e p zh.nl>, art 5 1-2e @k ollektiv-media.com>
Onderwerp: Afspraak werkgroep

Goedemiddag art 5 1-2e

Ben even kwijt wie er nog op vakantie is dus even naar jullie allebei.

1 september staat de eerste presentatie ingepland met art 5 1-2e en art 5 1-2e . Daar moet een vervolg op komen met de hele werkgroep. Hieronder de lijst met namen.
Kunnen jullie kijken wanneer dit zou kunnen? Voor keur voor woensdag of vrijdag in de ochtend.
Mag weer een teams call van max 1,5uur.

art 5 1-2e

Met vriendelijke groet,
art 5 1-2e

Projectleider

Ik ben bereikbaar o art 5 1-2e
Aanwezig op ma | di | do | vrij (ochtend)

Van 31 juli t/m 21 augustus heeft GH+O haar eigen bouwvak: 'makersverlof'. In deze periode zijn veel makers op vakantie en is onze capaciteit beperkt. Natuurlijk zijn we voor dringende vragen bereikbaar. En heb je een nieuwe opdracht? Bel gerust. We pakken de planning en uitvoering dan na het makersverlof op. Is jouw project al ingepland? Dan gaan we daar uiteraard volgens afspraak mee aan de slag.

Fijne vakantie! Team GH+O

Leiden
Nieuwstraat 31a
2312 KA Leiden
071 203 21 23

Leeuwarden
Zuidergrachtswal 3
8933 AD Leeuwarden
058 299 11 55

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art 5 1-2e
Telefoonnummer	
E-mail	art 5 1-2e pzh.nl
Organisatie-eenheid	Bureau Ontwikkeling
Kostenplaatscode	438

Benodigde gegevens

Is dit een diefstal of vermissing?	Diefstal
Is er al aangifte gedaan?	Nee
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH. Wat is het 06 nummer?	art 5 1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	In de trein in / nabij station Leiden Centraal, zaterdag 19 augustus 2023 rond 21:30 uur. (treinstel 8647 vanuit Venlo via Utrecht/Schiphol naar Den Haag Centraal, aankomst 21:45 uur; ik ben in Utrecht Centraal (20:42 uur) op deze trein gestapt. Ik zat in het achterste treindeel, bovenin, in een tweezitter.
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja

Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Ja
Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Onbekend
Zijn de gegevens versleuteld?	Onbekend
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Ja
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Ik was per trein onderweg van Münster (D), via Enschede en Utrecht naar Den Haag Centraal. Vanwege werkzaamheden moest ik in Utrecht de trein nemen (vertrek 20:42 uur) die via Schiphol naar Den Haag reed (aankomst 21:45 uur). Mijn bagage stond tussen mijn voeten, tijdens deze reis haalde ik mijn jas uit een tas en hing deze aan het haakje achter mijn stoel. Nabij station Leiden Centraal zette ik mijn werktelefoon op vluchtmodus en deed deze in mijn linkerjaszak, waarbij ik de rits dicht deed. Ongeveer 10 à 15 minuten later trok ik mijn jas aan en merkte dat de ristsluiting open was en de telefoon was verdwenen. Ik keek meteen naar de persoon op de tweezitter achter mij en sprak hem aan. Deze persoon hield zich van de domme, liet zijn eigen telefoon zien en hield vol dat hij van niets wist. Met mijn privételefoon belde ik mijn werknummer, maar omdat die op vluchtmodus stond ging die niet over. Bij aankomst in Den Haag Centraal sprak ik hem dwingender aan, waarna hij mij van racisme beschuldigde. Ik liep snel de trein uit en sprak enkele conducteurs op het perron aan. De verdachte werd door hen tegengehouden en de spoorwegpolitie kwam er snel bij. De verdachte werd door hem gefouilleerd en kleedde zich deels uit, hij had mijn telefoon niet bij zich. Een mededader zal in de trein (ik vermoed rond Leiden Centraal, in de stroom van in- en uitstappende reizigers) de telefoon van de verdachte hebben overgenomen en ik vermoed dat die persoon bij aankomst in Den Haag meteen in de trein aan de andere kant van het perron (spoor 8) zal zijn teruggereisd (die vertrok 21:46 uur naar Leiden-Schiphol-Utrecht). De persoon die door de Spoorwegpolitie werd ondervraagd had geen geldig vervoersbewijs en bleef daarom nog achter op het station. De NS-medewerkers gaven ook aan dat er zeer waarschijnlijk één of meer medeverdachten in het spel zijn geweest. Verspreid over de coupé zaten enkele andere passagiers, maar niet iemand die getuige was. Zelf heb ik de diefstal niet op het moment zelf opgemerkt, maar wel binnen minuten na de diefstal, zodat ik zeker weet dat de door mij aangesproken persoon deel is van een clubje zakkenrollers.

Melden datalek

Aanmelder

Naam	art 5 1-2e
Telefoonnummer	
E-mail	art 5 1-2e @pzh.nl
Organisatie-eenheid	Veiligheid, SecrOnderst, WagenpBeh en Grafimedia
Kostenplaatscode	373

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Een externe partij heeft per abuis voor- en achternamen van onze collega's naar een voor ons onbekende partij gemaild. Tevens is een privé e-mailadres van één collega meegestuurd.
Wat voor soort incident heeft er plaats gevonden?	Mail naar een verkeerde ontvanger
Wanneer vond de inbreuk plaats? Indien bekend	21 augustus 2023 14:34
Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☑

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☑
Telefoonnummers	☐

E-mailadressen of andere adressen voor digitale communicatie	☑
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☐
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	Werkenemers
Schatting van het aantal personen betrokken bij het datalek: minimaal	15
Schatting van het aantal personen betrokken bij het datalek: maximaal	20

art 5 1-2e

Van: art 5 1-2e
Verzonden: uari 2023 12:54
Aan: art 5 1-2e
CC: art 5 1-2e
Onderwerp: rijk update: Ransomware aanval

Ter info. Mogelijk datalek bij leverancier P8 van PZH. Of er daadwerkelijk data is buitgemaakt, is nog niet duidelijk. Daarover worden we geïnformeerd.

Wordt vervolgd.

Groet, art 5 1-2e

art 5 1-2e | CISO art 5 1-2e

Van: art 5 1-2e @pzh.nl>
Datum: maandag, 6 februari 2023 om 10:18
Aan: art 5 1-2e < art 5 1-2e @pzh.nl >, art 5 1-2e < art 5 1-2e @pzh.nl >
Onderwerp: RE: Belangrijk update: Ransomware aanval

Hoi art 5 1-2e

Het gaat vooral om verpachte en verhuurde eigendommen van de provincie, dat zijn percelen. Daarbij worden de gesloten overeenkomsten en facturen in P8 geregistreerd. BSN-nummers heb ik allemaal al eerder laten verwijderen, bankrekeningnummers staan er ook niet in. Wel KvK-nummers, namen en adressen van particulieren. En dat vanaf 2014/2015 ongeveer...

Gegevens over transacties zijn van 2015 en verouderd. Dus geen voorgenomen aan- en verkopen.

Groeten,
art 5 1-2e

Van: art 5 1-2e < art 5 1-2e @pz h.nl>
Verzonden: maandag 6 februari 2023 09:29
Aan: art 5 1-2e < art 5 1-2e @pzh. nl>; art 5 1-2e @pzh. nl> art 5 1-2e zh.nl>
CC art 5 1-2e @pzh. nl>
Onderwerp: Re: Belangrijk update: Ransomware aanval

Hi art 5 1-2e art 5 1-2e

Dank je voor informatie. Welke data heeft P8 van de provincie? Qua persoonsgegevens (niet zo veel wrs.) en gevoelige gegevens (bv. voorgenomen grondaankopen)?

Groet,
art 5 1-2e

art 5 1-2e | CISO art 5 1-2e

Van: art 5 1-2e < art 5 1-2e @pzh.nl>
Datum: maandag, 6 februari 2023 om 09:17
Aan art 5 1-2e @pzh.nl >, art 5 1-2e pzh.nl >, art 5 1-2e
< art 5 1-2e @pzh.nl >, art 5 1-2e @pzh.nl >
CC art 5 1-2e pzh.nl >
Onderwerp: Re: Belangrijk update: Ransomware aanval

Hi art 5 1-2e e dankt voor je bericht. Zou je art 5 1-2e en mij op de hoogte willen houden.

Alvast bedankt!

Groet,
art 5 1-2e

Verzonden vanaf Outlook voor Android

From: art 5 1-2e pzh .nl>
Sent: Monday, February 6, 2023 9:03:11 AM
To: art 5 1-2e < art 5 1-2e @p zh.nl>; art 5 1-2e < art 5 1-2e pzh.nl >; art 5 1-2e < art 5 1-2e @pzh. nl> art 5 1-2e
art 5 1-2e @pzh.nl>
Cc: art 5 1-2e @pzh. nl>
Subject: FW: Belangrijk update: Ransomware aanval

Goedemorgen heren,

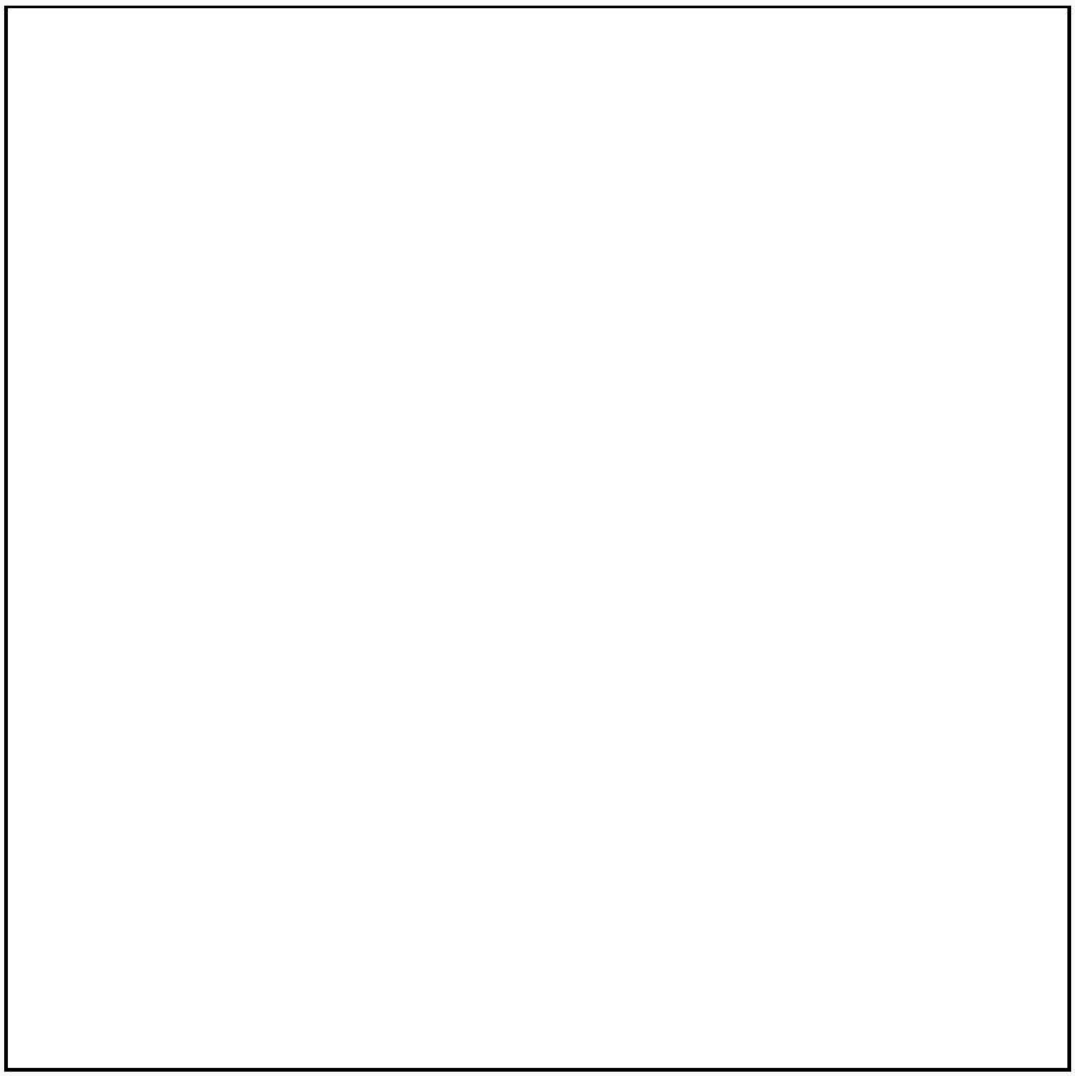
P8 Software is dit weekend slachtoffer van een ransomware aanval geworden. Zie de mail hieronder, en het NOS-bericht:
https://nos.nl/artikel/2462701-grootschalige-aanval-met-gijzelsoftware-op-duizenden-servers-wereldwijd

P8 draait op dit moment weer, ze hebben alles weer snel in de lucht gekregen. De vraag is nog of er data is gelekt. Vanmiddag hoor ik meer. Wie van jullie moet ik op de hoogte houden?

Groeten
art 5 1-2e

Van: P8 Software <info@p8.nl>
Verzonden: zondag 5 februari 2023 22:25
Aan: art 5 1-2e @pzh.nl>
Onderwerp: Belangrijk update: Ransomware aanval

View this email in your browser



Geachte relatie,

Dit weekend is er een ransomware aanval geweest op een groot aantal systemen in Nederland en de rest van de wereld. Ook de service provider van P8 Software en daarmee P8 is slachtoffer geworden van deze aanval. Een dergelijke inbraak heeft behoorlijke impact. Dit bericht is opgesteld om u zo goed mogelijk te informeren. We verwachten door de genomen maatregelen, de overlast en schade tot een minimum beperkt te hebben. Alle omgevingen worden opnieuw opgezet en daarmee zijn we in een vergevorderd stadium.

Ondervindt u hinder maandagochtend met inloggen?

Alles wordt in het werk gesteld om u maandagochtend te kunnen laten werken. Vooralsnog hebben we daarbij het pachtportaal een lagere prioriteit gegeven.

Voor het overgrote deel van de klantomgevingen zouden de problemen maandagochtend opgelost moeten zijn. Het kan zijn dat de DNS doorverwijzing nog niet werkt, dat duurt enkele uren.

Hoe is het met de beschikbaarheid van ons systeem?

We hebben een geheel nieuwe infrastructuur opgebouwd en migreren onze omgevingen naar Microsoft Azure. Vervolgens is uw omgeving weer ingericht. Een aantal omgevingen (RealWaste/RealSlib) draaiden op een ander platform en die zijn niet geraakt door de aanval.

Is er data data verloren gegaan?

We hebben alle data beschikbaar en hebben daarmee de nieuwe omgevingen opgezet. Naast de actuele data hadden we ook de back-ups achter de hand.

Is er data in handen van derden gekomen?

Hier wordt door een forensisch bureau (door ons ingehuurd) op dit moment onderzoek naar gedaan. Het is een geautomatiseerde hack waardoor de kans klein is dat data in handen van derden is gevallen. Volledige zekerheid hierover hebben we echter nog niet. Nadere informatie volgt zodra we meer weten.

Op dit moment heeft P8 Software heeft een voormelding gemaakt van een mogelijk datalek bij de Autoriteit Persoonsgegevens. Daarnaast wordt aangifte gedaan bij de politie.
We koppelen zo spoedig mogelijk terug als er vanuit uw kant ook actie vereist is. Mocht er toch data in handen van derden zijn gekomen, dan dient dit binnen 72 uur (wettelijke termijn) na melding door ons kenbaar gemaakt te worden. We geven u hier zo spoedig mogelijk een update over.

Wanneer kan ik een nadere update verwachten?

Maandag 6 februari rond de middag geven we u een nadere update hoe ver we zijn met het gereed maken van de omgevingen. Kunt u gewoon inloggen? Dan is uw omgeving klaar voor gebruik. Mocht inloggen nog niet lukken, dan komt uw omgeving later in de ochtend beschikbaar. Mocht u behoefte hebben aan een mondelinge toelichting dan zitten art 5 1-2e art 5 1-2e en art 5 1-2e voor u klaar. U k unt hen bereiken via het algemene nummer van P8 Software. Onze Servicedesk is doorgeschakeld naar het algemene nummer.

Natuurlijk betreuren we dit incident en bieden we onze excuses aan voor de eventuele overlast.

We stellen alles in het werk om dit tot een minimum te beperken voor u. Bedankt voor uw begrip.

Groeten,

art 5 1-2e

Klik hier voor meer informatie over het gevonden issue

Van: art 5 1-2e
Verzonden: 2023-03-31 15:50:15+00:00
Aan: art 5 1-2e
CC: Willy de Zoete - van der Hout; privacy; art 5 1-2e
Onderwerp: Datalek postkamer - printer print in de nacht bestanden met persoonsgegevens - advies: WEL datalek NIET melden
"
Beste art 5 1-2e

Bijgaand een advies inzake een datalek. De printer in de postkamer heeft buiten openingstijden automatisch bestanden met persoonsgegevens uitgeprint. Op ons verzoek doet I&A onderzoek naar de oorzaak. Ons advies is: niet melden alleen registreren intern.

Volg je het advies?

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7Cprivacy%40pzh.nl%7C10efaed5021a48bd8f8908db31eedb69%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638158674676598732%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=8pq2wDOSY0dv%2FBdlh9zklb3KIruADrk7tjy6hVfKTEM%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.
"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: defintief

Melding gegevens

Aangemeld door	:	art 5 1-2e (Bureau Infrastructuur en Support) (Informatisering en Automatisering))
Registratienummer van het incident	:	M23 03 03583
Datum en tijdstip van de melding	:	29-03-2023, 11.03
Route van de melding	:	melding datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	31 maart 2023 om 14.48 uur,
Advies besproken met	:	Besproken met art 5 1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Gedeeld met eenheid Privacy

Situatie

Melder geeft aan dat een printer in de postkamer (Alleen postkamer medewerkers hebben autorisatie om te printen via deze printer) automatisch bestanden heeft uitgeprint. Dit gebeurde in de nacht van zaterdag 25 maart op zondag 26 maart nadat de zomertijd is ingegaan. Gesproken met art 5 1-2e (Xerox) en art 5 1-2e (I&A). Zij hebben in de logboeken gekeken en daaruit valt niet op te maken wie de oorspronkelijke printopdracht naar de postkamer heeft gestuurd. Wel is geconstateerd dat de printopdracht in de nacht van zaterdag op zondag is uitgevoerd. Melder heeft de uitgeprinte stukken achter slot en grendel bewaard. Eenheid Privacy heeft de stukken overgedragen gekregen en deze veiliggesteld. De uitgeprinte stukken bevatten persoonsgegevens. Het zijn o.a. mailwisselingen tussen PZH en de gemeente Leidschendam-Voorburg, bestemmingsplannen, uitgifte van erfpacht en adviesrapportages.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Onbekend.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Waarschijnlijk 0 personen. Het vond plaats buiten de openingstijden van het Provinciehuis. De stukken zijn maandagochtend aangetroffen in de postkamer, waar deze stukken zich horen te bevinden.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen.
Welke persoonsgegevens betreft het?	Normale persoonsgegevens.

Vraag	Antwoord
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Naar alle waarschijnlijkheid wel.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Mogelijk, Informatieveiligheid is ingelicht.
Betreft het een datalek?	Ja.
Ondernomen beperkende maatregelen.	De stukken zijn door melder overgedragen aan Eenheid Privacy. Eenheid Privacy heeft de stukken veiliggesteld.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Verzoek bij art 5 1-2e (coordinator Bureau Infrastructuur en Support) ingediend om verder uit te zoeken hoe dit heeft kunnen gebeuren en dat er maatregelen getroffen worden zodat dit niet nogmaals voorkomt.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

Printer heeft documenten uitgeprint toen er niemand in het PZH pand aanwezig was. Hoe dit heeft kunnen gebeuren is nog niet bekend. Documenten zijn door de melder overgedragen aan Eenheid Privacy. De uitgeprinte stukken bevatten o.a. mailwisselingen tussen PZH en de gemeente Leidschendam-Voorburg, bestemmingsplannen, uitgifte van erfpacht en adviesrapportages. De uitgeprinte stukken zijn door Eenheid Privacy opgeborgen. Het datalek wordt niet gemeld bij de AP en/of betrokkenen, omdat het niet waarschijnlijk is dat het incident een hoog risico vormt voor betrokkenen. De stukken bevatten geen bijzondere en/of gevoelige persoonsgegevens. Op verzoek van Eenheid Privacy onderzoekt I&A dit incident verder. Dit is van belang om soortgelijke incidenten in de toekomst te voorkomen.

Conclusie en advies

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt NIET gemeld bij de Autoriteit Persoonsgegevens of betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.


provincie
Zuid-Holland

"Van: art 5 1-2e
Verzonden: 2019-09-27 09:58:06+00:00
"Aan: art 5 1-2e, art 5 1-2e
CC:
Onderwerp: Datalek PZH
"
Hoi art 5 1-2e, art 5 1-2e

Wij hebben woensdag de pers gehaald.

Hierbij het artikel tkn.

Gr. art 5 1-2e
"

DEEL DIT ARTIKEL:

WOENSDAG 25 SEPTEMBER 2019, 11:14

Datalek provincie Zuid-Holland: 'Persoonlijke gegevens politici onvoldoende beschermd'

Het Provinciehuis in Den Haag is oranje verlicht (Foto: Remco Zwinkels / Provinc

DEN HAAG - Door een datalek bij de provincie Zuid-Holland zijn de persoonlijke gegevens van Provinciale Statenleden en hun medewerkers

'tijdelijk onvoldoende beschermd' geweest. Dat blijkt uit een brief van de provincie die in handen is van Omroep West.

Om hoeveel politici en hun medewerkers het gaat, is niet duidelijk. Wel is de brief aan alle provinciale fracties gestuurd die momenteel in het provincieparlement actief zijn. Mogelijk zijn ook oud-Statenleden en hun medewerkers aan het lek blootgesteld.

Het ging om een lek in het IT-systeem van de provincie, waarin de persoonsgegevens worden geregistreerd 'voor de salarisverwerking, het verstrekken van toegangspassen en IT-middelen'. Voor zover bekend ging het om een intern lek, dus alleen medewerkers van de provincie hebben informatie kunnen verkrijgen die zij niet voor hun werk nodig hebben.

'Alert zijn op identiteitsfraude'

Het datalek is ontdekt door een alerte medewerker van de provincie, die opmerkte dat hij meer gegevens kon inzien dan nodig was voor zijn werkzaamheden. Hij heeft daarvan melding gedaan bij de provincie. Na onderzoek van de provincie bleek dat ook een andere groep medewerkers van de provincie, 406 personen, de persoonsgegevens van de politici en hun medewerkers kon inzien.

De gevolgen van het datalek bij de provincie zijn niet bekend, zo staat in de brief te lezen. Zo is niet zeker of medewerkers de informatie hebben ingezien. 'We hebben geen aanwijzing dat dit daadwerkelijk is gebeurd, maar we kunnen dit helaas niet uitsluiten.' De provincie hoopt dat de eigen medewerkers geen misbruik hebben gemaakt van de situatie. 'Al onze collega's leggen een ambtseed af en wij verwachten integer gedrag van ze. Niettemin raden wij u aan om alert te zijn op signalen van identiteitsfraude of ander misbruik van uw persoonsgegevens.'

Melding bij Autoriteit Persoonsgegevens

De provincie heeft na de ontdekking direct actie ondernomen om het datalek te dichten. 'Na constatering zijn uw persoonsgegevens uit het bewuste systeem verwijderd en de werkwijze is direct aangepast, zodat dit niet opnieuw kan gebeuren.'

De functionaris voor gegevensbescherming van de provincie, de concerndirectie en het provinciale bestuur (Gedeputeerde Staten) zijn op de hoogte van het lek. Daarnaast is er een officiële melding gedaan bij de Autoriteit Persoonsgegevens.

Op de Faalkaart is te zien dat onze provincie in de slechtste categorie valt - *Jeremy Mooiman (PVV)*

PVV-Statenlid Jeremy Mooiman vroeg onlangs nog aandacht voor de beveiliging van het IT-systeem van de provincie, nadat de provincie voorkwam op de Faalkaart, een lijst met overheden die slecht scoren als het gaat om ICT-beveiliging. Mooiman: 'Op de Faalkaart is te zien dat onze provincie in de slechtste categorie valt. Als naar de data wordt gekeken blijkt dat op 22-8-2019 (week 34) er 224 risico's zijn waargenomen, waarvan 29 'hoog risico' en 76 'gemiddeld risico'. Zuid-Holland is hiermee de derde meest kwetsbare provincie.'

CORRECTIE MELDEN >

provincie ZUID-HOLLAND

Gedeputeerde Staten

Postadres Provinciehuis
Postbus 90602
2509 LP Den Haag
T 070 - 441 66 11
www.zuid-holland.nl

Datum
24-9-2019

Mandaatnummer
-
Ons kenmerk
DOS-2018-0006727

Bijlagen
-

[naam]
[adres]

Onderwerp
Melding mogelijk datalek

Geachte heer/mevrouw,

O
nlangs is een datalek geconstateerd in één van onze systemen. Door dit lek zijn persoonlijke gegevens van u tijdelijk onvoldoende beschermd geweest. Met deze brief informeer ik u graag verder.

Melding datalek
Sinds vorig jaar mei is de Algemene Verordening Gegevensbescherming (AVG) van kracht. Deze verordening voorziet in een versterking van de privacyrechten en bescherming van persoonsgegevens. We hebben naar aanleiding van deze verordening onder meer een functionaris voor gegevensbescherming aangesteld en het toezicht op de verwerking van persoonsgegevens verder aangescherpt. Doordat wij onze bestaande werkwijzen en processen nu meer dan vroeger kritisch tegen het licht houden komen zwakke plekken sneller in beeld en kunnen we snel gepaste maatregelen nemen. Dat is ook nu het geval. Een alerte medewerker heeft op 11 september opgemerkt dat hij meer gegevens kon inzien dan hij nodig heeft voor het uitoefenen van zijn functie en heeft daar melding van gemaakt.

Toelichting aard en omvang
Voor het aanmelden van nieuwe statenleden en fractiemedewerkers maakt de provincie gebruik van een IT-systeem. Hierin worden de persoonsgegevens geregistreerd die u de provincie heeft verstrekt met oog op de salarisverwerking en het verstrekken van toegangspassen en IT-middelen. Dit gebeurt door daartoe aangewezen medewerkers van ondersteunende afdelingen. Een van deze medewerkers wees er op dat hij in dit IT-systeem meer van uw persoonsgegevens kon inzien dan strikt noodzakelijk voor de uitvoering van zijn taak. Daarnaast is na onderzoek gebleken dat een andere groep behandelaren (406 personen) – zij het met wat meer moeite – deze persoonsgegevens ook zou kunnen inzien. We hebben geen aanwijzing dat dit daadwerkelijk is gebeurd, maar kunnen dit helaas niet uitsluiten. Bovenstaand proces betreft alleen de incidentele tussentijdse personele wijzigingen en niet de aanmelding van meerdere personen bij de installatie van PS na de verkiezingen.

Bezoekadres
Zuid-Hollandplein 1
2596 AW Den Haag

Tram 9 en de buslijnen 90, 385 en 386 stoppen dichtbij het provinciehuis. Vanaf station Den Haag CS is het tien minuten lopen. De parkeerruimte voor auto's is beperkt.

v

provincie ZUID HOLLAND

Afhandeling en maatregelen
Na constatering zijn uw persoonsgegevens uit het bewuste systeem verwijderd en de werkwijze is direct aangepast, zodat dit niet opnieuw kan gebeuren. De functionaris voor gegevensbescherming, de concerndirectie en Gedeputeerde Staten zijn op de hoogte gesteld. Er is ook een officiële melding gedaan bij de Autoriteit Persoonsgegevens.

Wat betekent dit voor u?
Ik begrijp het als u zich mogelijk zorgen maakt over dit datalek. Het betreft immers uw persoonlijke gegevens. Echter: het feit dat de *mogelijkheid* bestond om uw gegevens in te zien, wil niet zeggen dat dit ook daadwerkelijk is gebeurd, laat staan dat er misbruik van is gemaakt. Helaas hebben we in dit geval niet kunnen uitsluiten dat te veel provinciale medewerkers mogelijk uw gegevens hebben kunnen inzien. Al onze collega's leggen een ambtseed af en wij verwachten integer gedrag van ze. Niettemin raden wij u aan om alert te zijn op signalen van identiteitsfraude of ander misbruik van uw persoonsgegevens. Daarom vind ik het van belang u dit bericht te sturen.

Vragen?
Ik kan me voorstellen dat er bij u nog vragen leven als het gaat om uw persoonlijke situatie. U kunt hiervoor contact opnemen met art 5 1-2e personeels- en salarisadministrateur via art 5 1-2e@pzh.nl o art 5 1-2e Ook is onze functionaris gegevensbescherming, de heer art 5 1-2e art 5 1-2e beschikbaar voor om uw vragen te beantwoorden. U kunt hem bereiken per e-mail via fg@pzh.nl of telefonisch op art 5 1-2e

Hoogachtend,

art 5 1-2e

Van: art 5 1-2e
Verzonden: 2023-09-29 10:39:34+00:00
Aan: art 5 1-2e
CC:
Onderwerp: art 5 1-2e heeft een opmerking in Memo Data IDMS beantwoord
"
<https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?url=https%3A%2F%2Fpzh-my.sharepoint.com%2Fpersonal%2 art 5 1-2e 2FDocuments%2FAVG%2FAdviezen%2FMemo%2520Data%2520IDMS.docx%3Fd%3Dw51745043f72e4fc8964573fab95f0dd2%26nav%3DeyJjIjoyMzY2NTQ1MzV9%26ne%3Dew0KICAidnQiOiB7DQogICAgImIiOiA3NTU1Nw0KICB9DQp9%26e%3D5Yc8bJBNYUKTFLoZci6exA%26at%3D16&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl%7C7599635b16674af4f8c008dbc0c7a3d0%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638315737171107260%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=v0bbxIoaVLpiuxjBYgNU4ol4mkyifDi728eE2Ke9y1I%3D&reserved=0> Memo Data IDMS.docx
<https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?url=https%3A%2F%2Fpzh-my.sharepoint.com%2Fpersonal%2 art 5 1-2e 2FDocuments%2FAVG%2FAdviezen%2FMemo%2520Data%2520IDMS.d%3Dw51745043f72e4fc8964573fab95f0dd2%26nav%3DeyJjIjoyMzY2NTQ1MzV9%26ne%3Dew0KICAidnQiOiB7DQogICAgImIiOiA3NTU1Nw0KICB9DQp9%26e%3D5Yc8bJBNYUKTFLoZci6exA%26at%3D16&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl%7C7599635b16674af4f8c008dbc0c7a3d0%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638315737171263475%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=sliXCrAJq1fecApT2QT6ypkVo9vU3HZP0%2FDYkSheSXw%3D&reserved=0>

U hebt een opmerking geplaatst

Dit leidt tot vraag waarom dat niet voor 5 oktober plaatsvindt, waarom dit zo lang duurt.. Wij melden AP toch dat de 3 gesonstateerde lekken zijn ""opgelost"".

art 5 1-2e heeft geantwoord

Zie mijn zin omtrent de tot dusver bedachte methodiek

De ernst van het datalek en de impact voor betrokkenen is afhankelijk van meerdere factoren. Het hangt onder meer af van het aantal betrokkenen, de aard van de persoonsgegevens en of daadwerkelijk ongeoorloofde toegang heeft plaatsgevonden. PZH voert op dit moment met een interdisciplinair team een onderzoek uit naar de omvang van het gemelde datalek en de mogelijke impact daarvan voor betrokkenen. PZH onderzoekt in hoeverre documenten met de gemelde trefwoorden vrij toegankelijk zijn en of, en

Ga naar opmerking <https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?url=https%3A%2F%2Fpzh-my.sharepoint.com%2Fpersonal% art 5 1-2e %2FDocuments%2FAVG%2FAdviezen%2FMemo%2520Data%2520IDMS.docx%3%3Dw51745043f72e4fc8964573fab95f0dd2%26nav%3DeyJjIjoyMzY2NTQ1MzV9%26ne%3Dew0KICAidnQiOiB7DQogICAgImIiOiA3NTU1Nw0KICB9DQp9%26e%3D5Yc8bJBNYUKTFLoZci6exA%26at%3D16&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl%7C7599635b16674af4f8c008dbc0c7a3d0%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638315737171263475%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=sliXCrAJq1fecApT2QT6ypkVo9vU3HZP0%2FDYkSheSXw%3D&reserved=0>
Waarom ontvang ik deze melding van Office?
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgo.microsoft.com%2Ffwlink%2F%3Flinkid%3D2113319&data=05%7C01 art 5 1-2e art 5 1-2e %40pzh.nl%7C7599635b16674af4f8c008dbc0c7a3d0%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638315737171263475%7CUnknown

%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=uoklQbxR%2BnFzhn4aeJCupWaPQ6CQD3mNLgvDsXn1hkw
%3D&reserved=0>

Privacyverklaring <https://eur03.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fprivacy.microso
%2Fprivacystatement&data=05%7C01 art 5 1-2e art 5 1-2e 40pzh.nl
%7C7599635b16674af4f8c008dbc0c7a3d0%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638315737171263475%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=FMZLhLf8w8sjhkQ5B0EbXuTtRE5Kanxt1Ka4QKwLRjM
%3D&reserved=0> | Instellingen voor meldingen
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fpzh-
my.sharepoint.com%2Fpersonal%2 art 5 1-2e F layouts
%2F15%2Fonedrive.aspx%3Fp%3D22&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7C7599635b16674af4f8c008dbc0c7a3d0%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638315737171263475%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=x9YuzaXumypG3x9JacQRuU0pQYAMvQCw24Qwr6Fa%2Bnk
%3D&reserved=0>
<https://westeuroper-notifyp.svc.ms:443/api/v2/tracking/method/View?
mi=5Yc8bJBNYUKTFLoZci6exA> "

https://autoriteitpersoonsgegevens.nl/nl/nieuws/de-registers-van-de-rdw-bevatten-persoonsgegevens-%C2%A0
Website AP persbericht 17-01-2000

Kentekens van motorvoertuigen zijn in elk geval persoonsgegevens **voor degenen die toegang hebben tot het kentekenregister van de Rijksdienst voor het Wegverkeer**. Zij kunnen immers de tenaamstelling van het kenteken zonder bijzondere inspanning te weten komen. Het behoeft geen betoog dat bij uitstek de RDW zelf die mogelijkheid heeft. De conclusie is dat kentekens bij de RDW persoonsgegevens zijn. Dit geldt ook voor daaraan gerelateerde gegevens, zoals de overige voertuiggegevens.

Evaluatiepunten datalek warmtebedrijf

- Incident per e-mail door art 5 1-2e gemeld;
  - Praktisch puntje: hoe registreren in Topdesk? En hoe te koppelen aan de datalek registratie?

- Onduidelijkheid over integriteitsmelding
  - Parallel aan het datalek onderzoek werd een melding gedaan. Deze werd niet bestempeld als integriteitsmelding. Werd in eerste instantie als potentieel datalek beschouwd art 5 1-2e Benodigde informatie kwam niet los (namen en document). Onduidelijkheid over de afhandeling, rollen en verantwoordelijkheden. Concreet: door art 5 1-2e art 5 1-2e privacyteam wordt dan gelopen op integriteit.

- Grensvlak datalek versus schending van geheimhouding c.q. integriteit
  - Onderzoek van audit log leidt tot vragen over schending van geheimhouding.
  - Welke procedure volgen? Wie bepaalt? Wie is eindstation: art 5 1-2e art 5 1-2e
  - Mag datalekteam überhaupt de audit log raadplegen?
  - Is vrijwaring onderzoekers nodig of voldoende om de namen in het advies te noemen?

- Betrof een beperkt toegankelijk dossier met geheime stukken.
  - Wie krijgt vanuit datalekteam toegang tot de geheime stukken en op welke basis is dat?
  - Wie die doet de beoordeling op of er een datalek is? Zijn de criteria helder?
    - Eerste conclusie FG op 20/5 was: geen datalek. Is later herroepen.

- Beschouwen gevolgen van melden van datalek bij AP/betrokkenen versus aandacht en politiek/bestuurlijke reuring die dat oplevert.

- Wordt melder betrokken bij vervolg of krijgt hij terugkoppeling en van wie?

- Managen van verwachtingen en communicatie; ging dat goed?
  Er moet een goede reden zijn om melding te maken van een datalek in een terugkoppeling van de GS-vergadering. Die lijkt hier echt wel te ontbreken.

Van: " art 5 1-2e < art 5 1-2e @pzh.nl >
Datum: 14 mei 2019 om 17:43:13 CEST
Aan: " art 5 1-2e art 5 1-2e < art 5 1-2e @pzh.nl >, " art 5 1-2e < art 5 1-2e @pzh.nl >, " art 5 1-2e < art 5 1-2e @pzh.nl >
Kopie: " art 5 1-2e < art 5 1-2e @pzh.nl >, art 5 1-2e @pzh.nl >, " art 5 1-2e <j. art 5 1-2e @pzh.nl >
Onderwerp: Antw.: Onderzoek beveiligingsincident c.q. datalek

Hoi art 5 1-2e art 5 1-2e

In de GS terugkoppeling staat:

Gedeputeerde Baljeu meldt vervolgens een datalek in Warmtedossier in IDMS. Er blijken mensen (intern) bij geheime stukken te kunnen die officieel geen toegang hebben. Betreft technische fout in het systeem, is hersteld.
Het College bespreekt de zwakke punten van IDMS.

IDMS lijkt de boosdoener. Dat staat toch niet vast? Kan roch ook aan de mens liggen. En er staat dat er een datalek is. Ook dat klopt toch niet. Dat wordt toch onderzocht? Als het klopt wat ik zeg dan aandacht aan besteden in rapportage anders ontstaat een nieuwe werkelijkheid.

Groet,
art 5 1-2e

"Van: art 5 1-2e
Verzonden: 2019-01-14 12:54:38+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Flow PZH procedure datalek.pptx
"
""Flow PZH procedure datalek.pptx"" kan via de volgende koppeling worden geopend: http://idms/otcs/llisapi.dll/properties/PZH-2018-672819664

Ha art 5 1-2e zeze kreeg je nog van me.
"

Van: art 5 1-2e art 5 1-2e
Verzonden: 2023-09 +00:00
Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: FW: Additioneel onderzoek iDMS nav zeer ernstig datalek
"
Op basis van het fa- wob account:

1e zoekopdracht:

Privacy-gevoelige Zoektermen iDMS

* BSN
* Burgerservicenummer
* IBAN
* Rekeningnummer
* Afschrift
* Kopie+paspoort
* Kopie+identiteitsbewijs
* Kopie+rijbewijs
* Kopie+legitimatie
* Legitimatie
* Vergunningsaanvraag
* Kopie+vergunningsaanvraag
* Loonstrook
* Kopie+loonstrook
* Personeelsdossier
* Lidmaatschap+vakbond

2e zoekopdracht:

Kunnen jullie een PowerBI-visualisatie creëren van de volgende additionele zoektermen, inclusief de iDMS-locatie van de gevonden bestanden?

* curriculum+vitae
* cv
* kopie+curriculum+vitae
* kopie+cv

(verfijnen op pdf, doc, docx en msg)

* paspoort

(verfijnen op pdf, jpg, jpeg, png en msg)

* bibob+vertrouwelijk
* bibob+weigeren
* bibob+intrekken
* bibob+ernstig+gevaar
* bibob+gevaarsbeoordeling
* bibob+strafbaar
* bibob+strafbare

Is het mogelijk om dit binnen een week te realiseren? Ivm de meldingstermijn van de Autoriteit Persoonsgegevens zullen wij zeer spoedig moeten handelen.

Bij voorbaat dank!

Met vriendelijke groet,

art 5 1-2e

Privacy Officer

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e %40pzh.nl
%7Cb358a88b10cb422d601c08dbb39c4a65%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638301256095444960%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=85WBgtu1ROWl1R0ISjWZqaur0dhBAeqimMBp1DdN42A
%3D&reserved=0>

Werkdagen: ma, di, wo, do

Elke dag beter. Zuid-Holland.

"


provincie
Zuid-Holland

"Van: art 5 1-2e
Verzonden: 2019-08-30 19:07:45+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e
"CC: art 5 1-2e
art 5 1-2e
Onderwerp: FW: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"

Goedenavond art 5 1-2e art 5 1-2e en art 5 1-2e

art 5 1-2e op verzoek va n art 5 1-2e stuur ik je advies bijgaand toe. Wellicht kan je dit advies delen met collega's binnen SamEc met het doel vergellijkbare datalekken te voorkomen.

@ art 5 1-2e / art 5 1-2e is het een suggestie om dit voorbeeld met alle collega's van de provincie te delen. Ik weet uit ervaring dat diverse collega's op dezelfde wijze uitnodigingen, verslagen e.d. versturen zonder de regelgeving goed voor ogen te hebben.

Hartelijke groet

art 5 1-2e

art 5 1-2e

Senior beleidsmedewerker

Erfgoedlijn Goeree-Overflakkee/Digitalisering Cultureel Erfgoed/Monumenten

Afdeling Samenleving/Economie | bureau Cultuur en Vrije Tijd

T art 5 1-2e of art 5 1-2e

art 5 1-2e @pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>

-Wanneer u de provincie Zuid-Holland een e-mail stuurt, ontvangt u binnen 2 werkdagen een reactie en binnen twee weken een antwoord. Al uw informatie wordt vertrouwelijk behandeld. Persoons- of adresgegevens worden uitsluitend gebruikt waarvoor u ze heeft verstrekt. Uw e-mailbericht wordt op een goede en veilige manier gearchiveerd.

-Vragen kunt u stellen via het contactformulier <https://eformulieren.zuid-holland.nl/Default.aspx?scenarioID=scContact> .

Van: art 5 1-2e
Verzonden: vrijdag 30 augustus 2019 18:14
Aan: art 5 1-2e
Onderwerp: Re: Advies aan concerndirecteur in het kader van de meldplicht datalekken

art 5 1-2e

Moeten we lering uit trekken. Geldt voor ons allemaal. Wil je art 5 1-2e ook informeren?

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Fri, Aug 30, 2019 at 3:38 PM +0200, "" art 5 1-2e "
art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> > wrote:

Beste allen,

In vervolg op mijn email van afgelopen week, bijgaand het advies van onze AVG-collega's aan de concerndirecteur (= verplichting).

Groet

art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 30 augustus 2019 15:09
Aan: art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: FW: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Ter informatie.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>

Van: art 5 1-2e
Verzonden: vrijdag 30 augustus 2019 15:08
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
CC: Baljeu, J.N. <j.baljeu@pzh.nl>
Onderwerp: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Beste art 5 1-2e

Bijgaand een advies in het kader van een gemeld datalek.

De beoordeling is dat er sprake is van een datalek.

Er is sprake van een laag risico.

Het advies is niet te melden aan de AP en niet aan de betrokkenen.

De melding en het advies zijn zoals gebruikelijk opgenomen in onze administratie.

Ik hoor graag of je akkoord bent met dit advies.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>
"


provincie
ZUID HOLLAND

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Definitief

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	M19 08 02408
Datum en tijdstip van de melding	:	Dinsdag 27 augustus 15:53
Route van de melding	:	Datalek formulier

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 30-08-2019 14:55
Advies besproken met	:	art 5 1-2e (FG) art 5 1-2e art 5 1-2e privacyjurist)
Advies ter kennisgeving gedeeld met	:	art 5 1-2e

Situatie

(*korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*

De erfgoedtafel Goeree-Overflakkee is een netwerk waarin overheden, ondernemers en maatschappelijke organisaties samen beoogde doelen bereiken. Een deelnemer aan de erfgoedtafel Goeree-Overflakkee attendeerde art 5 1-2e (namens PZH betrokken bij het netwerk) op een mogelijke datalek i.v.m. een door art 5 1-2e per e-mail verstuurde uitnodiging aan de deelnemers van de erfgoedtafel. De e-mailadressen staan in het vak 'geadresseerde' en zijn daardoor voor alle geadresseerden zichtbaar. De e-mailadressen bestaan uit en voor- en achternaam van de deelnemers met meestal de vermelding van de organisatie die zij vertegenwoordigen.

Van art 5 1-2e @veero.org]
Verzonden: dinsdag 27 augustus 2019 11:13
Aan: art 5 1-2e
Onderwerp: Re: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019

Geachte art 5 1-2e

Naar aanleiding van een bestuursoverleg wil ik u hierbij attenderen op het feit dat - conform de AVG - uw organisatie onjuist handelt bij het versturen van e-mailberichten met betrekking tot de Erfgoedlijn. Er wordt geen gebruik gemaakt van de optie BCC waardoor alle e-mailadressen zichtbaar zijn voor alle ontvangers zonder dat zij hiervoor expliciet toestemming hebben gegeven.
Er is dus sprake van een zgn. datalek, naar alle waarschijnlijkheid zou dit door u als versturende partij moeten worden gemeld worden bij de Autoriteit Persoonsgegevens.
Erop vertrouwend u hiermee van dienst te zijn verblijf ik.
Met vriendelijke groet,
Secretariaat VEERO

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	76 e-mailadressen

Vraag	Antwoord
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	De 76 geadresseerden
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen en kopiëren van de e-mailadressen
Welke persoonsgegevens betreft het?	E-mailadres
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Nee, de e-mail was gericht aan de deelnemers van de erfgoedtafel.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Het voor de deelnemers aan het netwerk zichtbaar zijn van de e-mailadressen levert geen hoog risico op. Dit geldt evenzeer voor de inhoud van de uitnodiging.
Betreft het een beveiligingsincident?	Ja.
Betreft het een datalek?	Ja. Het ging hier om een uitnodiging voor een bijeenkomst. Voor het overbrengen van de boodschap aan elk van de deelnemers is het niet noodzakelijk dat iedereen ieder anders e-mailadres kan zien. Ook hebben de betrokkenen geen expliciete toestemming gegeven voor het op deze wijze gebruiken van hun e-mailadres. Strikt genomen is het daarom een inbreuk in verband met persoonsgegevens, beter bekend als: datalek.
Ondernomen beperkende maatregelen.	Geen.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Geen.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

<u>Analyse van dit specifieke geval</u>
De e-mailadressen van de deelnemers aan het netwerk erfgoedtafel zijn zichtbaar geweest voor alle deelnemers. Omdat betrokkenen hiervoor geen expliciete toestemming hebben gegeven en het openbaar maken van de e-mailadressen strikt gezien niet nodig is voor het overbrengen van de uitnodiging, is er sprake van een datalek.
Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. Dat is hier niet het geval. De inhoud van de mail is niet gevoelig (een uitnodiging voor een bijeenkomst van project Erfgoedlijn Goeree-Overflakkee) en alle geadresseerden maken zelf deel uit van dit netwerk. Om dezelfde reden hoeft dit datalek ook niet aan betrokkenen te worden gemeld.

Advies
De conclusie is dat er sprake is van een datalek. Het advies is om dit datalek niet te melden aan de Autoriteit Persoonsgegevens en niet aan betrokken personen.


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-08-30 15:08:59+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: FW: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Ter informatie.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>

Van: art 5 1-2e
Verzonden: vrijdag 30 augustus 2019 15:08
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
CC: Baljeu, J.N. <j.baljeu@pzh.nl>
Onderwerp: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Beste art 5 1-2e

Bijgaand een advies in het kader van een gemeld datalek.

De beoordeling is dat er sprake is van een datalek.

Er is sprake van een laag risico.

Het advies is niet te melden aan de AP en niet aan de betrokkenen.

De melding en het advies zijn zoals gebruikelijk opgenomen in onze administratie.

Ik hoor graag of je akkoord bent met dit advies.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>
"


provincie
ZUID HOLLAND

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Definitief

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	M19 08 02408
Datum en tijdstip van de melding	:	Dinsdag 27 augustus 15:53
Route van de melding	:	Datalek formulier

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 30-08-2019 14:55
Advies besproken met	:	art 5 1-2e (FG art 5 1-2e art 5 1-2e privacyjurist)
Advies ter kennisgeving gedeeld met	:	art 5 1-2e

Situatie

(*korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*

De erfgoedtafel Goeree-Overflakkee is een netwerk waarin overheden, ondernemers en maatschappelijke organisaties samen beoogde doelen bereiken. Een deelnemer aan de erfgoedtafel Goeree-Overflakkee attendeerde art 5 1-2e (namens PZH betrokken bij het netwerk) op een mogelijke datalek i.v.m. een door art 5 1-2e per e-mail verstuurde uitnodiging aan de deelnemers van de erfgoedtafel. De e-mailadressen staan in het vak 'geadresseerde' en zijn daardoor voor alle geadresseerden zichtbaar. De e-mailadressen bestaan uit en voor- en achternaam van de deelnemers met meestal de vermelding van de organisatie die zij vertegenwoordigen.

Van art 5 1-2e @veero.org]
Verzonden: dinsdag 27 augustus 2019 11:13
Aan: art 5 1-2e
Onderwerp: Re: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019

Geachte art 5 1-2e

Naar aanleiding van een bestuursoverleg wil ik u hierbij attenderen op het feit dat - conform de AVG - uw organisatie onjuist handelt bij het versturen van e-mailberichten met betrekking tot de Erfgoedlijn. Er wordt geen gebruik gemaakt van de optie BCC waardoor alle e-mailadressen zichtbaar zijn voor alle ontvangers zonder dat zij hiervoor expliciet toestemming hebben gegeven.
Er is dus sprake van een zgn. datalek, naar alle waarschijnlijkheid zou dit door u als versturende partij moeten worden gemeld worden bij de Autoriteit Persoonsgegevens.
Erop vertrouwend u hiermee van dienst te zijn verblijf ik.
Met vriendelijke groet,
Secretariaat VEERO

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	76 e-mailadressen

Vraag	Antwoord
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	De 76 geadresseerden
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen en kopiëren van de e-mailadressen
Welke persoonsgegevens betreft het?	E-mailadres
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Nee, de e-mail was gericht aan de deelnemers van de erfgoedtafel.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Het voor de deelnemers aan het netwerk zichtbaar zijn van de e-mailadressen levert geen hoog risico op. Dit geldt evenzeer voor de inhoud van de uitnodiging.
Betreft het een beveiligingsincident?	Ja.
Betreft het een datalek?	Ja. Het ging hier om een uitnodiging voor een bijeenkomst. Voor het overbrengen van de boodschap aan elk van de deelnemers is het niet noodzakelijk dat iedereen ieder anders e-mailadres kan zien. Ook hebben de betrokkenen geen expliciete toestemming gegeven voor het op deze wijze gebruiken van hun e-mailadres. Strikt genomen is het daarom een inbreuk in verband met persoonsgegevens, beter bekend als: datalek.
Ondernomen beperkende maatregelen.	Geen.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Geen.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

<u>Analyse van dit specifieke geval</u>
De e-mailadressen van de deelnemers aan het netwerk erfgoedtafel zijn zichtbaar geweest voor alle deelnemers. Omdat betrokkenen hiervoor geen expliciete toestemming hebben gegeven en het openbaar maken van de e-mailadressen strikt gezien niet nodig is voor het overbrengen van de uitnodiging, is er sprake van een datalek.
Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. Dat is hier niet het geval. De inhoud van de mail is niet gevoelig (een uitnodiging voor een bijeenkomst van project Erfgoedlijn Goeree-Overflakkee) en alle geadresseerden maken zelf deel uit van dit netwerk. Om dezelfde reden hoeft dit datalek ook niet aan betrokkenen te worden gemeld.

Advies
De conclusie is dat er sprake is van een datalek. Het advies is om dit datalek niet te melden aan de Autoriteit Persoonsgegevens en niet aan betrokken personen.

"Van: art 5 1-2e
Verzonden: 2019-11-14 17:36:45+00:00
"Aan: art 5 1-2e
"CC: Zoete - van der Hout, WH, de; art 5 1-2e
Onderwerp: FW: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Ha art 5 1-2e

Dankjewel voor het heldere advies, ik neem het integraal over,

Hartelijke groet, art 5 1-2e

Van: art 5 1-2e
Verzonden: donderdag 14 november 2019 11:27
Aan: art 5 1-2e
CC: Zoete - van der Hout, WH, de; art 5 1-2e
Onderwerp: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Beste art 5 1-2e

Bijgaand het advies van het privacyteam in het kader van een gemeld datalek.

De beoordeling is dat er sprake is van een datalek.

Er is sprake van een laag risico.

Het advies is niet te melden aan de AP en niet aan de betrokkenen.

De melding en het advies zijn afgestemd met onze FG en zoals gebruikelijk opgenomen in onze administratie.

Ik hoor graag of je akkoord bent met dit advies.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>
"


provincie
ZUID HOLLAND

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Definitief

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	M19 11 01654
Datum en tijdstip van de melding	:	Dinsdag 12 november 2019 14:43
Route van de melding	:	Datalek formulier

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Woensdag 13 november 2019
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e privacy jurist)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerker e art 5 1-2e coördinator FZ)

Situatie

(*Korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*
Op 24 oktober 2019 is vanuit Het Loket een mail verstuurd naar 439 medewerkers van PZH in verband met hun OV-chipkaart. De e-mailadressen staan in het vak 'geadresseerde' en zijn daardoor voor alle geadresseerden zichtbaar. In 59 gevallen gaat het om het persoonlijke e-mailadres van de PZH-medewerker. Eén van deze medewerkers heeft hierover op 12 november 2019 geklaagd bij de FG.
De melding is mondeling gedaan aan de FG PZH en door de FG vervolgens geregistreerd in Topdesk

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	59 privé e-mailadressen
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	380 geadresseerde collega's hebben de privé e-mailadressen van 59 collega's kunnen zien.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen
Welke persoonsgegevens betreft het?	E-mailadres
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot	Ja. Alle geadresseerden zijn provinciale medewerkers.

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.

Vraag	Antwoord
personeel van PZH? Zo ja, tot welke gebruikersgroepen?	
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Het voor collega's zichtbaar zijn van privé e-mailadressen wordt niet beoordeeld als een hoog risico voor de betrokkenen.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja, in relatie tot de vertrouwelijkheid van de 59 privé e-mailadressen. Niet ten aanzien van de 380 provinciale e-mailadressen
Betreft het een datalek?	Ja. Voor het overbrengen van de boodschap aan elk van de geadresseerden is het niet noodzakelijk dat privé e-mailadressen voor collega's zichtbaar gemaakt worden. Ook hebben de betrokkenen geen expliciete toestemming gegeven voor het op deze wijze kenbaar maken van hun privé e-mailadressen. Onrechtmatige verwerking (misbruik van de privé e-mailadressen) door PZH-collega's achten wij onwaarschijnlijk, maar kan niet uitgesloten worden, zodat er strikt genomen sprake is van een inbreuk in verband met persoonsgegevens, beter bekend als: datalek.
Ondernomen beperkende maatregelen.	De FG heeft de coördinator van Het Loket geïnstrueerd voortaan de geadresseerden in het Bcc-veld op te nemen, zodat deze niet zichtbaar zijn voor de ontvangers. Deze instructie is overigens ook te vinden op de AVG-pagina op het Binnenplein.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Verdere maatregelen zijn niet nodig.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

Een aantal privé e-mailadressen van provinciale collega's is zichtbaar geweest voor de andere geadresseerden van de e-mail. Betrokkenen hebben hiervoor geen expliciete toestemming gegeven en het openbaar maken van de e-mailadressen strikt gezien niet nodig is voor het overbrengen van de boodschap. Onrechtmatige verwerking (het misbruik maken van de privé e-mailadressen) door PZH-collega's achten wij onwaarschijnlijk en het hiermee verbonden risico voor de betrokkenen niet hoog. Ook de inhoud van de e-mail is niet gevoelig en geeft geen aanleiding tot misbruik.
Onrechtmatige verwerking is echter niet uit te sluiten, zodat er volgens de AVG wel sprake is van een inbreuk in verband met persoonsgegevens, beter bekend als: datalek.

Conclusie en advies

Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. Dat is hier naar ons oordeel niet het geval.

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert het Privacyteam om:

- Het datalek niet te melden bij de Autoriteit Persoonsgegevens.
- Het datalek niet te melden bij de betrokkenen.
- De melding en beoordeling zoals gebruikelijk te administreren in het provinciale logboek.

"Van: art 5 1-2e
Verzonden: 2020-05-11 10:19:18+00:00
"Aan: art 5 1-2e
"CC: Zoete - van der Hout, WH, de; art 5 1-2e
Onderwerp: FW: Advies datalek
"
Ha art 5 1-2e

Graag akkoord met je advies en ik ben blij met de vermelde herstelmaatregelen/verbeteracties. Dit is wel een dingetje zeg

Hartelijke groet, art 5 1-2e

PS. Managerial vind ik hier wel wat van, mag ik van je horen om welk bureauhoofd het gaat? Ik wil daar graag even contact mee leggen.

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: maandag 11 mei 2020 09:58
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
CC: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Advies datalek
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste art 5 1-2e

Bijgaand het advies m.b.t. het datalek van vrijdag jl.

Het advies is afgestemd met onze FG en zoals gebruikelijk opgenomen in onze administratie.

Ik hoor graag of je hiermee instemt.

Na jouw besluit kunnen we de voorlopige melding die ik afgelopen vrijdag heb gedaan bij de AP intrekken, aanpassen of definitief maken.

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 8 mei 2020 18:45
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
CC: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: Aankondiging datalek

Voorlopige melding bij AP gedaan:

Tijdstip ontvangst

08-05-2020 18:41:34

Uniek nummer

art 5 1-2e

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 8 mei 2020 17:16
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >

CC: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
<art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Aankondiging datalek

Hallo art 5 1-2e

Na een melding te hebben ontvangen, heb ik in de loop van de middag de datalek procedure gestart.

Ik ben met het privacy team nog bezig aan het advies.

Je ontvangt dit uiterlijk maandagochtend, nadat het door betrokkene en privacy team is gezien.

Wij zullen je in het advies adviseren om het te beschouwen als een datalek en het datalek te melden aan de AP.

Om binnen de wettelijke termijn te blijven, zal ik vast een voorlopige melding bij de AP doen.

Na jouw besluit kunnen we deze melding intrekken, aanpassen of definitief maken.

Situatie:

Het betreft een interne zaak waarbij een collega in Microsoft Teams een opname heeft gemaakt van een telefoongesprek dat een andere collega met haar teamleider had.

In de opname komen persoonlijke zaken voor.

De opname is door 1 persoon gemaakt en potentieel door 8 collega’s af te luisteren.

Er wordt nog gezocht naar een manier om de opname uit Teams te verwijderen, maar dat blijkt niet eenvoudig.

Ik doe dit in het advies verder uit de doeken.

Mocht je op voorhand vragen hebben dan hoor ik het uiteraard graag.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>
"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Concept

Melding gegevens

Naam melder	:	art 5 1-2e betrok kene)
Registratienummer van het incident	:	M20 05 00547
Datum en tijdstip van de melding	:	Vrijdag 8 mei 2020 14:39
Route van de melding	:	E-mail

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Maandag 11 mei 2020 09:30
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e (privacy jurist)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerker

Voorlopige melding gedaan bij de Autoriteit Persoonsgegevens:

Tijdstip ontvangst: 08-05-2020 18:41:34

Uniek nummer: art 5 1-2e

Situatie

(*Korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*

Betrokkene voerde per telefoon een gesprek met haar teamleider, waarin ook vertrouwelijke zaken werden besproken.

Tijdens het telefoongesprek probeerde betrokkene een Teams chat met deze teamleider te starten, zodat ze elkaar ook konden zien. Daar ging iets mis, want ze startte per ongeluk een vergadering met een Team waar ze deel van uit maakt. De microfoon van de laptop stond daarbij open.

Omdat betrokkene en teamleider elkaar niet te zien kregen hebben ze het gesprek verder telefonisch gedaan.

Een ander lid van dat Team zag dat er een vergadering werd geopend en kwam (op de laptop) in die chat. De collega kon - doordat de microfoon en camera van de laptop open stonden - meeluisteren met het telefoongesprek. Betrokkene had dit niet in de gaten.

Een deel van het gesprek ging over persoonlijke aangelegenheden. Het meeluisterende teamlid heeft daar niet alleen in meegeluisterd, maar daar ook in Teams een opname van gemaakt.

Hij heeft dat later per e-mail bij betrokkene gemeld.

Het opgenomen audio gesprek staat opgeslagen in de chat waar de andere teamleden ook bij kunnen. Dit audio gesprek kan daar niet uit worden verwijderd. Automatisch gebeurt dit wel maar pas na 20 dagen.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Betreft een gesprek.

Vraag	Antwoord
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	1 persoon heeft meegeluisterd en een opname gemaakt. 8 collega's hebben potentieel toegang tot de opname.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Luisteren en opname
Welke persoonsgegevens betreft het?	Persoonlijk gesprek tussen betrokkene en teamleider, onder meer over de samenwerking met een collega.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja. Directe collega's.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Ja. Betreft het uitlekken van een persoonlijk gesprek. De samenwerking tussen collega's kan onder druk komen te staan. Betrokkene voelt zich aangetast in haar persoonlijke levenssfeer. Haar vertrouwen is geschaad.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja, in relatie tot de vertrouwelijkheid van de informatie.
Betreft het een datalek?	Ja. Deze informatie is bij de verkeerde persoon terecht gekomen.
Ondernomen beperkende maatregelen.	Het opgenomen audiogesprek staat in de chat waar de andere teamleden ook bij kunnen. Door de I&A Teams beheerder is gepoogd de opname uit de chat te verwijderen. Dit bleek niet mogelijk. Automatisch gebeurt dit wel maar pas na 20 dagen. De collega die de opname heeft gemaakt is Teamlid is hierop aangesproken door het bureauhoofd.

[1] Art.9 AVG: Gegevens over ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

Vraag	Antwoord
	Het bureauhoofd heeft in de chat een bericht geplaatst over het niet afluisteren van de opname.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	De I&A beheerder van Teams is op zoek naar een manier om het audio gesprek weg te halen, misschien door de hele chat te verwijderen als dat kan. I&A doet onderzoek naar de wenselijkheid en voorwaarden van het maken van opnamen in Teams, om te zorgen dat de privacy van de Teams gebruikers niet wordt geschaad. In de Teams training dient aandacht te worden besteed aan de gevaren van het ongemerkt openzetten van camera en microfoon. In de communicatiecampagne Data Donderdag zal aandacht worden besteed aan zorgvuldig gebruik van Teams en het maken van opnamen.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.

- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval
Er is sprake van een datalek, omdat er persoonsgegevens in verkeerde handen zijn gekomen.
Gezien de vertrouwelijke aard van de informatie en omdat het de directe werkkring van betrokkene betreft, achten wij het hiermee verbonden risico voor aantasting van de persoonlijke levenssfeer van betrokkene hoog.

Conclusie en advies
Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. Dat is hier naar ons oordeel wel het geval. Het betreft informatie die de positie van betrokkene in de directe werksituatie kan schaden.

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert het Privacy team om:

- De datalek melding en beoordeling zoals gebruikelijk te administreren in het provinciale logboek.
- Het datalek te melden bij de Autoriteit Persoonsgegevens.

Het datalek is besproken met direct betrokkenen, zodat verdere actie hier niet nodig is.


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2020-07-09 16:28:59+00:00
"Aan: art 5 1-2e
"CC: Zoete - van der Hout, WH, de"
Onderwerp: FW: advies in het kader van de meldplicht datalekken
"
Hoi art 5 1-2e

Wat een vervelend incident zeg. Ik volg je advies. Bij het melden aan betrokkenen graag hen ook melden welke herstelacties zijn/worden genomen natuurlijk.

Je stelt een drietal herstelacties voor, terecht mijns inziens. Gezien de aard van dit incident wil ik op 15 september graag gerapporteerd krijgen hoe en wanneer deze herstelacties zijn uitgevoerd. Wil je dat ajb aan de betreffende actiehouders doorgeven.

Hartelijke groet, art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: donderdag 9 juli 2020 15:51
Aan: art 5 1-2e <art 5 1-2e pzh.nl>
CC: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl>
Onderwerp: advies in het kader van de meldplicht datalekken
Urgentie: Hoog

Beste art 5 1-2e

Hierbij een advies in het kader van het melden van een datalek.

Het betreft hier een melding van een Statenlid die bij mij is ingediend. Ik heb met dit lid afgesproken om het zelf af te handelen.

art 5 1-2e is in globale zin op de hoogte van het datalek.

Met vriendelijke groet,

art 5 1-2e

Functionaris voor Gegevensbescherming

M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>

-Wanneer u de provincie Zuid-Holland een e-mail stuurt, ontvangt u binnen 2 werkdagen een reactie en binnen twee weken een antwoord. Al uw informatie wordt vertrouwelijk behandeld. Persoons- of adresgegevens worden uitsluitend gebruikt waarvoor u ze heeft verstrekt. Uw e-mailbericht wordt op een goede en veilige manier gearchiveerd.

-Vragen kunt u stellen via het contactformulier <https://www.zuid-holland.nl/contact/contactinformatie/> .
"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: CONCEPT

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	
Datum en tijdstip van de melding	:	08-07-2020 10:18u
Route van de melding	:	Email melding

Advies

Opgesteld door	:	art 5 1-2e (FG)
Datum en tijdstip advies	:	09-07-2020 15:41u
Advies besproken met	:	
Advies ter kennisgeving gedeeld met	:	Het advies zal worden gedeeld met de betrokkene en de fractievoorzitter van de betreffende partij

Situatie

(*korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*
In het kader van het uitvoeren van een wettelijke regeling zijn er documenten per post verstuurd aan een fractie van PS. Deze documenten zijn door de postkamer en de scanstraat verwerkt, maar vervolgens verstuurd naar de afdeling Financiële Zaken, en vervolgens naar de salarisadministratie. Echter, het betrof hier documenten die betrekking hebben op een medewerker van een fractie, niet zijnde een medewerker van PZH. Nadat duidelijk werd dat het voor een medewerker van een fractie was, zijn de stukken vervolgens doorgestuurd naar de fractie van, helaas, een andere partij. Deze medewerker heeft de fout ontdekt en heeft vervolgens de afdeling FJZ weer ingelicht en aangegeven welke fractie wel moest worden aangesproken. Een vergelijkbaar voorval heeft zich 2-3 maart ook al voorgedaan, zo werd duidelijk gedurende het onderzoek. Het betrof daarbij dezelfde medewerker van de fractie.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	<10
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Nog niet geheel bekend, maar meer dan 10
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen, mailen
Welke persoonsgegevens betreft het?	Naam, adres, woonplaats, geboortedatum, BSN, financiële gegevens
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in	Financiële gegevens

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties,

Vraag	Antwoord
artikel 9 AVG?	
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Nee, de informatie is ook gedeeld met een medewerker van een andere fractie
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Ja, reputatieschade, identiteitsfraude, stigmatisering
Betreft het een beveiligingsincident?	Ja
Betreft het een datalek?	Ja
Ondernomen beperkende maatregelen.	Geen
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	1. Het proces in de postkamer en de scanstraat moet onder de loep worden genomen en wellicht worden aangepast. Nogmaals met de medewerkers doornemen. 2. Met de afdeling Financiën en de salarisadministratie afspraken maken over het beperken van de medewerkers die in de CC worden meegenomen. 3. Stel een aparte postbus in voor de fracties en/of geef de stichtingen een meer onderscheidende naam

Afweging

<u>Kaders</u>

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van

gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.

[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Conclusie
(*korte beschrijving van de conclusie)*
Vertrouwelijke documenten zijn niet naar de fractie gestuurd maar zijn in het concern terechtgekomen. Daar is verwarring ontstaan voor wie de documenten bestemd waren. Vervolgens zijn er circa 10 medewerkers betrokken in de mailstroom. Voordat het bij de juiste fractie beland is, zijn de documenten ook nog gestuurd naar een andere fractie. In de documenten staan zeer gevoelige gegevens van een fractiemedewerker. Dit kan mogelijk leiden tot reputatieschade, stigmatisering en/of identiteitsfraude.

Advies
De conclusie is dat er WEL sprake is van een beveiligingslek en dat er WEL sprake is van een datalek in de zin van de AVG.
Gezien de afwegingscriteria in de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679[3], komen we tot het oordeel dat:
- het datalek WEL meldingsplichtig is bij de Autoriteit Persoonsgegevens.
- er WEL melding wordt gedaan bij betrokkenen.

[3] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 – Groep Gegevensbescherming Artikel 29, versie 6 februari 2018


provincie
ZUID HOLLAND

Van: art 5 1-2e
Verzonden: 2023-09-30 17:24:32+00:00
Aan: art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: FW: Data IDMS
"

Beste art 5 1-2e en alle anderen,

Ik heb het allemaal gelezen, er een nachtje over geslapen, opnieuw gelezen, en dan nu mijn reactie. In drie punten:

1. Heel veel dank voor de gepleegde inspanning en inzet om dit op zo korte termijn op papier te krijgen door jullie!
2. Ik heb nog enkele vragen/opmerkingen bij de verschillende stukken. Die som ik hieronder op.
3. Alles overziende, zie ik dat er allerlei lopende activiteiten zijn die stukjes van de hele puzzel bevatten (informatietransitie, nieuw beleid IenA, GS-nota, BIO, e.d.). Maandag zal ik aan de orde stellen hoe we komen tot een samenhangend Plan van Aanpak / samenhangend Overzicht van de totale puzzel, met aandacht voor systemen, processen, gedrag en verantwoordelijkheden, inclusief een kalender.

Dan de uitwerking van bovenstaande punt 2:

* Memo data idsm: graag de notie toevoegen dat we meerdere zelfgecreëerde lekken netjes gaan melden + ik lees nix over de FG die de afgelopen maanden onderzoek deed en mij daarvan via een brief op de hoogte stelde + ik zoek in deze notitie of ergens anders een timeline van de afgelopen paar weken waarin we steeds opeenvolgende iteraties doen van onderzoek&actie + ik mis nog de update van de 2 tabellen vorige week in de presentatie met allerlei kolommen waarin aantal staan per zoekterm + in de paragraaf ‘verantwoordelijkheden tav idsm’ worden vanuit OGO verantwoordelijkheden geduid maar waarop is dat gebaseerd?
* Memo datalek: wat betekent ECM + in 2016 is blijkbaar besloten 6 mln uit te trekken voor vervanging idms, is dat toen ook gebeurd?
* Memo beschrijving idsm: graag aanvullen met inzicht hoe het geregeld is met rechtenbeheer/autorisaties.

Tenslotte, nogmaals veel dank. Zou het jullie mogelijk zijn maandag einde dag de genoemde opmerkingen verwerkt te hebben? Dan ga ik er dinsdag mee richting DT en gedeputeerde.

Hartelijke groet, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: vrijdag 29 september 2023 16:39
Aan: art 5 1-2e art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Data IDMS
Gevoeligheid: Vertrouwelijk

Beste art 5 1-2e

Zoals afgesproken hierbij een memo over het proces tot op heden, een blik op de te ondernemen acties en de bredere context om een en ander in perspectief te plaatsen. Daarnaast vind je als bijlagen een document over IDMS en een document over de weg naar informatietransitie aan. Tot slot de planning op hoofdlijnen t/m 5 oktober.

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art 5 1-2e art 5 1-2e %40pzh.nl %7Cb234ad4e77e84acf2ed408dbc1c958a1%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638316845165158792%7CUnknown %7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=1ziE8j5GIERjtGPJ5yR8l4DX%2FFk7Wh%2BqHXG6HT25tAE%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

"


provincie
Zuid-Holland

provincie Zuid-Holland

Memo

Contact
art 5 1-2e

art 5 1-2e @pzh.nl

Datum
29 september 2023

Aan
art 5 1-2e

Kopie aan

Onderwerp
Data IDMS

Geachte art 5 1-2e beste art 5 1-2e

In deze memo beschrijven wij op uw verzoek de stand van zaken met betrekking tot de omgang met persoonsgegevens in IDMS. De directe aanleiding voor deze memo is de melding van een datalek[1] op 7 september door de Chief Information Security Officer (CISO) van PZH. Ook in de periode voor 7 september hebben zich al datalekken voorgedaan in IDMS. De Functionaris voor Gegevensbescherming heeft in zijn jaarverslagen van 2019 en 2021 er op gewezen dat IDMS niet is ingericht op een adequate naleving van de AVG. Dit heeft zo moeten wij nu constateren niet geleid tot een voldoende besef van de gebrekkige staat van IDMS ten aanzien van AVG compliancy.

Wij beschrijven in deze memo achtereenvolgens:

1. De aanleiding voor deze memo: het datalek
2. De tot dusver ondernomen acties
3. De voorgenomen acties
4. Stand van zaken privacy en informatieveiligheid
5. Overige acties

Datalek van 7 september 2023

Op 7 september jl. ontvingen de Functionaris voor Gegevensbescherming (FG) en de eenheid Privacy (EP) van PZH een melding van de Chief Information Security Officer (CISO) dat hij waarschijnlijk ongeoorloofd toegang

1

[1] In de wet wordt een datalek als volgt gedefinieerd: *"een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens."*

heeft gehad tot persoonsgegevens in het IDMS. De CISO had middels de zoektermen “curriculum vitae”, “kopie paspoort” en “Bibob” toegang tot documenten waar hij uit hoofde van zijn functie geen toegang toe behoeft.

IDMS is het centrale document- archiefsysteem van PZH en is alleen intern toegankelijk voor alle medewerkers van PZH (ong. 2460 medewerkers d.d. 22 september '). Er is voor dit datalek geen aanleiding te veronderstellen dat persoonsgegevens onterecht buiten PZH terecht zijn gekomen.

De tot dusver ondernomen acties

Voorlopige melding bij de Autoriteit Persoonsgegevens

PZH heeft op 8 september jl. (binnen de wettelijke termijn van 72 uur) bij de Autoriteit Persoonsgegevens (AP) een voorlopige melding gedaan dat er mogelijk sprake is van een datalek dat risico’s inhoudt voor de rechten en vrijheden van betrokkenen[2]. PZH moet uiterlijk op 5 oktober as. de AP informeren of er sprake is van een datalek met risico voor betrokkenen. De EP bereidt dat voor en meldt dit na akkoord van u.

Onderzoek naar ernst datalek

De ernst van het datalek en de impact voor betrokkenen is afhankelijk van meerdere factoren. Het hangt onder meer af van het aantal betrokkenen, de aard van de persoonsgegevens en of daadwerkelijk ongeoorloofde toegang heeft plaatsgevonden. PZH voert op dit moment met een interdisciplinair team een onderzoek uit naar de omvang van het gemelde datalek en de mogelijke impact daarvan voor betrokkenen. PZH onderzoekt in hoeverre documenten met de gemelde trefwoorden vrij toegankelijk zijn en of, en zo ja wanneer, die door welke medewerkers ongeoorloofd zijn geraadpleegd. De trefwoorden waarop het onderzoek plaatsvindt leveren nog een groot aantal 'false positives' op omdat niet ieder document in IDMS waar in de trefwoorden voorkomen ook daadwerkelijk persoonsgegevens betreffen. De resultaten komen in verschillende iteraties naar boven en een definitief inzicht in de omvang en ernst wordt niet voor 5 oktober verwacht. Tot dusver is nog geen methodiek gevonden die voldoende zekerheid gaat bieden om de vraag naar omvang en impact te kunnen beantwoorden. PZH kan de AP op 5 oktober informeren over de verwachte omvang van het datalek en impact maar kan de AP niet berichten dat het datalek is opgehouden te bestaan. Uiteraard kunnen wel de tot dan getroffen mitigerende maatregelen worden gerapporteerd, de bevindingen tot dusver alsmede het verdere actieplan.

Bredere steekproef op toegankelijkheid persoonsgegevens in IDMS

Om te onderzoeken of er sprake is van een incidenteel datalek hebben de FG en EP parallel aan het lopende onderzoek een aantal steekproeven uitgevoerd in IDMS met andere trefwoorden naar persoonsgegevens in IDMS die mogelijk te ver open staan. Dit heeft tot de voorlopige conclusie geleid dat er mogelijk meer datalekken in IDMS zijn opgetreden die nog niet zijn opgemerkt en gemeld.

Onderzoek naar oorzaak van het datalek

De melding betreft informatie die onvoldoende afgeschermd stond in IDMS. Toegangsrechten tot gevoelige documenten en/of mappen moeten worden beperkt tot medewerkers die daar voor hun functie toegang toe moeten hebben. In het onderzoek is voorlopig vastgesteld dat onvoldoende gebruik is gemaakt door map-/documenteigenaren van de afschermingsmogelijkheden die IDMS biedt.

Verantwoordelijkheden t.a.v. IDMS

De verantwoordelijkheden voor informatiesystemen zijn beschreven in het Informatieveiligheidsbeleid van PZH. Er wordt onderscheid gemaakt in (1) zg. *business* applicaties die door een specifieke afdeling/opdracht voor een afgebakende taak worden ingezet en in (2) *generieke* informatiesystemen die door de hele organisatie worden gebruikt. Generieke informatiesystemen betreffen de kantoorautomatisering (email, tekstverwerking) en documentmanagement en archief zoals IDMS. Voor generieke informatiesystemen ligt volgens het informatieveiligheidsbeleid een centrale verantwoordelijkheid bij het DT c.q. concerndirecteur met uitvoering door I&A. Proceseigenaren (binnen OGO: domeindirecteuren/ambtelijk opdrachtgevers) blijven binnen generieke informatiesystemen verantwoordelijk voor de verwerking en afscherming van hun informatie. DT en

[2] Een betrokkene is degene wiens persoonsgegeven het betreft.

I&A moeten zorgdragen dat een informatiesysteem zoals IDMS beveiligingstechnisch op orde is en proceseigenaren in staat stelt hun informatie veilig te verwerken.

De voorgenomen acties

De hiervoor genoemde gebeurtenissen geven aanleiding tot een structureler onderzoek naar de omgang met persoonsgegevens in systemen van PZH.

Doorzoeking van IDMS op ongeoorloofde toegangsmogelijkheden

PZH gaat IDMS risico gebaseerd[3] doorzoeken op mogelijk ongeoorloofde toegangsmogelijkheden voor medewerkers tot privacygevoelige informatie. Leidt dit onderzoek tot de conclusie dat medewerkers toegang hebben tot privacygevoelige informatie die zij niet nodig hebben in hun functie dan worden de autorisaties gecorrigeerd. Daarnaast worden er logbestanden gecontroleerd om te zien of er ongeoorloofd toegang is verkregen tot documentatie met in afstemming met HR en P-manager zo nodig passende acties jegens de medewerker.

Onderzoek naar andere systemen die persoonsgegevens bevatten

Daarnaast is PZH gestart met een voorbereidend onderzoek naar andere systemen die mogelijke persoonsgegevens bevatten. Op advies van de FG worden twee informatiesystemen die ook (ongestructureerde) documenten bevatten aan het vervolgonderzoek toegevoegd (MS TEAMS en MS Sharepoint).

Stand van zaken privacy en informatieveiligheid PZH

PZH heeft de afgelopen jaren de inspanning op het gebied van privacy en informatieveiligheid en geïntensiveerd.

De EP is in juni 2022 opgericht om het privacy volwassenheidsniveau van PZH te verbeteren. Op dat moment bleek uit een onderzoek van de eenheid Audit en Advies dat het volwassenheidsniveau zich nabij de 1 bevond. Een niveau van 3 is minimaal gewenst om aantoonbaar aan de AVG te kunnen voldoen. PZH heeft zich ten doel gesteld dit niveau in 2025 bereikt te hebben. De EP heeft zich gericht op het ontwikkelen van een organisatie breed privacy beleid. Dit is enige tijd geleden voorgelegd aan het DT en bevindt zich in fase richting vaststelling door GS. Daarnaast is de EP onder meer actief om het privacy bewustzijn binnen PZH te vergroten, het register van verwerkingen up-to-date te krijgen en de achterstand met betrekking tot het uitvoeren van Data Protection Impact Assessments in te halen. De EP constateert dat er op onderdelen binnen PZH nog onvoldoende urgentie wordt gevoeld voor het belang en (verplichte) karakter van de AVG.

Informatieveiligheid heeft een bredere taak dan het beschermen van persoonsgegevens en heeft betrekking op de algehele beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening van PZH. Informatieveiligheid raakt onderwerpen zoals governance en verantwoordelijkheden, IT, security testen, personeel, bewustwording en fysieke beveiliging.

In 2022 is een CISO betrokken en is er geïnvesteerd om aantoonbaar aan de verplichte Baseline Informatiebeveiliging Overheid (BIO), de interprovinciaal afgesproken ISO 27001, en straks de NIS2, te voldoen. Vanaf 2022 is de implementatie van de ISO 27001 projectmatig vormgegeven en het strategische informatieveiligheidsbeleid is geactualiseerd. Tactische beleidsdocumenten zijn eveneens geactualiseerd of ontwikkeld, zoals wachtwoordbeleid of risicomanagementbeleid. PZH voert regelmatig pentesten uit. Momenteel wordt er een aanbesteding voor een IT-monitoring, detectie en responsedienst voorbereid om de incidentresponse van de provincie te verbeteren. Daarnaast neemt PZH deel aan alle interprovinciale ontwikkelingen op het gebied van informatieveiligheid, zoals het IP CSIRT, waardoor provincies dreigingsinformatie vanuit het NCSC kunnen ontvangen.
De BIO en de ISO zijn nog niet aantoonbaar in de hele organisatie geïmplementeerd. Het gestelde doel van volwassenheidsniveau 3 wordt naar verwachting eind 2024 aantoonbaar bereikt. Implementatie van nieuw vastgesteld beleid en werkwijzen, het uitvoeren van bredere recovery testen en crisisoefeningen, versterken van

[3] PZH start het onderzoek met de meest privacy gevoelige informatie zoals bijzondere persoonsgegevens.

het ISMS (PDCA-cyclus voor informatieveiligheid) en het uitbreiden van trainingen en bewustwording zijn nog belangrijke aandachtspunten.

Overige acties

Voorgestelde beleidsaanpassing 'open tenzij'

Op 14 september '23 heeft het AOG I&A op voorstel van de CISO ingestemd met een beleidsaanpassing voor de informatiehuishouding van 'open tenzij', naar 'gesloten tenzij'. Het voorstel wordt binnenkort aangeboden aan het DT ter vaststelling. PZH heeft momenteel een op de uitgangspunten van 'open tenzij'-gebaseerde informatievoorziening. Dit betekent dat alle informatie voor alle PZH-medewerkers toegankelijk zijn, *tenzij* de documenten actief worden afgeschermd. Dit is foutgevoelig en kan daarmee leiden tot risico's voor de bescherming van persoonsgegevens en andere gevoelige informatie. Het voorstel is om alle informatiesystemen, waar mogelijk, in te richten zodat informatie in beginsel niet voor alle PZH-medewerkers beschikbaar is, *tenzij* deze actief (door een handeling) worden opgesteld. Dit is in lijn met het uitgangspunt van de AVG dat persoonsgegevens alleen mogen worden verwerkt als dat noodzakelijk is.

Bewustwordingscampagne(s)

In 2019 is na een 0-meting een eerste campagne, “Up to data”, geïnitieerd door I&A in samenwerking met bestuur (AVG, Woo en provinciaal archivaris) en P&O (integriteit). De onderwerpen van deze campagne zijn: Data- en informatiekwaliteit, Informatie veiligheid, Privacy, Informatiebeheer en Integriteit. In 2021 is er door EAA een 1-meting uitgevoerd over de bewuste omgang met informatie, de resultaten daarvan zijn gebruikt om te komen tot een nieuwe campagne, “Zo doen we dat”, die binnenkort van start gaat. In deze campagne wordt er vanuit gedragsleer gekeken naar wat er nodig is om mensen het ‘gewenste gedrag’ te laten vertonen.

Informatietransitie

31 januari jl. heeft GS besloten 23 miljoen toe te kennen, over een periode van 6 jaar) aan het programma Informatietransitie. Hoe de weg is verlopen naar deze mijlpaal, is te vinden in de bijlage.
In de voorafgaande “visie op een toekomstbestendig informatiebeheer” is vastgesteld dat er een aantal zaken ernstig te kort schiet binnen PZH. Ook is er een aanzet gegeven tot een programmalijn om te komen tot een toekomstbestendig informatiebeheer. Een belangrijke notie daarin: als organisatie ben je hier nooit mee ‘klaar’.

In actielijn 1 ‘Bewustzijn en vaardigheden verhogen’ bevorderen we een cultuur waarin medewerkers gaan handelen in lijn met de kaders van ‘goed’ informatiebeheer en data/informatie-gedreven werken. Initiëren en ondersteunen van activiteiten die het
I-bewustzijn bevorderen en bijdragen aan het gewenste gedrag van directie, regisseurs, managers en medewerkers.

In actielijn 2 ‘Opzetten I-governance en I–control & optimaliseren werkwijze’ zorgen we voor de juiste sturende en ondersteunende processen om risico’s te vermijden en waarde te verhogen. Ontwerpen en implementeren van een I-governance en gesloten
I-control-cyclus & het ontwikkelen van kaders en een werkwijze die bijdragen aan het sturen op gewenste resultaten.

In actielijn 3 ‘Saneren en moderniseren IV-middelen, platformen en informatie’ zorgen we voor een adequaat instrumentarium voor het toekomstbestendig informatiebeheer en data/informatiegedreven werken. Saneren en verbeteren van middelen en informatie, zodat daarmee de strategische doelen meer passend ondersteund worden.

Tot slot

PZH onderzoekt verder welke andere acties effectief en nuttig kunnen zijn om het risico op datalekken te verminderen. Duidelijk is wel dat proces-/systeemeigenaren actiever op hun rol en verantwoordelijkheden moeten worden aangesproken. Voor advies en ondersteuning bij de invulling van hun rol kunnen zij terecht bij

de EP en CISO. Daarnaast moet het privacy bewustzijn bij proceseigenaren en medewerkers worden vergroot. Hierover informeren wij u op een ander moment nader.

art 5 1-2e (EP)
art 5 1-2e Communicati e)
art 5 1-2e FB IDMS)
art 5 1-2e (CISO)
art 5 1-2e art 5 1-2e BI)
art 5 1-2e I&A)
art 5 1-2e I&A)

Stappen gezet afgelopen jaren sinds ongeveer 2013

Dit overzicht pretendeert zeker niet volledig te zijn, het geeft 'slechts' een impressie weer van een aantal onderzoeken, initiatieven en uitgevoerde activiteiten in de afgelopen jaren.

Audit - Eenheid Audit & Advies (EAA), 2013

De afdeling I&A heeft in 2013 het bureau Eenheid Audit en Advies (EAA) een onderzoek naar het informatiebeheer laten uitvoeren. Op grond van de uitkomsten en gedane aanbevelingen is veel energie gestoken in het opschonen van de dossiers en het overbrengen van kennis op ambtenaren in de zogenaamde 'week van het e-dossier'.

ECM visie door Cap Gemini, 2015

ECM is er primair op gericht om de levenscyclus van ongestructureerde informatie (van initiële creatie via bijvoorbeeld publicatie tot aan archivering en vernietiging) te ondersteunen. Belangrijke aspecten hierbij zijn het terugvinden van de betreffende content, en het bewaken van de integriteit ervan. Het resultaat hiervan is efficiëntie en transparantie voor de medewerker en de organisatie.

Governance en Compliancy

Compleet inzicht in de aanwezige content, volgend ook vanuit het eerder genoemde volledig in control zijn, gaat verder dan alleen records management. *De informatie lifecycle management en compliancy moet gelden voor alle content.*

Beleid en organisatie (information governance)

Capgemini raadt aan het project om te komen tot een goede inbedding van Information Governance voor content, en bij voorkeur ook voor data, zo spoedig mogelijk op te zetten ten einde tijdig randvoorwaarde stellend voor andere programma's te kunnen zijn.

Beveiliging en autorisatie

Het algemeen geldend principe van "alles content is voor iedereen beschikbaar, tenzij… " wordt voor de toekomstige ECM ontwikkelingen op het gebied van kennisdelen, content analyse, openheid en samenwerking als meest van toepassing zijnde gezien. Aansluiting bij, opname door of opvolging vanuit het project Informatie Veiligheid dat momenteel loopt wordt geadviseerd.

nav Coalitieakkoord – toezegging coalitie van 5 miljoen voor vernieuwing IDMS is besteed aan TOP (nu DZH), 2015

Vooraf aangeleverd aan coalitietafel: 7 mln gevraagd waarvan 6 mln voor vervanging iDMS en 1 mln voor transparantie.

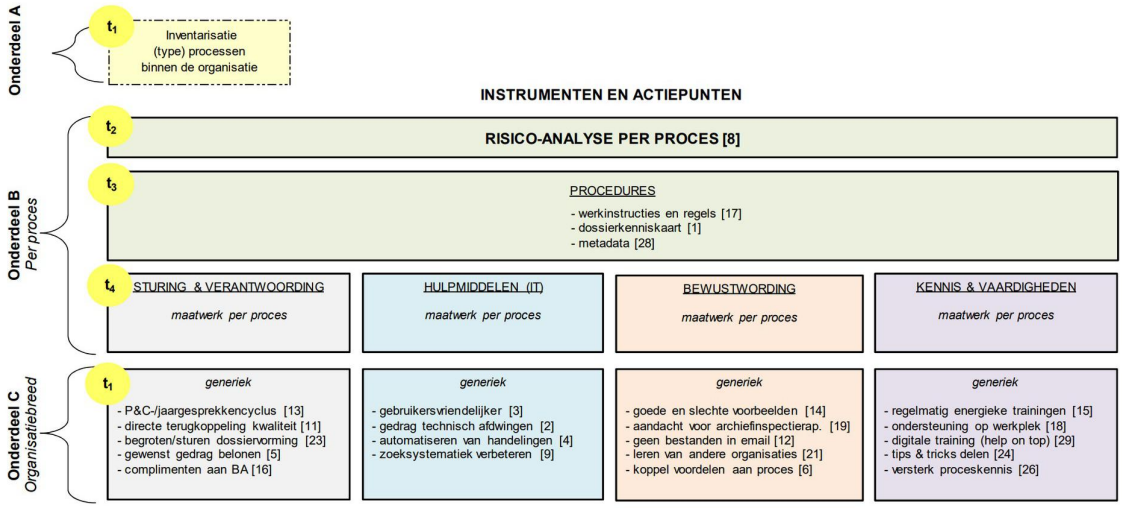
In het Hoofdlijnenakkoord is opgenomen dat Zuid-Holland voorop wil lopen in het transparant maken van de provincie en daarvoor incidenteel € 5 miljoen investeert in ICT-infrastructuur en werkprocessen die een grotere transparantie mogelijk maken. Deze investering is nadrukkelijk bedoeld als impuls voor het transparant maken van de provincie. Er wordt dus geen regulier werk mee bekostigd. Voor dit bedrag is het DataWarehouse gerealiseerd waarbij de governance nog niet geregeld is.

Archiefinspectie, 2016

Een van de belangrijkste conclusies uit de inspectie is dat de digitale archivering in het daartoe ingerichte documentmanagementsysteem (iDMS) in vergelijking met vier jaar geleden nog steeds niet op orde is. De behandelend ambtenaren zijn op grond van provinciale regelgeving verplicht zelf hun dossiers te vormen en te beheren.

EAA: Meervoudige kennis onderzoek, 2016

Naar aanleiding van de inspectierapport van de provinciearchivaris 2015 is aan Provinciale Staten toegezegd om de conclusies en aanbevelingen hieruit met alle directeuren te bespreken en op basis hiervan vóór het zomerreces van 2016 te komen met een concreet plan van aanpak (‘archief op koers’) met maatregelen en acties ter verbetering van de situatie van het archief- en informatiebeheer. EAA bevelen aan om het advies, zoals weergegeven in de onderstaande roadmap, te integreren in een plan van aanpak. Op deze manier wordt voortgebouwd op de inspanningen en resultaten die in de afgelopen periode zijn geleverd met een grote groep betrokken medewerkers.



Figuur 1: Roadmap actiepunten t.b.v. dossiervorming en archivering

NB.: De instrumenten zijn onderstreept. De actiepunten zijn voorzien van een nummer [X]. Op basis hiervan kan de uitwerking van het actiepunt worden gevonden in bijlage 3.

Uitkomst: mensen zien dat hun gedrag bepalend is, echter bij oplossingsmogelijkheden wordt vooral naar een systeem/IT verwezen.

Besluit directeur concernzaken, 2016

ECM visie gaat geen vervolg krijgen, alleen de urgente zaken uit de archiefinspectie worden opgepakt uit middelen van I&A. Daaruit is het programma Archief op Koers ontstaan.

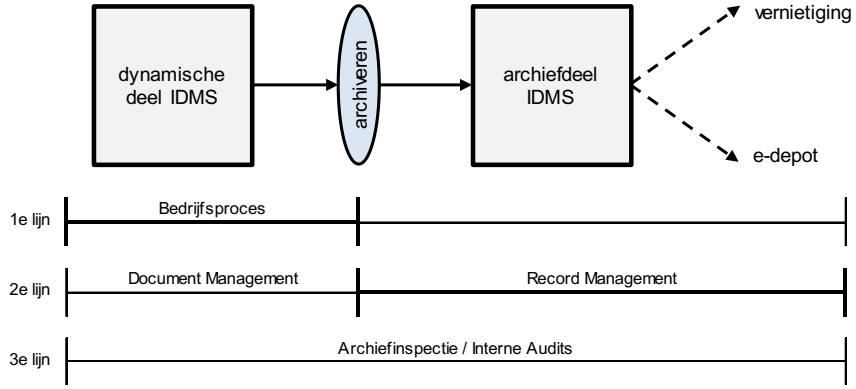
Archief op Koers, 2016-2018

Met de oplevering van Archief op Koers zijn de aanbevelingen en verbeterpunten van de provinciearchivaris en van EAA uitgevoerd. Al eerder namelijk in 2012/2013 is een programma uitgevoerd om de kwaliteit van dossiervorming te verbeteren.
Om te voorkomen dat om de paar jaar programma’s uitgevoerd moeten worden om achterstanden in te halen en dossiervorming weer op niveau te brengen heeft de programmanager AoK de eenheid Audit en Advies gevraagd, het programma tegen het licht te houden en aanbevelingen te doen voor de structurele inbedding van de resultaten in de organisatie.

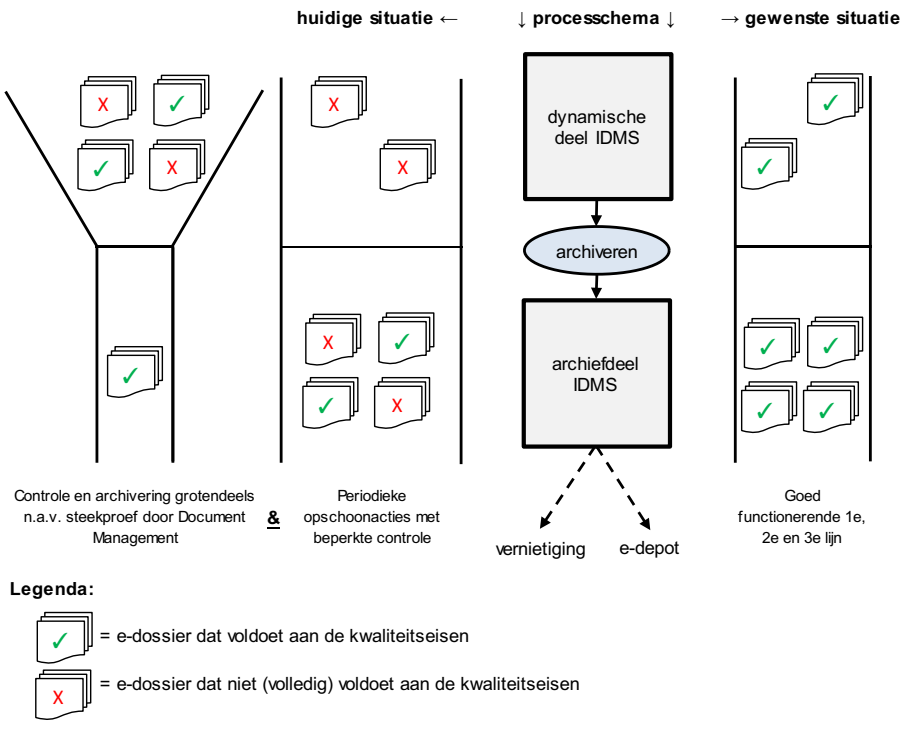
EAA, Management Letter onderzoek naar inbedding informatiebeheer, 2017

- Diverse afdelingshoofden hebben geen duidelijk beeld bij informatiebeheer en/of hun verantwoordelijkheid daarvoor.

- Afdelingshoofden vinden over het algemeen dat ze onvoldoende zijn toegerust om hun verantwoordelijkheid voor informatiebeheer te nemen. Het schort volgens hen met name aan managementinformatie en duidelijke kaders, maar ook over de andere stellingen oordelen ze weinig positief.
- Bij de meeste, maar niet alle, afdelingen zijn bureauhoofden ook verantwoordelijkheid voor informatiebeheer. Slechts een deel van de afdelingshoofden geeft antwoord op de vraag welke taken bureauhoofden in dat kader hebben. Sommigen geven expliciet aan dat hierover geen scherpe afspraken zijn gemaakt.



Figuur 1: verdeling verantwoordelijkheden tussen 1e, 2e en 3e lijn



Figuur 2: huidige en gewenste situatie

Startbrief 2018 - Overzicht integrale bedrijfsvoeringonderwerpen, 2017

Een I-strategie ontwikkelen met betrokkenheid van collega's uit de hele organisatie.

Versterken van centrale agendering en coördinatie (CIO-functie) om een goede verbinding te leggen met ontwikkelingen op het gebied van Public Intelligence en TOP.

Versterken van de afdeling I&A waar het gaat om actief en alert ontwikkelen en faciliteren van de I-kant richting beleid en uitvoering, om zo bij te dragen aan een moderne en responsieve provincie.

Elke afdeling heeft dit jaar het onderdeel informatie op moeten nemen in zijn jaarplan, dit is enkel dit jaar zo uitgevraagd.

Beoogd resultaat: Een PZH die voldoende toegerust is voor de toekomst als het gaat om de wijze waarop wij omgaan met informatie in samenhang met de opgaven waar we voor staan.

Evaluatie proces bestemmingsplan Zwethof, 2018

Eindconclusie

Niet tijdig onderkennen gevoeligheid locatie Zwethof heeft belangrijke invloed op verloop proces en besluitvorming. Zorg voor een betere informatievoorziening naar Provinciale Staten, bijvoorbeeld door het beschikbaar stellen van informatie over de voorgeschiedenis bij stukken en het expliciet maken van deze locaties in het Programma ruimte en attendeer Provinciale Staten hierop.

Rapportage Archiefinspectie, 2018

Archief op Koers heeft grote verbeteringen in de digitale dossiervorming weten te realiseren.

Aanbevelingen

Digitaal archief- en informatiebeheer

De digitale archivering in iDMS is verbeterd, evenals de ondersteuning van de behandelend ambtenaren. Een nieuwe manier van dossiervorming is geïntroduceerd, die het werken met iDMS heeft vereenvoudigd en de archivering in applicaties buiten het iDMS is onderzocht en beheermaatregelen worden per applicatie geregeld.

ICT-beheer en informatiebeveiliging

Het ICT-beheer en de informatiebeveiliging zijn waar het de archief wettelijke aspecten aangaat op orde. De aanbevelingen die de Eenheid Audit en Advies doet voor het informatiebeheer in relatie tot de invoering van de Algemene Verordening Gegevensbescherming worden onderschreven.

Digitale archivering buiten IDMS

Buiten het iDMS zijn er meerdere systemen waarin digitale informatie in de vorm van documenten of data wordt opgeslagen en gedeeld, waarbij dit soms in interne applicaties geschied, maar ook in de Cloud of bij derden. Sinds 2016 zijn over de opslag van informatie goede afspraken gemaakt en maatregelen genomen om de archiefwaardige bescheiden in de intern in gebruik zijnde applicaties goed te (laten) beheren, te archiveren en duurzaam op te slaan.

Jaarverslag FG, 2019

De volgende belangrijkste adviezen zijn door de FG benoemd die betrekking hebben op de risico's bij de verwerking van persoonsgegevens.

- Zorg op korte termijn dat de rollen en rechten op orde zijn in iDMS. Vervang iDMS en stel daarbij deadlines voor de keuze van een nieuw programma en de implementatie. Reactie: Dit is deels overgenomen. iDMS wordt geupdate, vernieuwd en er zullen diverse verbeteringen doorgevoerd worden.

- PZH beschikt niet over een beleid ten aanzien van het omgaan met persoonsgegevens, niet op afdelingsniveau en niet als concern. Er is soms wel wat beleid op deelaspecten. Daarnaast beschikt PZH wel over een privacyverklaring, welke is gepubliceerd op haar website. De AVG vereist echter een beleid op het gebied van privacy waarin ook is vastgelegd op welke wijze de kwaliteit van het omgaan met persoonsgegevens is geborgd.
- Zet ook in 2020 vol in op bewustwording binnen de organisatie door middel van campagnes waarbij het thema datalek centraal staat.

EAA onderzoek (0-meting) bewuste omgang met informatie, 2019

Conclusies:

- Bewustzijn is aanwezig: men weet dat we wat te beschermen hebben. Dilemma hierbij is de transparantie
- Men heeft behoefte aan meer informatie over veilig werken: omgang met wachtwoorden, gebruik wifi, verlies tablet/telefoon, bij wie melden, opslaan van info, delen van info met derden, omgaan met updates e.d.
- FG en informatiebeveiligingsspecialist zijn onbekend
- Er zijn verschillende opvattingen over (de noodzaak van) het vergrendelen. Er is niet veel verschil tussen de antwoorden van managers en die van overige medewerkers. Met betrekking tot het vergrendelen van de computer moet bepaald worden wat vanuit beveiliging wenselijk is
- Delen van gebruikersnamen en wachtwoorden is een belangrijk aandachtspunt. Dit heeft soms een technische oorzaak, maar ook gemak. De privacy als bv secretaresses inloggen als leidinggevende, wordt hierbij genoemd als zorgpunt
- Als oorzaak dat dossiers niet op orde zijn wordt de gebruikersonvriendelijkheid van IDMS vaak genoemd
- Men maakt zich zorgen over het gebruik van SAAS-oplossingen (Amerikaanse bedrijven), whats app, beheer van informatie

Bewustwordingscampagne Up to data opgestart, 2019

In 2019 is na een 0-meting een eerste campagne, “Up to data”, geïnitieerd door I&A in samenwerking met bestuur (AVG, Woo en provinciaal archivaris) en P&O (integriteit). De onderwerpen van deze campagne zijn: Data- en informatiekwaliteit, Informatie veiligheid, Privacy, Informatiebeheer en Integriteit. Diverse succesvolle acties zijn opgezet en in de organisatie gedeeld.

Vernieuwing IDMS, 2019

Projectleider is gestart met ID (Initiatie Document) voor een traject dat na afronding van de onderhanden iDMS upgrade moet leiden tot een verbeterde/gewijzigde inzet van het iDMS in de ondersteuning van de organisatie. Is gebaseerd op functionaliteit die straks met de nieuwe versie beschikbaar komt, en de ‘noodzaak’ beter in te spelen op wensen t.a.v. betere samenwerking, inzet van nieuwe tooling als Teams (office365 traject), data gedreven werken. De analyse voor dit vernieuwingstraject willen we al parallel aan de upgrade opstarten. Dit traject is uiteindelijk niet doorgezet ivm ontbreken financiële middelen.

Warmtedossier, 2019

Vertrouwelijke stukken gekopieerd naar openbaar deel van iDMS. Dit is vertrouwelijk opgeruimd en dichtgezet.

Wob verzoek Shell, 2019

Een omvangrijk Wob-verzoek van een juridisch adviseur over Shell (zgn. Shellpapers). Het verzoek is in november 2019 nader ingeperkt/gepreciseerd, wat niet heeft geresulteerd in een Wob-verzoek die

in behandeling genomen kon worden, het Wob-verzoek is daarom door PZH buiten behandeling gesteld (afgewezen). Inmiddels (2023) is dit verzoek weer relevant en krijgt deze mogelijk een vervolg.

Archiefinspectie, 2020

Aanbevelingen

Het beheer van digitale documenten en data is onvoldoende. Ontvangen of verzonden informatie is slecht of niet terug te vinden en dat vereist niet alleen beter beheer van documenten en data door betrokken medewerkers, maar ook daartoe ingerichte en veilige informatiesystemen. Aanbevelingen van de provinciearchivaris zijn om meer voorlichting en scholing over archivering, informatiebeheer, privacybescherming en informatieveiligheid te geven en archieven en databestanden daadwerkelijk te schonen en te inventariseren. Dit vraagt onder meer om een structurele vernieuwing van het archiefsysteem iDMS en de aanpassing van andere applicaties om de duurzame vastlegging van data mogelijk te maken.

De duurzame bewaring en beveiliging van de fysieke en digitale informatie is grotendeels op orde. De risico's op datalekken in de provinciale informatiesystemen, waaronder in het archiveringssysteem iDMS, zijn wel zorgelijk. De aanbevelingen die de Functionaris Gegevensbescherming in zijn Jaarverslag Privacy over 2019 doet over informatiebeheer en informatieveiligheid onderschrijft hij.

Hefbrug Boskoop, 2020

Dossier is niet volledig en versnippert over verschillende digitale mappen en bronnen.

Aanbeveling EAA

De onderzoekers hebben veel tijd moeten investeren in het achterhalen van de juiste stukken. Er zijn veel digitale mappen over de hefbrug Boskoop (in IDMS en op de Q-schijf van DBI). De samenhang tussen deze mappen is gebrekkig en de erin opgenomen informatie niet altijd volledig. Goede dossiervorming en het eigenaarschap hiervoor zijn voorwaarden voor kennisborging en om het leerproces van de organisatie verbeteren.

Wij bevelen DBI aan om zorg te dragen voor verbetering van de kwaliteit en volledigheid van dossiers en het eigenaarschap hiervoor te organiseren.

Professionaliteit

Informatiebeheer vraagt blijvend inzet van alle ambtenaren. Dit is niet altijd leuk, maar is een onderdeel van de professionaliteit/verantwoordelijkheid van elke medewerker. Positief gevolg van goed informatiebeheer door iedereen is de terugvindbaarheid van onze bescheiden.

Blijvend aandacht

Het onderwerp informatiebeheer heeft blijvend aandacht nodig, we zijn nooit klaar. Elke dag wordt er nieuwe informatie/data toegevoegd aan onze systemen, daar zal altijd over nagedacht moeten worden: hoe slaan we dit op? waarom slaan we dit op? voor wie moet het beschikbaar/vindbaar zijn? etc.

Gedrag

Het gedrag van mensen blijft de grootste uitdaging, een systeem staat of valt met hoe goed dit gebruikt en nageleefd wordt. Er kan en wordt veel ondersteund, echter niet alles is af te vangen.

Jaarverslag Functionaris voor Gegevensbescherming, 2021

De provincie voldoet niet altijd aan gegevensminimalisatie, vooral niet bij haar document management systeem (iDMS). De FG wees hier al op in het jaarverslag over 2019. Ondanks dat de organisatie het systeem verbeterde, blijft duidelijk dat het systeem niet is ingericht op een adequate

naleving van de AVG. Daarnaast weten medewerkers vaak niet goed hoe ze persoonsgegevens in het iDMS moeten verwerken, waardoor gevoelige en soms ook bijzondere persoonsgegevens in strijd met de AVG worden verwerkt. In 2021 kwam de afdeling I&A met een nieuwe visie op het informatiebeheer binnen de provincie, waarin ook het document management systeem een plaats heeft. De provincie blijft de AVG schenden totdat er een nieuw en/of sterk verbeterd DMS is, met alle risico's op sancties door de Autoriteit Persoonsgegevens

EAA onderzoek (1-meting), 2021

Conclusies

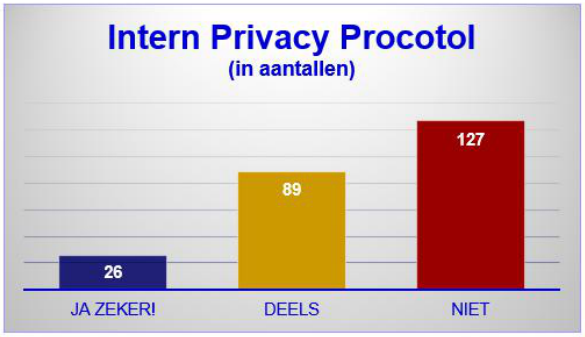
1. De bekendheid met de Campagne Up-to-Data is wisselend: sommige activiteiten uit de campagne zijn redelijk goed bekend bij de respondenten en anderen zijn minder opgevallen. Recente initiatieven zijn het meest bekend.
2. Uit ons onderzoek blijkt dat respondenten bewust zijn van de waarde van informatie.
3. Bewustzijn van provinciale medewerkers met betrekking tot privacy, informatiekwaliteit/-integriteit, informatieveiligheid, informatiebeheer en archivering is aanwezig, maar moet wel verbeterd worden.
4. Er volgen hierna aandachtspunten die de waarde van informatie en de bewustzijn bij de omgang met informatie kunnen vergroten.
5. Kracht van herhaling: bewustzijn is een "on going" proces.

Aanbevelingen om bewustzijn te vergroten

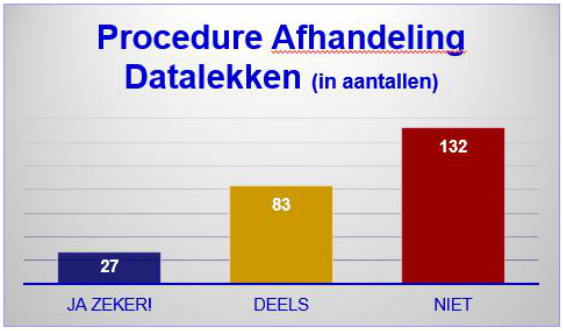
1. Bewustzijn bij de omgang met informatie is een continu proces. Gebruik de kracht van herhaling en sluit de campagne aan op de behoefte aan informatie van de respondenten.
2. Er is behoefte aan training, webinars, opleiding op specifieke gebieden (cybersecurity, veilig thuiswerken, iDMS, enz.). Deze zijn belangrijk voor nieuwe medewerkers, maar opfriscursussen kunnen helpen om bewustzijn op peil te houden.
3. Geef aandacht aan de richtlijnen voor archiveren (iDMS, Teams, OneDrive, Whatsapp enz.). De bekendheid met de richtlijnen is verschillend bij de respondenten.
4. Geef aandacht aan de vindbaarheid en gebruikersvriendelijkheid van documenten met relevante procedures, beleid en richtlijnen. Hierbij gaat het ook om op het werkproces en de opgaven gerichte informatie.

Kennis van interne procedures en richtlijnen over AVG kan worden verbeterd

Intern Privacy Protocol is bij 52% van de respondenten niet bekend



Procedure Afhandeling Datalekken is niet bekend bij 55% van de respondenten



Visie op toekomstbestendig informatiebeheer- met Gartner, 2021

Fundament van het informatiebeheer is niet op orde en vereist dringend actie

Er is een veelheid aan technologieën, platforms en een wildgroei aan informatie. Er dreigt op dit punt een onbeheersbare situatie te ontstaan

Er is in het I-domein geen werkende en gesloten I-besturingscyclus

Door een gebrek aan sturing is er te weinig focus en onvoldoende richting. Veel initiatieven bestaan 'los' van elkaar en eindigen door een gebrek aan regie in het 'niets'

Het verder ontwikkelen van het data/informatie-gedreven werken is essentieel

In het werkveld van het data/informatie-gedreven werken worden de komende jaren 'de kaarten opnieuw geschud'. Als PZH zich niet nadrukkelijk op dit vlak ontwikkelt, wordt het lastiger haar rol te behouden

Het betreft een omvangrijke PZH-brede veranderopgave met een aanzienlijke ICT-component

De verandering zal alle medewerkers beïnvloeden. Veel aandacht voor verandermanagement en communicatie is cruciaal. Voorbeeldgedrag van directeuren, regisseurs en leiders is essentieel

De organisatie is nooit 'klaar'

Informatiebeheer en data/informatie-gedreven werken blijven in ontwikkeling en vergen voortdurende verandering en investeringen. Het is 'nooit af'.

Memo aan MT I&A Persoonsgegevens, 2022

In 2022 is er door twee adviseurs Recordmanagement onderzoek gedaan naar persoonsgegevens in de schadedossiers in het iDMS en onderzocht hoelang deze gegevens bewaard moeten worden op grond van de AVG en de Archiefwet. De volgende persoonsgegevens zijn bij het onderzoek in de schadedossiers in het iDMS naar voren gekomen:

- Naam van de persoon die schade geleden of veroorzaakt heeft
- Bankrekeningnummer van de persoon aan wie schade vergoed wordt
- Bankrekeningnummer van de PZH.

In het geval van schadedossiers gaat het om een beperkt aantal persoonsgegevens, maar dat kan in andere dossiers wellicht veel meer zijn. Het is dan ook aan te bevelen om te onderzoeken welke

andere dossiers in iDMS persoonsgegevens bevatten. Tegelijkertijd is het zaak ook andere informatiesystemen en applicaties buiten iDMS hierop te onderzoeken. Deze aanvullende vraag heeft geresulteerd in deze memo over de wijze waarop onze organisatie dient om te gaan met persoonsgegevens. De inhoud van deze memo is afgestemd met de Functionaris voor Gegevensbescherming, de provinciearchivaris, de bestuurlijk-juridisch adviseur en strategisch adviseur informatiebeveiliging.

Advies aan MT

Gezien de urgentie en de risico's die samenhangen met dit onderwerp vragen wij het MT om op korte termijn iemand aan te wijzen die het beleid gaat formuleren. Daarnaast vragen wij het MT om mee te denken wat de meest effectieve manier is om het beleid binnen de organisatie uit te dragen.

Nota van bevinding- Randstedelijke Rekenkamer, 2022

Grotendeels werkt de provincie al volgens het nieuwe regime van de Woo. Zo is elektronische indiening van Wob-verzoeken al mogelijk en worden besluiten (inclusief achterliggende documenten) op Wob-verzoeken gepubliceerd op de website. De beslistermijnen zijn nog een aandachtspunt op weg naar de Woo.

Stukken beter bewaard, 2022

Met Stukken Beter Bewaard (SBB) zal PZH haar efficiëntie en effectiviteit van de informatiehuishouding verbeteren. De "Visie op een toekomstbestendig Informatiebeheer" van Gartner1 geeft aan wat er nodig is om de informatiehuishouding sterkte verbeteren. Dit zal gerealiseerd worden door onder anderen het optimaal inzetten van kaders, opleidingen, technologie, veranderingsbeheer. Mede door het inzetten van een organisatie brede bewustwordingscampagne, zal het besef vergroot worden dat 'een informatiehuishouding op orde' een gemeenschappelijke verantwoordelijkheid is. Stukken Beter Bewaard is opgegaan in het programma Informatietransitie.

Programma Informatietransitie, 2023

De PZH investeert de komende jaren fors in digitalisering. De digitale provincie is één van de speerpunten. Als basis voor de digitalisering wordt de komende jaren het informatiebeheer op orde gebracht. Op 31-1-2023 heeft GS besloten 23 mln toe te kennen aan het programma Informatietransitie, verdeeld over een periode van 6 jaar.

Met het op orde brengen van het informatiebeheer zet de PZH ook belangrijke stappen in het proces van actieve openbaarmaking van informatie. De uitvoering van het programma zorgt voor een belangrijke andere manier van kijken naar en omgaan met data en informatie binnen de provincie.

Ook wordt met de uitvoering van het programma een grote stap gezet in het data- en informatie-gedreven werken van de provincie. Dit betekent dat de provincie in toenemende mate in de beleidsontwikkeling en besluitvorming in staat is om gebruik te maken van inzichten die uit haar data en informatie met geavanceerde hulpmiddelen worden ontsloten.

Informatieveiligheidsbeleid "Open tenzij" vs "Gesloten tenzij"- AOG-I&A, 2023

- Akkoord met de voorgestelde memo, met de kanttekening dat er een impact analyse uitgevoerd moet worden op (consequenties huidige systemen en gedrag mensen). Ook meenemen lopende ontwikkelingen/trajecten waarbij dit nieuwe beleid niet bij start is meegegeven (bijvoorbeeld programma Informatietransitie).
- Er moet goede aansluiting zijn bij lopende initiatieven zoals het werkend maken van OGO, spoor 2, de systemen en processen, met het OGO geschikt van systemen. Deze aspecten zullen ook in scope moeten komen van deze projecten.

- Daarnaast is het belangrijk om alles by design (zowel archivering, informatieveiligheid, privacy, ethics, transparantie etc) in te regelen, én het makkelijk werken by design moet ook altijd een belangrijk principe zijn.

Vervolg bewustwordingscampagne, 2023

"Zo doen we dat", start november 2023

In 2021 is er door EAA een 1-meting uitgevoerd over de bewuste omgang met informatie, de resultaten daarvan zijn gebruikt om te komen tot een nieuwe campagne, "Zo doen we dat", die binnenkort van start gaat. In deze campagne wordt er vanuit gedragsleer gekeken naar wat er nodig is om mensen het 'gewenste gedrag' te laten vertonen.

Conclusie:

Er zijn vele initiatieven en onderzoeken geweest, vaak is daar opvolging aan gegeven, echter is de urgentie op diverse niveaus vaak niet voldoende onderkend en zijn financiële middelen daardoor veelal niet geboden. De conclusies uit het rapport opgeleverd door Gartner "visie op toekomstbestendig informatiebeheer" komen niet uit de lucht vallen.

provincie Zuid-Holland

Memo

Contact

art 5 1-2e
art 5 1-2e
art 5 1-2e @pzh.nl

Datum

29 september 2023

Aan

art 5 1-2e

Kopie aan

art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e

Onderwerp

Beschrijving iDMS

Het huidige informatiebeheersysteem van de PZH is opgebouwd rondom iDMS: het integraal document managementsysteem. De hiermee verbonden techniek was in 2007, toen het werd aangeschaft, de logische keuze in een periode waarin de transformatie van een papieren naar een digitale werkwijze plaatsvond. Toentertijd was er binnen de provincie een sterke focus op control van de stukkenstromen. De inrichtingskeuzes van iDMS zijn gemaakt op basis van de toen door de organisatie gestelde randvoorwaarden, de aanwezige kennis en de beschikbare technieken. Momenteel bevat iDMS zo'n 50 miljoen documenten verdeeld over primaire-, ondersteunende processen, organisatieomgeving en digitale archiefomgeving. Daarnaast heeft elke gebruiker een persoonlijke werkomgeving. De medewerker is vanaf dit moment zelf verantwoordelijk voor de compleetheid van zijn of haar informatie.

Ondanks verschillende acties en voorlichtingscampagnes de afgelopen jaren, is IDMS feitelijk nooit helemaal gevuld zoals bedoeld. Er zijn de afgelopen jaren vele voorlichtingscampagnes en acties geweest om betere dossiervorming te stimuleren, van De Week van het E-dossier alweer heel wat jaren terug, programma Archief op Koers, tot Up-to-Data van recente datum. Het vestigt even de aandacht op het onderwerp, daarna verslapt deze weer.

Kaders en ontwikkeling

De inrichting en het gebruik van iDMS zijn onderhevig aan verschillende wettelijke kaders , beleid en andere regelingen. Bij de ingebruikname van iDMS in 2007 waren andere kaders van toepassing. Destijds is gekozen voor het principe “Openbaar, tenzij” wat nog steeds gehanteerd wordt, de AVG was nog niet van kracht.

Vanuit wetgeving worden steeds meer eisen gesteld die van toepassing zijn op informatiebeheer. iDMS is niet in alle gevallen voldoende aangepast op deze veranderingen. Denk bijvoorbeeld aan de AVG die in 2018 in werking is getreden. Het beleid dat thans wordt gebruikt voor het opslaan van vertrouwelijke informatie stamt uit 2009. Vanuit Team Informatieveiligheid heeft in het kader van de ISO 27001 implementatie hier onlangs een

actualisatie voor plaatsgevonden. Het AOG I&A heeft met dit voorstel ingestemd en het wordt binnenkort aan het DT voorgelegd. In dat voorstel wordt ook het 'open tenzij'-beleid aangepast.

Voor zover er gegevens aangetroffen worden die niet voldoende zijn afgeschermd, wordt indien nodig hiervan melding gemaakt bij de Autoriteit Persoonsgegevens. De structurele verbetering voor AVG-conform informatiebeheer wordt de komende jaren opgepakt vanuit het programma Informatietransitie door onder andere het opschonen van de huidige informatie, het stevig sturen op informatiebeheer, kennisvergroting en gedragsverandering bij alle medewerkers en het moderniseren en saneren van onze middelen.

Beheer en onderhoud
Voor de continuïteit en veiligheid in Zuid-Holland zijn we mede afhankelijk van iDMS. De beschikbaarheid van iDMS is essentieel; hier is het beheer ook op ingericht.

Het dagelijks beheer iDMS wordt procesmatig uitgevoerd door interne functioneel- en technisch beheerders en staan direct in contact met de organisatie. Wijzigingen met functionele impact worden samen met de gebruiker afgestemd en getest.

IDMS krijgt met regelmaat een software update. Deze is in beginsel technisch van aard en zorgt in zeer beperkte mate voor impact op de gebruikers. Bijna maandelijks worden kleine wijzigingen uitgevoerd ten behoeve van continuïteit en betrouwbaarheid. Technisch is iDMS in alle jaren goed onderhouden, de inrichting is grotendeels zoals die in 2007 is opgebouwd.

Planning datalek 7 september

Acties	Actiehouder	Status	Gereed (j/n)	Deadline
Query “curriculum vitae”	art 5 1-2e / art 5 1-2e	Klaar	J	
Query “paspoort”	art 5 1-2e / art 5 1-2e	Klaar	J	
Logs “Bibob”	art 5 1-2e	Ter validatie		
Logs “curriculum vitae”	art 5 1-2e	Klaar	J	
Logs “paspoort”	art 5 1-2e	Klaar	J	
Brief JVG	art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e	Klaar	J	29 september
Geïsoleerde en geidentificeerde bestanden beoordelen	Eenheid privacy	Start 29 september		
Definitieve melding AP	art 5 1-2e / art 5 1-2e			5 oktober
(Besluit) informeren betrokkenen	art 5 1-2e / art 5 1-2e			5 oktober

"Van: art 5 1-2e
Verzonden: 2
"Aan: art 5 1-2e
art 5 1-2e
"CC: art 5 1-2e art 5 1-2e , art 5 1-2e
Onderwerp: FW: Datalek iDMS
"
TK. Zie opmerking Willy: hieruit blijkt te meer de urgentie voor een vernieuwd iDMS én de noodzaak voor een goed communiceerbaar plan van aanpak met (haalbare) planning en benodigd budget. Na het reces of eerder als het kan graag weer bespreken in MT.

art 5 1-2e

Naast een vernieuwd iDMS staan er in dit werkveld nog 2 opgaven op mijn netvlies die een duidelijke plek in ons portfolio moeten krijgen:

* De opgave Duurzaam informatiebeheer dat in opdracht van GS gaat starten als nasleep va het incident rond de hefbrug Boskoop
* De wettelijke verplichtingen rond digitale toegankelijkheid (waarvan we de eerste deadline niet art 5 1-2e omdat we nog niet gestart zijn)

En dat roept weer de vraag op of dit allemaal haalbaar is samen met nog 2 urgenties: het project IAM en NIS.

Kenmerkend is in ieder geval dat al deze opgaven (behalve duurzaam informatiebeheer dat nog moet starten) niet volgens planning verlopen of verliepen.

En als de onderliggende oorzaak is dat we te weinig capaciteit kunnen vrijmaken vanwege onze beheertaken dan moeten we hier mogelijk in de begroting 2021 een budget voor claimen en ook kijken of dat iets voor onze sourcingstrategie betekent.

Groet,

art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: donderdag 30 juli 2020 16:10
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e
art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: FW: Datalek iDMS

Collega’s,

Zie hieronder de reactie van art 5 1-2e en Willy de Zoete (zie bijlage voor haar eerdere reactie).

Groeten,

art 5 1-2e

Van: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl
<mailto:wh.de.zoete@pzh.nl> >
Verzonden: donderdag 30 juli 2020 15:02
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Re: Datalek iDMS

Dank art 5 1-2e

Wat betreft het snel vervangen van iDMS ben ik het helemaal met je eens. Het

moet niet mogelijk zijn om onbevoegd toegang te krijgen tot gegevens. Ik weet dat er aan gewerkt wordt, maar zal er in het najaar extra aandacht en voortvarendheid voor vragen.

Vriendelijke groet,

Willy de Zoete

Van: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: Thursday, July 30, 2020 2:50:27 PM
Aan: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl
<mailto:wh.de.zoete@pzh.nl> >; art 5 1-2e <art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> >; art 5 1-2e <art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> >
Onderwerp: RE: Datalek iDMS

Dag Willy en art 5 1-2e

Zoals art 5 1-2e al heeft geschreven in haar mail deel ik de conclusie niet dat het niet zou gaan om een datalek.

Het valt op basis van de audittrails in iDMS niet uit te sluiten dat er geen onbevoegden toegang hebben gehad tot mappen of bestanden die niet voor hun ogen bestemd waren.

Daarvoor schieten de logmogelijkheden van iDMS eenvoudigweg tekort. Bovendien wordt bij het loggen een van de basisregels van logging en monitoring geschonden, namelijk dat alle acties worden vastgelegd in het logbestand en dat deze niet kunnen worden veranderd. Mijns inziens is dat bij iDMS niet het geval. Bijvoorbeeld bij het veranderen van rechten kan niet uit de logbestanden worden gehaald welke rechten, van wie en op welke wijze zijn veranderd. De reactie van het functioneel beheer van iDMS dat dit kan worden teruggevonden in het wijzigingsverzoek in Topdesk, voldoet niet aan de vereisten die gesteld mogen worden aan logging, namelijk dat deze onder andere niet achteraf kunnen worden gewijzigd. Voor zover mij bekend is, kan ook toegang worden verkregen tot de vertrouwelijke mappen door het team dat met behulp van BI-tools aan data-mining kan doen en dat bijvoorbeeld ook heeft gedaan inzake het WOB-verzoek rond Shell. Nogmaals voor zover mij bekend, zijn daarvan ook geen sporen terug te vinden in de logging van iDMS.

Ook het maken van aanvullende procedurele afspraken over het gebruik van en toegang tot bepaalde mappen in iDMS biedt mijns inziens onvoldoende waarborgen voor de toekomst. Dit ziet in onvoldoende mate op de technische maatregelen waar de AVG om vraagt.

Derhalve blijf ik van mening dat niet kan worden uitgesloten dat onbevoegden toegang hebben gehad tot zeer vertrouwelijke en geheime mappen in iDMS.

Ik ben dan ook van mening dat met verhoogde inspanning werk gemaakt moet worden van de vervanging van iDMS. In de tussentijd zou moeten worden gezocht naar een oplossing die wel voldoende technische maatregelen in zich bergt voor het veilig kunnen opslaan van vertrouwelijke en geheime stukken zoals die worden gebruikt door het team Bibob.

Dat onbevoegde toegang niet uit te sluiten valt, wordt ook bevestigd in de conclusie die door art 5 1-2e aan jullie is gestuurd.

Met vriendelijke groet,

art 5 1-2e

Functionaris voor Gegevensbescherming

M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>

-Wanneer u de provincie Zuid-Holland een e-mail stuurt, ontvangt u binnen 2 werkdagen een reactie en binnen twee weken een antwoord. Al uw informatie wordt vertrouwelijk behandeld. Persoons- of adresgegevens worden uitsluitend gebruikt waarvoor u ze heeft verstrekt. Uw e-mailbericht wordt op een goede en veilige manier gearchiveerd.

-Vragen kunt u stellen via het contactformulier <https://www.zuid-holland.nl/contact/contactinformatie/> .

Van: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl <mailto:wh.de.zoete@pzh.nl> >
Verzonden: donderdag 30 juli 2020 13:16
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
CC: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Re: Datalek iDMS

Dank art 5 1-2e

voor dit uitgebreid verslag van je onderzoek. Het geeft mij vertrouwen. Ik wacht verder af.

Vriendelijke groet

Willy de Zoete

Wh.de.zoete@pzh.nl <mailto:Wh.de.zoete@pzh.nl>

Outlook voor Android downloaden <https://aka.ms/ghei36>

From: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Sent: Thursday, July 30, 2020 1:02:17 PM
To: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl <mailto:wh.de.zoete@pzh.nl> >
Cc: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Subject: Datalek iDMS

Beste art 5 1-2e Willy,

Naar aanleiding van een melding van een datalek in iDMS heb ik afgelopen 2 weken onderzoek verricht. Ik kom tot de conclusie dat hier geen sprake is van een datalek en wel om onderstaande redenen:

Aanleiding voor het melden van een datalek is de onrust bij het Bibob-team over de toegang tot hun vertrouwelijke iDMS-mappen en in het bijzonder de mappen over C-quential. art 5 1-2e (coördinator Bibob) is, op maandag 20 juli, voorzien van informatie over het verkrijgen van inzicht in wie, welke documenten heeft geraadpleegd. Uit een eerste controle, onder mijn toezicht, is gebleken dat er geen sprak is van onbevoegde toegang of onjuist rechtenstructuur. Alleen indien

bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. In dit specifieke geval is er geen sprake van een beveiligingsincident of datalek. Er is geen aanwijzing dat er persoonsgegevens verloren zijn gegaan of dat er “onrechtmatige verwerking” van persoonsgegevens heeft plaats gevonden. Indien uit een tweede controleslag (uitvoering door art 5 1-2e toch blijkt dat er onbevoegd toegang is verkregen tot de mappen van Bibob dan neemt art 5 1-2econtact op met FG en team informatieveiligheid.

Verder is gebleken uit de audittrial dat enkel bevoegde beheerders toegang hebben verkregen tot de mappen van het Bibob-team (ter uitvoering van hun werkzaamheden). Binnen het team van beheerders zijn dan ook onderling afspraken gemaakt over de beheertaken met betrekking tot de mappenstructuur van het Bibob-team. De stelling dat bestand bekeken kunnen worden zonder de juiste rechten is niet aan de orde. Het functioneel beheer wordt uitgevoerd as designed. Er is geen sprake dat er ongeautoriseerd personeel toegang heeft tot persoonsgegevens. Omdat er behoefte is aan extra beveiligingsmaatregelen heeft art 5 1-2e art 5 1-2e (beheer iDMS) aangeboden om verdere uitleg te geven over de technische beveiligingsmogelijkheden van iDMS. art 5 1-2ekrijgt een beheerdersrol toegewezen, zodat zij o.a. zelf de toegangsrechten kan aanmaken en intrekken. art 5 1-2een art 5 1-2e stemmen verdere procedurele- en technische maatregelen met elkaar af.

art 5 1-2e(FG) heeft een andere mening over deze kwestie.

Ik hoop jullie zo voldoende te hebben geïnformeerd, indien er vragen zijn dan verneem ik die graag.

Een prettige middag gewenst en hartelijke groet,

art 5 1-2e
"


provincie
ZUID HOLLAND

"Van: Zoete - van der Hout, WH, de"
Verzonden: 2020-07-30 13:15:57+00:00
"Aan: art 5 1-2e art 5 1-2e
"CC: art 5 1-2e
Onderwerp: Re: Datalek iDMS
"
Dank art 5 1-2e

voor dit uitgebreid verslag van je onderzoek. Het geeft mij vertrouwen. Ik wacht verder af.

Vriendelijke groet

Willy de Zoete

Wh.de.zoete@pzh.nl

Outlook voor Android downloaden <https://aka.ms/ghei36>

_____

From: art 5 1-2e <art 5 1-2e pzh.nl>
Sent: Thursday, July 30, 2020 1:02:17 PM
To: art 5 1-2e <art 5 1-2e pzh.nl>; Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl>
Cc: art 5 1-2e <art 5 1-2e pzh.nl>
Subject: Datalek iDMS

Beste art 5 1-2e en Willy,

Naar aanleiding van een melding van een datalek in iDMS heb ik afgelopen 2 weken onderzoek verricht. Ik kom tot de conclusie dat hier geen sprake is van een datalek en wel om onderstaande redenen:

Aanleiding voor het melden van een datalek is de onrust bij het Bibob-team over de toegang tot hun vertrouwelijke iDMS-mappen en in het bijzonder de mappen over C-quential. art 5 1-2e (coördinator Bibob) is, op maandag 20 juli, voorzien van informatie over het verkrijgen van inzicht in wie, welke documenten heeft geraadpleegd. Uit een eerste controle, onder mijn toezicht, is gebleken dat er geen sprak is van onbevoegde toegang of onjuist rechtenstructuur. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. In dit specifieke geval is er geen sprake van een beveiligingsincident of datalek. Er is geen aanwijzing dat er persoonsgegevens verloren zijn gegaan of dat er “onrechtmatige verwerking” van persoonsgegevens heeft plaats gevonden. Indien uit een tweede controleslag (uitvoering door art 5 1-2e toch blijkt dat er onbevoegd toegang is verkregen tot de mappen van Bibob dan neemt art 5 1-2e contact op met FG en team informatieveiligheid.

Verder is gebleken uit de audittrial dat enkel bevoegde beheerders toegang hebben verkregen tot de mappen van het Bibob-team (ter uitvoering van hun werkzaamheden). Binnen het team van beheerders zijn dan ook onderling afspraken gemaakt over de beheertaken met betrekking tot de mappenstructuur van het Bibob-

team. De stelling dat bestand bekeken kunnen worden zonder de juiste rechten is niet aan de orde. Het functioneel beheer wordt uitgevoerd as designed. Er is geen sprake dat er ongeautoriseerd personeel toegang heeft tot persoonsgegevens. Omdat er behoefte is aan extra beveiligingsmaatregelen heeft art 5 1-2e art 5 1-2e (beheer iDMS) aangeboden om verdere uitleg te geven over de technische beveiligingsmogelijkheden van iDMS. art 5 1-2e krijgt een beheerdersrol toegewezen, zodat zij o.a. zelf de toegangsrechten kan aanmaken en intrekken. art 5 1-2e en art 5 1-2e stemmen verdere procedurele- en technische maatregelen met elkaar af.

art 5 1-2e (FG) heeft een andere mening over deze kwestie.

Ik hoop jullie zo voldoende te hebben geïnformeerd, indien er vragen zijn dan verneem ik die graag.

Een prettige middag gewenst en hartelijke groet,

art 5 1-2e

"

Van: art 5 1-2e
Verzonden: 2022-12-02 10:42:28+00:00
Aan: art 5 1-2e
CC: art 5 1-2e
Onderwerp: FW: Melding mogelijk datalek A 94293
"
Akkoord?

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protect outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7Ccb08420103c1434ec09908dad44986b5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638055709511376054%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=RMw6P9o2IHIGzMcfNeLqDqZpMejIS7Kek2HU%2FBl%2B4YU
%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: vrijdag 2 december 2022 10:39
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: RE: Melding mogelijk datalek A 94293

De definitieve versie

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 2 december 2022 10:26
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: Melding mogelijk datalek A 94293

Pas maar aan dan, zitten met de 72 uur

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art 5 1-2e art 5 1-2e 40pzh.nl%7Ccb08420103c1434ec09908dad44986b5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638055709511376054%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=RMw6P9o2IHIGzMcfNeLqDqZpMejIS7Kek2HU%2FBl%2B4YU%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 2 december 2022 10:04
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: Melding mogelijk datalek A 94293

Oja, dat gedeelte (analyse) ben ik vergeten aan te passen. Ik heb geprobeerd haar te bellen, maar geen gehoor. Kan dit blijven liggen tot maandag? Anders kan ik de analyse ook aanpassen naar: ‘De smartphone is beveiligd met een toegangscode, dus het lijkt onwaarschijnlijk dat er persoonsgegevens raadpleegbaar zijn geweest.’

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 2 december 2022 09:57
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: Melding mogelijk datalek A 94293

Hi art 5 1-2e

Voor afhandeling van de melding is wel belangrijk om te weten of de telefoon gewist is. Dat staat nu wel in het advies maar weten we dus niet. Kun je haar misschien even bellen?

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C0 art 5 1-2e art 5 1-2e 40pzh.nl%7Ccb08420103c1434ec09908dad44986b5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638055709511376054%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=RMw6P9o2IHIGzMcfNeLqDqZpMejIS7Kek2HU%2FBl%2B4YU%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 2 december 2022 09:40
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: Melding mogelijk datalek A 94293

Hi art 5 1-2e

Bijgaand het concept voor de onderstaande datalek. Het enige is dat de collega mij gistermiddag zu bellen om mij te laten weten of de telefoon gewist is, maar dat heeft zij niet meer gedaan. Ik heb haar net gemaild, maar in haar agenda

staat dat ze vandaag vrij is. Vandaar dat ik toch maar het concept heb afgemaakt.

Laat maar weten of het concept aangepast moet worden!

Groet,

art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: maandag 28 november 2022 15:37
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> >
Onderwerp: RE: Melding mogelijk datalek A 94293

Hoi,

Morgenmiddag pakken art 5 1-2e en ik deze op.

Het is de eerste datalek voor art 5 1-2e

Ik heb morgenmiddag een afspraak ingepland en dan kunnen we met zijn tweeën alles fysiek even doornemen.

Vriendelijke groet,

art 5 1-2e

Coördinator eenheid & Privacy Officer

Eenheid Privacy

T art 5 1-2e Mail art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2F&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl%7Ccb08420103c1434ec09908dad44986b5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7

C638055709511376054%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=dG2ae8%2FGWkOhlwb8k1kgWpQtRyz5KV3bfGV%2BmF%2FEJnw
%3D&reserved=0>

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: maandag 28 november 2022 15:30
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> > ; art 5 1-2e
art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: RE: Melding mogelijk datalek A 94293

Lekker op tijd gemeld

Met vriendelijke groet,

art 5 1-2e art 5 1-2e

Functionaris voor Gegevensbescherming

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art 5 1-2e art 5 1-2e 40pzh.nl
%7Ccb08420103c1434ec09908dad44986b5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638055709511376054%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=RMw6P9o2IHIGzMcfNeLqDqZpMejIS7Kek2HU%2FBl%2B4YU
%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: maandag 28 november 2022 15:27
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> > ; art 5 1-2e
art 5 1-2e pzh.nl <mailto: m art 5 1-2e pzh.nl> >
Onderwerp: FW: Melding mogelijk datalek A 94293

Van: loket@pzh.nl <mailto:loket@pzh.nl> <loket@pzh.nl <mailto:loket@pzh.nl> >
Verzonden: maandag 28 november 2022 15:26:49 (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Melding mogelijk datalek A 94293

Beste collega,

Er is een melding gedaan van een mogelijk datalek:

Zie voor meer informatie:
Activiteitnummer: A 94293
Wijzigingsnummer: W22 11 00349

Hier kan je de activiteit <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fpvzh.topdesk.net%2Ftas%2Fsecure%2Fcontained%2Fchangeactivity%3Funid%3Da6506357e41d4c63b809565f4f1aa31e&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl%7Ccb08420103c1434ec09908dad44986b5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638055709511532297%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=3KTBAHqqNwbkdBnhi%2BIkeEJ3P%2FvZ2AeLa0qFNt%2BXI0U%3D&reserved=0> bekijken.

Met vriendelijke groet,

<HTTPS://pvzh.topdesk.net/tas/images/email_footer.jpg>

Het Loket telefoon 070 4417777 pvzh.topdesk.net
<https://eur03.safelinks.protection ook.com/?url=https%3A%2F%2Fpvzh.topdesk.net%2F&data=05%7C01 art 5 1-2e art 5 1-2e 40pzh.nl%7Ccb08420103c1434ec09908dad44986b5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638055709511532297%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=GnJsgjLLc5KQm9LoDjh0fOsSsTGml1HrEczEnZL2Ej0%3D&reserved=0>

"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art 5 1-2e Bureau Realisatie Water en Groen)
Registratienummer van het incident	:	A 94293
Datum en tijdstip van de melding	:	28 november 2022 15:25 (ontvangst melding)
Route van de melding	:	vermissing ICT middel Security formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	1 december 2022 om 11:04 uur
Advies besproken met	:	Besproken met art 5 1-2e FG)
Strekking advies ter kennisgeving gedeeld met	:	Gedeeld met eenheid Privacy

Situatie

Bij vertrek in de middag (22 november 2022) vanuit gebouw A5 zaten de smartphone en het notitieboekje van de collega niet meer in haar tas. In het notitieboekje stonden werkaantekeningen geschreven. De collega is woensdag 30 november 2022 gebeld door de beveiliging dat de smartphone en het notitieboekje zijn gevonden door de schoonmaak bij dezelfde ruimte (A5/B5) als dat zij de spullen is kwijtgeraakt. De collega heeft de spullen donderdagmiddag (1 december 2022) opgehaald en op vrijdagochtend (2 decmber 20222) heeft zij Eenheid Privacy bericht dat de smartphone niet is gewist.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	De smartphone is beveiligd met een toegangscode. Dus lijkt het onwaarschijnlijk dat er persoonsgegevens raadpleegbaar zijn geweest.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Onbekend.
Welke persoonsgegevens betreft het?	Onbekend.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in	Onbekend.

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met

Vraag	Antwoord
artikel 9 AVG?	
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Onbekend.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Onbekend.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Onbekend.
Betreft het een datalek?	Ja.
Ondernomen beperkende maatregelen.	Onbekend.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Geen.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van

oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.

[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval
De smartphone is beveiligd met een toegangscode en een week later teruggevonden op dezelfde plek. Dus het lijkt onwaarschijnlijk dat er persoonsgegevens raadpleegbaar zijn geweest.

Conclusie en advies
De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:
- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt NIET gemeld bij de Autoriteit Persoonsgegevens of betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.


provincie
Zuid-Holland

Van: art 5 1-2e
Verzonden: 2023-09-27 16:55:37+00:00
Aan: art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: FW: art 5 1-2e heeft ‘Memo Data IDMS’ met u gedeeld
"
Beste collega’s,

Ik heb een eerste aanzet gedaan. Er moet ongetwijfeld nog aan gesleuteld worden. Ik kijk er morgen weer naar

@art 5 1-2e <mailto :art 5 1-2e pzh.nl> : we hebben afgesproken voor art 5 1-2e een memo over de ontstane situatie en de ingestelde acties te schrijven die hij kan delen met anderen

@art 5 1-2e <mailto :art 5 1-2e pzh.nl> : ik neem je ter info even mee in de e-mail

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto :art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%art 5 1-2eart 5 1-2e40pzh.nl%7C02071592e4a04d74a08d08dbbf69cf46%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638314233391134114%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=1rncyeN50gu4oPGj5Im5EeauX2iahJ2uyI1ADkUeki8%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: woensdag 27 september 2023 15:51
Aan: art 5 1-2e art 5 1-2e @pzh.nl>; art 5 1-2e <art 5 1-2e pzh.nl>; art 5 1-2e <art 5 1-2e pzh.nl>
Onderwerp: art 5 1-2e heeft ‘Memo Data IDMS’ met u gedeeld

art 5 1-2e heeft een bestand met u gedeeld

Work in progress

<https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?url=https%3A%2F%2Fpzh-my.sharepoint.com%2F%3Aw%3A%2Fg%2Fpersonal%2art 5 1-2e%2FEUNQdFEu98hPlkVz-rlfDdIBdjnsIZ5pLyT1Sb_KTHDvdw%3Fe%3D4%253ad4CJ1W%26fromShare%3Dtrue%26at%3D9&data=05%7C01%art 5 1-2eart 5 1-2e40pzh.nl%7C02071592e4a04d74a08d08dbbf69cf46%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638314233391134114%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3

D%7C3000%7C%7C%7C&sdata=QA68OKAFMkSeEtc11KXNomAEJhH6uickr2e9BHevnJo
%3D&reserved=0>

Memo Data IDMS <https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?
url=https%3A%2F%2Fpzh-my.sharepoint.com%2F%3Aw%3A%2Fg%2Fpersonal
%art 5 1-2e2FEUNQdFEu98hPlkVz-rlfDdIBdjnsIZ5pLyT1Sb_KTHDvdw%3Fe
%3D4%253ad4CJ1W%26fromShare%3Dtrue%26at%3D9&data=05%7C01%art 5 1-2eart 5 1-2e40pzh.nl
%7C02071592e4a04d74a08d08dbbf69cf46%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638314233391134114%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=QA68OKAFMkSeEtc11KXNomAEJhH6uickr2e9BHevnJo
%3D&reserved=0>

Deze koppeling werkt alleen voor de directe geadresseerden van dit bericht.

<https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?url=https%3A%2F
%2Fpzh-my.sharepoint.com%2F%3Aw%3A%2Fg%2Fpersonal%art 5 1-2e
%2FEUNQdFEu98hPlkVz-rlfDdIBdjnsIZ5pLyT1Sb_KTHDvdw%3Fe%3D4%253ad4CJ1W%26fromShare
%3Dtrue%26at%3D9&data=05%7C01%art 5 1-2eart 5 1-2e40pzh.nl
%7C02071592e4a04d74a08d08dbbf69cf46%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638314233391134114%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=QA68OKAFMkSeEtc11KXNomAEJhH6uickr2e9BHevnJo
%3D&reserved=0>

Privacyverklaring <https://eur03.safelinks.protection.outlook.com/?url=https%3A
%2F%2Fprivacy.microsoft.com%2Fprivacystatement%2F&data=05%7C01%art 5 1-2eart 5 1-2e
%40pzh.nl
%7C02071592e4a04d74a08d08dbbf69cf46%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638314233391134114%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=dinml3iAMaDgVV8f7NkkxRtlUB72HascrWFQ7%2BB0DmE
%3D&reserved=0>

<https://northeuroper-notifyp.svc.ms:443/api/v2/tracking/method/View?mi=TY6Y7-
ZiA0WbxCyGVfYM7Q>
"


provincie
Zuid-Holland

Van: art 5 1-2e
Verzonden: 2023-09-29 11:45:10+00:00
Aan: art 5 1-2e
CC: art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: FW: art 5 1-2e heeft ‘Memo Data IDMS’ met u gedeeld
"
Hoi art 5 1-2e

Ik denk dat de brief klaar is voor jouw review. Ik hoor graag je reactie.

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7C00c5900bc3b14c3d79ad08dbc0d0c5f7%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638315775134148051%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=sIFxx2mefVSi%2BvI0DbhDRol0XSKA8XkJWPcm3Iw4UIk
%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e
Verzonden: vrijdag 29 september 2023 10:33
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e
< art 5 1-2e pzh.nl>
CC: art 5 1-2e art 5 1-2e)pzh.nl>
Onderwerp: FW: art 5 1-2e heeft ‘Memo Data IDMS’ met u gedeeld

art 5 1-2e en art 5 1-2e hebben input geleverd. Willen jullie mij informeren zodra jullie input gereed is dan rond ik het concept af en kan het ter beoordeling naar art 5 1-2e

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7C00c5900bc3b14c3d79ad08dbc0d0c5f7%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7

C638315775134148051%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=sIFxx2mefVSi%2BvI0DbhDRol0XSKA8XkJWPcm3Iw4UIk
%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 29 september 2023 10:26
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
art 5 1-2e art 5 1-2e pzh.nl <mailt o art 5 1-2e @pzh.nl> >
derwerp: RE: art 5 1-2e heeft ‘Memo Data IDMS’ met u gedeeld

Mijn reacties en die van art 5 1-2e (de disclaimer) staan er in.

Groeten,
art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 29 september 2023 10:23
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >;
art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
art 5 1-2e art 5 1-2e pzh.nl <mail t art 5 1-2e pzh.nl> >
Onderwerp: Re: art 5 1-2e heeft ‘Memo Data IDMS’ met u gedeeld

ik heb mijn opmerking net telefonisch met art 5 1-2e gedeeld. Hij neemt het mee.

From: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Sent: Friday, September 29, 2023 9:41 AM
To: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
art 5 1-2e)pzh.nl <mailt o art 5 1-2e)pzh.nl> >
Subject: RE: art 5 1-2e heeft ‘Memo Data IDMS’ met u gedeeld

Ik kijk er nu naar art 5 1-2e

Groeten,
art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 29 september 2023 07:58
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >;
art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >;
art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e
art 5 1-2e)pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: RE: art 5 1-2e heeft ‘Memo Data IDMS’ met u gedeeld

Goedemorgen allen,

art 5 1-2e art 5 1-2e en art 5 1-2e kunnen jullie aangeven wanneer jullie je input hebben geleverd dan wel hebben meegelezen? Dan kan art 5 1-2e daarna met zijn expertise naar de brief kijken.

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7C00c5900bc3b14c3d79ad08dbc0d0c5f7%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638315775134148051%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=sIFxx2mefVSi%2BvI0DbhDRol0XSKA8XkJWPcm3Iw4UIk
%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: donderdag 28 september 2023 14:35
Aan: art 5 1-2e < art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> >; art 5 1-2e < art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> >; art 5 1-2e art 5 1-2e pzh.nl
<mailto art 5 1-2e pzh.nl> >
CC: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: art 5 1-2e heeft ‘Memo Data IDMS’ met u gedeeld

Ha art 5 1-2e en art 5 1-2e

art 5 1-2e heeft jullie zojuist toegang gegeven tot de memo die voor art 5 1-2e wordt
geschreven. Hiermee kunnen jullie meelezen en teksten aanleveren, redigeren.

@ art 5 1-2e <mailto : art 5 1-2e pzh.nl> , art 5 1-2e informeert je als memo in
concept klaar is.

Groeten,
art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: donderdag 28 september 2023 14:33
Aan: art 5 1-2e < art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> >; art 5 1-2e < art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> >; art 5 1-2e < art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> >
Onderwerp: art 5 1-2e heeft ‘Memo Data IDMS’ met u gedeeld

art 5 1-2e heeft een bestand met u gedeeld

Dit is het document dat art 5 1-2e met u heeft gedeeld.

<https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?url=https%3A%2F
%2Fpzh-my.sharepoint.com%2F%3Aw%3A%2Fg%2Fpersonal% art 5 1-2e
%2FEUNQdFEu98hPlkVz-rlfDdIBdjnsIZ5pLyT1Sb_KTHDvdw%3 fromShare
%3Dtrue%26at%3D9&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7C00c5900bc3b14c3d79ad08dbc0d0c5f7%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638315775134148051%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3

D%7C3000%7C%7C
%7C&sdata=06pWV9%2BIbGr4EjhSbVzxQyrBjTzvKwmtxJdhATc7d28%3D&reserved=0>

Memo Data IDMS <https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?
url=https%3A%2F%2Fpzh-my.sharepoint.com%2F%3Aw%3A%2Fg%2Fpersonal
%2 art 5 1-2e 2FEUNQdFEu98hPlkVz-rlfDdIBdjnsIZ5pLyT1Sb_KTHDvdw%3Fe
%3D4%253ajOYkgU%26fromShare%3Dtrue%26at%3D9&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7C00c5900bc3b14c3d79ad08dbc0d0c5f7%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638315775134148051%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C
%7C&sdata=06pWV9%2BIbGr4EjhSbVzxQyrBjTzvKwmtxJdhATc7d28%3D&reserved=0>

Deze koppeling werkt alleen voor de directe geadresseerden van dit bericht.

<https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?url=https%3A%2F
%2Fpzh-my.sharepoint.com%2F%3Aw%3A%2Fg%2Fpersonal% art 5 1-2e
%2FEUNQdFEu98hPlkVz-rlfDdIBdjnsIZ5pLyT1Sb_KTHDvdw%3 Share
%3Dtrue%26at%3D9&data=05%7C01% art 5 1-2e art 5 1-2e 40pzh.nl
%7C00c5900bc3b14c3d79ad08dbc0d0c5f7%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638315775134148051%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C
%7C&sdata=06pWV9%2BIbGr4EjhSbVzxQyrBjTzvKwmtxJdhATc7d28%3D&reserved=0>

Privacyverklaring <https://eur03.safelinks.protection.outlook.com/?url=https%3A
%2F%2Fprivacy.microsoft.com%2Fprivacystatement%2F&data=05%7C01% art 5 1-2e art 5 1-2e
%40pzh.nl
%7C00c5900bc3b14c3d79ad08dbc0d0c5f7%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638315775134148051%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=v5MKCfLoVLQMUo63FsbrTBz061IKEwOKp0a
%2BCCUoAI8%3D&reserved=0>

<https://northeuroper-notifyp.svc.ms:443/api/v2/tracking/method/View?
mi=d6c4DYN2gUivwtzLjz2DDg>
"


provincie
Zuid-Holland


provincie
Zuid-Holland

"Van: art 5 1-2e
Verzonden: 2019-03-19 13:30:21.365000+00:00
"Aan: Baljeu, J.N."
"CC: art 5 1-2e
Onderwerp: FW: terugkoppeling onderzoek registratie datalekken
"
Dag Jeannette,

Vandaag ontving ik bijgaande brief die wordt verstuur naar het College, aangaande het onderzoek dat de Autoriteit Persoonsgegevens in september heeft ingesteld naar de registratie van datalekken bij onder andere onze provincie.

In de brief wordt gemeld dat wij niet voldoen aan de richtlijnen van de AP in dezen. Dit strookt met mijn eigen waarneming. Ik was al in gesprek met een aantal betrokkenen binnen PZH over verbetering van de registratie.

Daarnaast vindt er op 25 april een sessie plaats bij de AP waarin zij nader ingaan op de onderzoeken en op de verbeteringen die plaats kunnen vinden.

Mijns inziens moet dit voor de zomer leiden tot een deugdelijke registratie van datalekken bij PZH. In juni, althans zo is de planning nu, wordt er vanuit de awareness campagne van I&A ook een maand lang aandacht besteed aan de bescherming van persoonsgegevens, en dus ook aan het melden van datalekken.

Mocht je nog vragen hebben over de brief dan hoor ik dat graag.

Met vriendelijke groet,

art 5 1-2e

Functionaris voor Gegevensbescherming

M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>

-Wanneer u de provincie Zuid-Holland een e-mail stuurt, ontvangt u binnen 2 werkdagen een reactie en binnen twee weken een antwoord. Al uw informatie wordt vertrouwelijk behandeld. Persoons- of adresgegevens worden uitsluitend gebruikt waarvoor u ze heeft verstrekt. Uw e-mailbericht wordt op een goede en veilige manier gearchiveerd.

-Vragen kunt u stellen via het contactformulier <https://www.zuid-holland.nl/contact/contactinformatie/> .

Van: art 5 1-2e autoriteitpersoonsgegevens.nl]
Verzonden: maandag 18 maart 2019 11:43
Aan: fg
Onderwerp: terugkoppeling onderzoek registratie datalekken

Geachte art 5 1-2e

Gisteren hebben wij de resultaten van ons verkennende onderzoek naar de registratie datalekken gepubliceerd, de Provincie Zuid-Holland was één van de onderzochte organisaties.

Afgelopen donderdag is een brief richting de verwerkingsverantwoordelijken/overheidsorganisaties gestuurd waarbij is aangegeven dat wij op zondag zouden gaan publiceren. Gezien wij de link eigenhandig aan de FG's wilden sturen is ervoor gekozen om vandaag (op maandag) FG's te informeren over de publicatie van het nieuwsbericht en het onderzoek zelf: https://autoriteitpersoonsgegevens.nl/nl/nieuws/kwaliteit-datalekregister-bij-overheidsorganisaties-loopt-nog-uiteen <https://autoriteitpersoonsgegevens.nl/nl/nieuws/kwaliteit-datalekregister-bij-overheidsorganisaties-loopt-nog-uiteen> .

Bijgevoegd zijn de resultaten van het verkennende onderzoek. Bijgevoegd is tevens de brief die aan het college van Gedeputeerde Staten is toegezonden. Zoals eerder al is aangegeven zal de AP geen individuele terugkoppeling geven aan de organisaties. We vertrouwen erop dat u kennis neemt van de stukken.

We nodigen iedere FG van de onderzochte organisaties uit voor een vrijblijvende sessie op donderdagmiddag 25 april van 15:00-17:00 om de best practices met elkaar door te spreken en om van elkaar te kunnen leren. We horen graag of u kunt deelnemen aan deze sessie.

Met vriendelijke groet,

art 5 1-2e

Senior inspecteur

art 5 1-2e autoriteitpersoonsgegevens.nl
<mailto:naam@autoriteitpersoonsgegevens.nl>
T art 5 1-2e
M
Bezuidenhoutseweg 30, 2594 AV Den Haag
Postbus 93374, 2509 AJ Den Haag
autoriteitpersoonsgegevens.nl <http://www.autoriteitpersoonsgegevens.nl/>

"

AUTORITEIT
PERSOONSGEGEVENS

AUTORITEIT
PERSOONSGEGEVENS

AP doet handreikingen om registratie datalekken te verbeteren

'Verantwoordingsplicht' onder de AVG

Sinds 25 mei 2018 is nieuwe privacywetgeving van toepassing, de Algemene verordening gegevensbescherming (AVG). De AVG legt de verantwoordelijkheid bij organisaties om aan te tonen dat ze aan de privacyregels voldoen. Eén van de verplichte maatregelen om aan de verantwoordingsplicht te voldoen is de verplichting tot het bijhouden van alle inbreuken in verband met persoonsgegevens, ofwel het bijhouden van een datalekregister. Dit staat in artikel 33, 5e lid AVG.

Het doel van deze documentatieverplichting is te stimuleren dat organisaties intern leren van eerdere inbreuken en maatregelen nemen om de kans op nieuwe inbreuken te verminderen. De documentatie biedt daarnaast handvatten om binnen de organisatie het gesprek aan te gaan in het kader van AVG-bewustzijn. Ook kan de AP als toezichthoudende autoriteit met de documentatie controleren of organisaties de meldplicht datalekken naleven.

Verkennend onderzoek van de AP

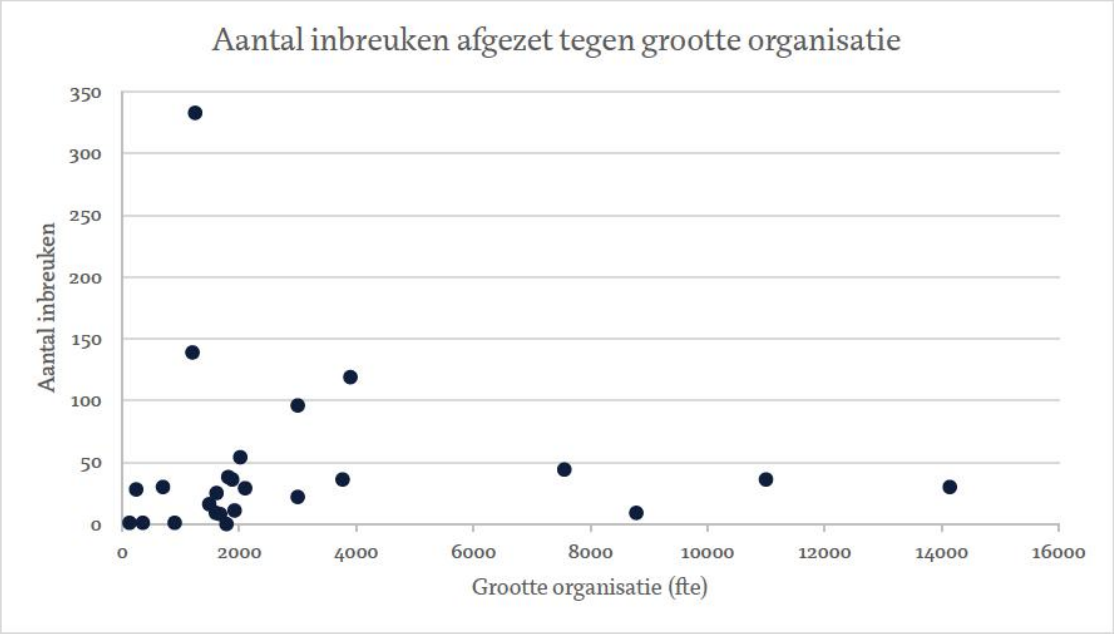
De AP heeft op 13 september 2018 26 overheidsorganisaties die veel persoonsgegevens verwerken gevraagd alle documentatie aan te leveren over de inbreuken op de beveiliging van persoonsgegevens in de periode van 25 mei tot aan 13 september 2018. Omdat de overheid een belangrijke informatiepositie en heeft eveneens een voorbeeldfunctie als het gaat om de naleving van wetgeving, is voor dit verkennend onderzoek gekozen voor de overheid. Doel van het onderzoek was om te verkennen op welke wijze organisaties invulling geven aan deze plicht. In deze rapportage deelt de AP haar beeld van de ontvangen documentatie, best en poor practices en aanbevelingen voor het bijhouden van deze registratie.

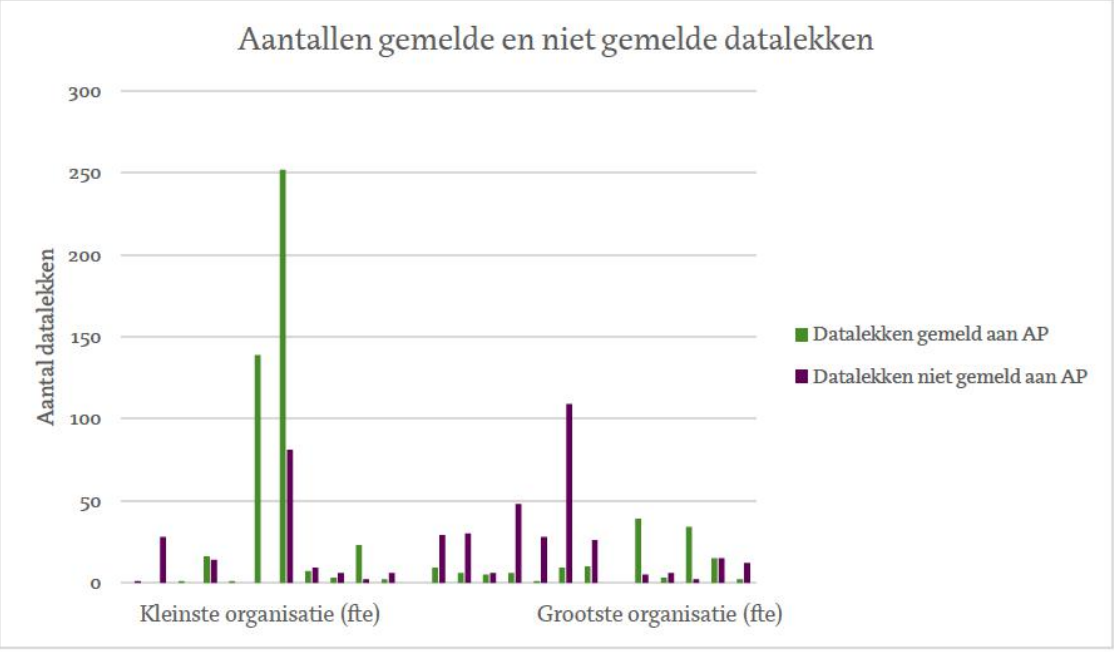
Beeld van de documentatie

De aangeleverde documentatie verschilde sterk per organisatie in opzet, inhoud en uitvoerigheid. Op basis van de vereisten uit artikel 33 AVG en de richtsnoeren datalekken hebben we alle registraties beoordeeld. Het valt de AP hoe de aantallen van de inbreuken verschillen. Van geen enkele inbreuk tot enkele honderden sinds 25 mei 2018 tot en met halverwege september 2018. De grootte van een organisatie lijkt niet veel te zeggen. Er kunnen verschillende redenen zijn waarom sommige organisaties meer inbreuken hebben gedocumenteerd dan anderen. In de volgende grafieken is af te lezen hoe de relatie is tussen het aantal gedocumenteerde inbreuken en de grote van de organisatie, de verhouding tussen de gemelde en niet gemelde datalekken, en het gemiddelde aantal datelekken per organisatievorm die wij hebben onderzocht.

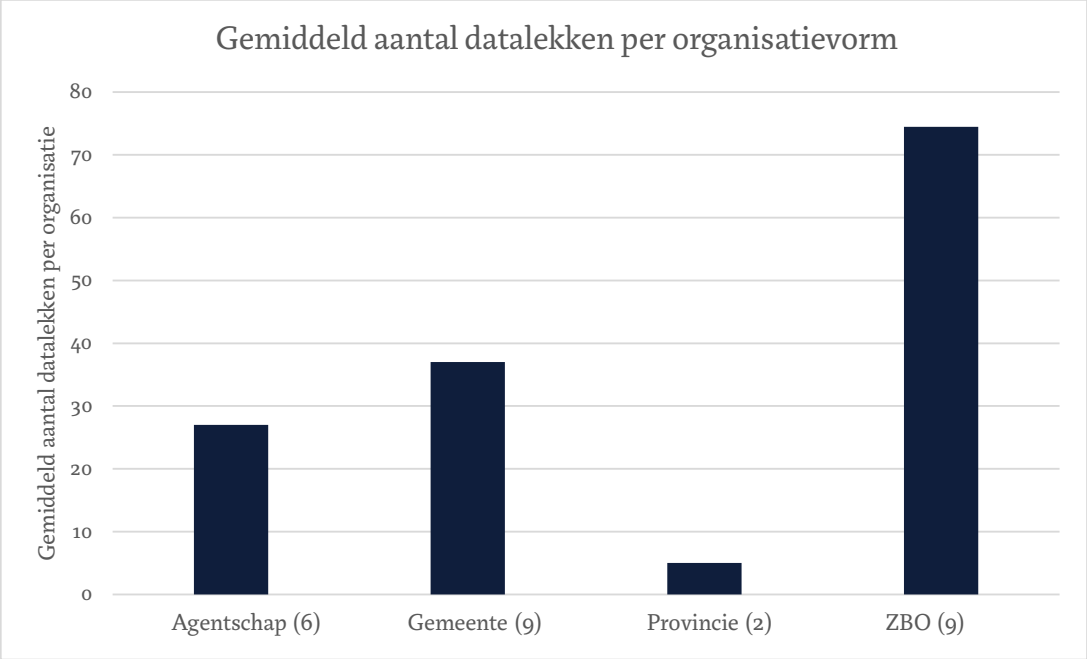
AUTORITEIT
PERSOONSGEGEVENS

De AP vat samen wat de meest voorkomende inbreuken, maatregelen en gevolgen zijn. De AP merkt hierbij wel op dat de voorbeelden die voortkomen uit de registers niet altijd voldoen aan de vereisten voor een volledige omschrijving van inbreuken, maatregelen en gevolgen.





AUTORITEIT
PERSOONSGEGEVENS



Samenvatting meest voorkomende inbreuken

De meest voorkomende inbreuken staan hieronder in afnemende volgorde van frequentie:

1 Post, fax of 'digitale' post die niet aankomt bij de juiste persoon waarbij het om meerdere redenen mis kan gaan, zoals: onjuiste adressering, juiste adressering maar onjuiste bezorging, dubbele of verkeerde brieven die per abuis worden meegestuurd in een envelop, of kwijtgeraakte post. Met 'digitale' post bedoelen we verzending van berichten via e-mail, berichtenboxen of klantportalen. Bij deze vormen van verwerkingen gaat het ook vaak om onjuiste adressering, per abuis naar de verkeerde klant gestuurde gegevens, of verkeerd van (andere betrokkenen) meegezonden bijlages. Voorbeelden van het type persoonsgegevens die niet, of bij de verkeerde persoon terechtkomen zijn divers zoals salarisgegevens, medische gegevens, NAW gegevens, BSN etc.[1]

2 Onbedoelde/onrechtmatige inzage van persoonsgegevens intern of extern. Voorbeelden zijn de publicatie van klantgegevens op het intranet waar alle medewerkers bij kunnen, het bijvoegen van een bijlage in het verkeerde dossier zodat medewerkers onbedoeld inzage kunnen verkrijgen in (bijzondere) persoonsgegevens die niet van hun eigen klanten zijn of bijvoorbeeld medewerkers van organisaties die onbedoeld inzage krijgen in verzuimgegevens van directe collega's.

3 Het verlies van documenten of informatiedragers (zoals telefoons, laptops of tablets). Voorbeelden hiervan zijn gestolen laptops en telefoons, maar ook verloren koffers met documenten.

[1] Dit komt ook overeen met eerdere publicaties over datalekken, hier te vinden: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-ontvangt-bijna-21000-datalekken-2018

AUTORITEIT
PERSOONSGEGEVENS

Voorbeelden van minder voorkomende inbreuken zijn: het vinden van documenten die (bijzondere) persoonsgegevens bevatten in een voor ieder toegankelijke prullenbak; printerproblemen waardoor gegevens kunnen worden ingezien door andere medewerkers of verdwijnen; hacks (4 vermoedelijke inbreuken als gevolg van hacks tegengekomen); phishing (2 vermoedelijke inbreuken als gevolg van phishing tegengekomen).

Samenvatting meest voorkomende gevolgen

De gevolgen worden vaak al meegenomen in de omschrijving van de gebeurtenis of van de feiten en omstandigheden. Sommige organisaties omschrijven bij de gevolgen ook de eventuele gevolgen die kunnen voortvloeien uit de inbreuken. Deze wijze van documenteren volgt waarschijnlijk uit het feit dat bij de beoordeling of een datalek moet worden gemeld aan de AP en/of de betrokkenen moet worden stilgestaan bij eventuele gevolgen voor de betrokkenen.[2] Het is verplicht om de daadwerkelijke gevolgen te documenteren, daarnaast mag de organisatie natuurlijk ook de eventuele gevolgen dan wel risico's opnemen.

De volgende omschrijvingen zijn voorbeelden van gevolgen die vaker voorkwamen in de registraties:

- Onbevoegde/ongeautoriseerde kennisname van persoonsgegevens;
- Blootstelling/risico op identiteitsfraude;
- Risico op stigmatisering, uitsluiting of discriminatie;
- Geen gevolgen voor de betrokkenen;
- Risico op reputatieschade;
- Gevolgen voor betrokkene(n) zijn groot vanwege expliciet verzoek om geheimhouding van de informatie betrokkenen bij de inbreuk;
- Ongunstige gevolgen voor de persoonlijke levenssfeer.

Samenvatting meest voorkomende genomen maatregelen

We constateren dat veel organisaties categorieën van maatregelen formuleren die zij herhaaldelijk registreren. We zien dat dezelfde corrigerende maatregel wordt ingezet voor dezelfde typen inbreuken.

De volgende omschrijvingen zijn voorbeelden van genomen maatregelen die vaker voorkwamen in de registraties:

- Zorgvuldiger omgaan met het versturen van documenten per post – aandacht aan besteden bij afdeling administratie;
- Meer awareness creëren voor zorgvuldiger omgaan met persoonsgegevens, wordt meegenomen in een organisatie brede awareness campagne;
- Medewerkers voorlichten over meer zorgvuldige omgang met social media;
- Extra checks/controles inrichten in het werkproces;
- Inzet van concrete maatregelen zoals verwijdering of vernietiging van de gegevens of extra beveiliging t.b.v. de data die betrokken is bij de inbreuk;

[2] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité, p.10

AUTORITEIT
PERSOONSGEGEVENS

- Postproces verbeteren;
- Informatie is door verkeerde ontvanger vernietigd;
- Het interne proces is geëvalueerd;
- De gestolen/verloren informatiedrager is vanaf een afstand gewist.

De poor en best practices

Grofweg 16 van de 26 registers bevatten – in meer of mindere mate – de in artikel 33, vijfde lid, AVG genoemde basiselementen: alle inbreuken met inbegrip van de feiten daaromtrent, de gevolgen van het lek en de genomen corrigerende maatregelen. De AP ziet ruimte voor verbetering van het aantal registraties dat aan de vereisten voldoet.

De AP ziet daarin aanleiding om meer uitleg te geven over wat een goede en slechte uitvoering van de documentatieplicht is, inclusief voorbeelden. Meer uitleg en voorlichting over de registratieplicht draagt bij aan de juiste naleving van deze verplichte documentatie en het adequaat bijhouden van deze documentatie kan helpen bij het verminderen van (de kans op) toekomstige datalekken. Tijdens onze beoordeling zijn we bepaalde aspecten in registraties tegengekomen die we graag delen zodat organisaties hiervan kunnen leren.

Poor practices

- Voorkom als organisatie een onduidelijke, (te) beperkte of onvolledige omschrijving van de (feiten van) het incident, de gevolgen en genomen corrigerende maatregelen.

Bijvoorbeeld een beperkte of onbegrijpelijk omschrijving van feiten zoals: '3-P-wet/wmo dossiers', 'toegangspas', 'verkeerd adres', 'scholingslening', en 'naamgebruik DVL'. Door het gebruik van dit soort afkortingen en (zeer) korte omschrijving van feiten wordt het niet duidelijk wat er is gebeurd.

- Voorkom als organisatie een onduidelijke, (te) beperkte of onvolledige omschrijvingen bij het omschrijven van de gevolgen.

Bijvoorbeeld: onduidelijke omschrijving van gevolgen zoals: er sprake van 'geen' risico, een 'verwaarloosbaar', 'laag', 'midden', of 'hoog' risico', zonder motivering waarom er geen risico's worden gezien of welke risico's wel worden onderkend.

- Voorkom als organisatie het niet opnemen van corrigerende maatregelen en de verwarring tussen verschillende maatregelen die wel worden opgenomen. Maak expliciet onderscheid tussen corrigerende en preventieve maatregelen.

Sommige organisaties vermelden alleen preventieve maatregelen, geen corrigerende maatregelen om bijvoorbeeld de gevolgen van het huidige incident te herstellen, al is dat onderscheid niet altijd even scherp.

AUTORITEIT
PERSOONSGEGEVENS

Verschil is dus dat sommige organisaties bijvoorbeeld gegevens m.b.t. de inbreuk vernietigen als corrigerende maatregel. Anderen vermelden bijvoorbeeld als preventieve maatregel voor het voorkomen van toekomstige inbreuken dat zij het postproces hebben geëvalueerd. Zorg ervoor dat duidelijk onderscheid wordt gemaakt tussen de (verplichte) corrigerende maatregelen en preventieve maatregelen.

- Voorkom versnippering van onderdelen van registraties, verschil in detailniveau en wisselende kwaliteit van registratie, dit kan zorgen voor een onoverzichtelijke geheel. De kwaliteit en bruikbaarheid van het register vermindert hierdoor.

Veel organisaties hebben niet één overzicht overgelegd en registreren de informatie niet in één overzichtelijk document. Een voorbeeld hiervan is dat door een organisatie een aparte lijst werd aangeleverd met vermiste mobiele telefoons waarbij het in het totale overzicht van inbreuken niet duidelijk werd of de vermiste telefoons daarin ook waren opgenomen. Een ander voorbeeld is dat sprake is van meerdere overzichten van verschillende 'typen' inbreuken waarbij niet duidelijk wordt wat de verhouding is tussen de verschillende overzichten.

Nog een voorbeeld is dat er soms voor elke individuele inbreuk gebruik wordt gemaakt van een meldingsformulier voor registratie waarbij het inhoudelijk detailniveau enorm verschilt per ingevuld formulier. Bij het ene meldformulier wordt er door een medewerker bijvoorbeeld uitgebreid bij alle kopjes informatie ingevuld, terwijl bij het andere meldformulier de helft van de onderwerpen wordt overgeslagen en zeer beknopt wordt beschreven wat de feiten, gevolgen en genomen maatregelen zijn. Sommige organisaties hebben alle informatie van alle inbreuken in één helder overzicht waarbij het detailniveau van de beschrijving en de kwaliteit een stuk meer uniform is. Als voor een medewerker bij de registratie alle eerdere registraties van inbreuken inzichtelijk zijn, kan dit bijdragen aan de uniformiteit van de registratie.

- Zorg ervoor dat de FG betrokken wordt bij de registratie. Bij de meeste registraties werd niet duidelijk of, en zo ja in welke mate, de FG betrokken is bij de datalekregistratie. Het Europees privacytoezichthoudersverband raadt aan dat een FG bijvoorbeeld kan bijdragen aan het opzetten van een structuur voor de registratie en bij de administratie die voortvloeit uit de datalekregistratie.[3]

Best practices

- Omschrijving waarom bepaalde datalekken wel of niet gemeld zijn aan de AP en/of aan de betrokkene(n). De EDPB beveelt dit ook aan in haar richtsnoeren[4], de verwerkingsverantwoordelijke kan op deze wijze aangeven waarom bepaalde datalekken wel of niet gemeld zijn en aldus aantonen dat zij de verplichting om bepaalde datalekken te melden op de juiste wijze naleeft.
- Een uniforme registratiewijze draagt bij aan de kwaliteit van de datalekregistratie, dit kan bijvoorbeeld worden bevorderd door handleidingen, trainingen of stroomschema's voor de registratie van datalekken.

[3] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité, p.32
[4] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité, P.31

AUTORITEIT
PERSOONSGEGEVENS

Slechts enkele organisaties lijken duidelijke regels en of instructies te hebben ten aanzien van de wijze van registreren. Hierdoor kan de registratie van de verschillende medewerkers per lek (enorm) verschillen. Dat maakt het leren en aanpakken van structurele fouten/zwakke plekken lastig. Een categorisering van de soorten datalekken (naar aard, gevolgen, betrokkenen) en mogelijke maatregelen zou al kunnen helpen om ook ontwikkelingen in de tijd te kunnen monitoren en op grond daarvan verbeteringen door te voeren. Daarnaast kan het helpen om de registratie overzichtelijk en inzichtelijk te maken voor alle medewerkers zodat zij het registratieoverzicht kunnen consulteren voorafgaand aan hun eigen registratie. Dit kan zorgen voor een meer uniforme registratiewijze. Andere manieren waarop een uniforme registratiewijze kan worden bevorderd is door middel van handleidingen of trainingen. De FG kan bijvoorbeeld ook bijdragen aan het opzetten van een structuur voor de registraties.[5]

Daar waar er gebruik wordt gemaakt van een uniforme registratiewijze is de registratie gemakkelijker leesbaar. De organisatie kan zo beter leren van de inbreuken die hebben plaatsgevonden en van de stappen die zijn genomen ter herstel van het lek, dan wel ter voorkoming van een lek in de toekomst.

- Zorg ervoor dat de registratie maximaal benut wordt en omschrijf zowel specifieke corrigerende maatregelen als preventieve maatregelen ter voorkoming van nieuwe datalekken. Neem deze maatregelen bijvoorbeeld mee in de plan-do-check/learn-act cyclus.

Voorbeelden van helder omschreven corrigerende en preventieve maatregelen zijn:
- Het proces van doorgeleiding is geëvalueerd. De gegevens zijn onverwijld verwijderd uit de openbare pagina's. Tevens bleek bij nader onderzoek dat slechts twee collega's die gemachtigd waren om de gegevens in te zien daadwerkelijk hadden ingezien;
- De telefoon was beveiligd met een pincode en is op afstand gewist. Tevens is de synchronisatie van de telefoon uitgezet;
- De ontvanger is verzocht om de data te vernietigen. Daarnaast hebben de verantwoordelijke managers en de postkamer samen gezeten om hier bewustwording over te creëren in het proces.

- Het registreren of, en zo ja welke, andere organisaties (bijvoorbeeld medeverwerkingsverantwoordelijken, verwerkers of sub-verwerkers) betrokken zijn geweest bij een inbreuk kan bijdragen aan het lerend vermogen van de organisaties ten aanzien van wat men in de toekomst kan doen om datalekken te voorkomen. Dit kan bijvoorbeeld ook worden meegenomen wanneer er nieuwe verwerkersovereenkomsten gesloten worden met de desbetreffende verwerkers.

[5] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité, p. 32

AUTORITEIT
PERSOONSGEGEVENS

Aanpak onderzoek

Voordat de AVG van kracht werd gold de verplichting tot het bijhouden register alléén voor datalekken die gemeld moesten worden bij de Autoriteit Persoonsgegevens (AP). Onder de AVG moeten twee soorten inbreuken worden gedocumenteerd: (1) inbreuken gemeld moeten worden bij de AP en (2) inbreuken die niet hoeven te worden gemeld bij de AP.[6] De documentatie bevat over deze inbreuken in ieder geval de volgende informatie:

- de feiten omtrent de inbreuk in verband met persoonsgegevens[7];
- de gevolgen daarvan;
- de genomen corrigerende maatregelen.

De AP heeft bij dit verkennende onderzoek de aangeleverde documentatie beoordeeld op enkele aspecten uit artikel 33 van de AVG en op de richtsnoeren van het Europese privacytoezichthoudersverband over datalekken. Daarbij heeft de AP gekeken naar:

- de omschrijving van de inbreuken;
- of de feiten voldoende duidelijk omschreven waren, inclusief de vermelding van de oorzaak van de inbreuk, het verloop van de inbreuk, en de getroffen persoonsgegevens;[8]
- of de gevolgen van de inbreuken en de genomen corrigerende maatregelen zijn opgenomen.

Naast deze vereisten beveelt het Europese privacytoezichthoudersverband aan de motivering voor de besluiten over een inbreuk vast te leggen. Dit zijn bijvoorbeeld besluiten om een inbreuk niet of juist wel te melden aan de toezichthouder[9] of over de vraag of de betrokkene(n) moeten worden geïnformeerd.[10]

De AP heeft vanwege het gebrek aan motivering in de toegezonden registraties in dit onderzoek niet kunnen nagaan of de inbreuken die zijn gemeld daadwerkelijk gemeld hadden moeten worden, of dat inbreuken gemeld hadden moeten worden die niet zijn gemeld. Ook heeft de AP niet kunnen nagaan of de inbreuken terecht of onterecht zijn gemeld aan de betrokkenen vanwege een gebrek aan motivering in de toegezonden registraties.

[6] Inbreuken dienen te worden gemeld aan de toezichthouder, tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

[7] De Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité verduidelijken dat onder deze 'feiten' onder meer worden verstaan: "de oorzaken, het verloop en de getroffen persoonsgegevens" p.30-31

[8] De Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité verduidelijken dat onder deze 'feiten' onder meer worden verstaan: "de oorzaken, het verloop en de getroffen persoonsgegevens". P.30-31

[9] Zie Richtsnoeren p.27: "Met name wanneer een inbreuk niet is gemeld, moet de motivering voor dat besluit worden gedocumenteerd."

[10] Zie Richtsnoeren p.27: "Indien de verwerkingsverantwoordelijke van mening is dat aan een van de voorwaarden van artikel 34, lid 3, is voldaan, moet hij afdoend bewijs kunnen leveren dat dit het geval is."

AUTORITEIT
PERSOONSGEGEVENS

Aanlevering van de documentatie

De AP heeft voor dit onderzoek alleen de documentatieplicht zoals neergelegd in de AVG verkend. Deze documentatieplicht geldt sinds 25 mei 2018. Het lag daarom in de rede dat de documentatie bij het verzoek in september 2018 gereed zou liggen waardoor het ook direct aangeleverd kon worden.

Op 13 september 2018 heeft de Autoriteit Persoonsgegevens 26 overheidsorganisaties aangeschreven. De AP heeft van hen allemaal een reactie ontvangen; 24 organisaties hebben hun datalekregistratie overgelegd, twee organisaties hebben aangegeven dat zij geen documentatie hebben omdat zij aangeven geen inbreuken te hebben gehad in de periode van 25 mei 2018 tot 13 september 2018.

Van 26 aangeschreven organisaties hebben echter slechts 8 de documentatie binnen de gestelde termijn aangeleverd. Drie organisaties hebben de documentatie een dag later aangeleverd. De overige 16 waren een week of meer later. De reden voor die (ver)late aanlevering van de documentatie was dat sommige organisaties voor zichzelf na moesten gaan welke documenten zij zouden moeten overleggen en in welke vorm deze konden worden aangeleverd. Daarnaast bleek dat de brief van AP pas na enige tijd op de juiste plek of bij de juiste persoon binnen de organisatie terecht kwam.

De documentatie is in de meeste gevallen digitaal en al dan niet beveiligd, aangeleverd. Een deel van de betreffende verwerkingsverantwoordelijken heeft contact opgenomen met de AP over de vorm waarin of wijze waarop, de documentatie aangeleverd moest worden. De AVG stelt geen eisen aan de wijze waarop de informatie gedocumenteerd moet worden en verwerkingsverantwoordelijken mogen dus zelf de vorm kiezen.

Afsluitend

De steekproef kent een beperkte opzet en leent zich derhalve niet voor brede conclusies . Daarom volstaan we met een beknopt samenvatting. Wel hebben we naar aanleiding van dit onderzoek een aantal praktische tips geformuleerd.

Uit het voorgaande blijkt dat alle aangeschreven verwerkingsverantwoordelijken, op twee na, documentatie met betrekking tot datalekken op verzoek van de AP hebben aangeleverd. Deze twee organisaties geven aan geen inbreuken te hebben gehad tussen 25 mei 2018 en 13 september 2018 die geregistreerd kunnen worden. Daardoor konden zij ook geen registratie aanleveren.

Dit is de eerste keer dat de AP aandacht besteedt aan de naleving van deze documentatieplicht. Zij hoopt met dit verkennend onderzoek bij te dragen aan de naleving hiervan. De AP vindt het belangrijk dat deze verantwoordingsplicht goed wordt nageleefd, een adequate registratie is namelijk niet alleen verplicht op grond van de AVG, maar kan bijdragen aan vermindering van het aantal inbreuken. De AP kan daarnaast bij het controleren van de meldplicht datalekken het register opvragen bij verwerkingsverantwoordelijken.

Alle aangeschreven organisaties krijgen deze rapportage toegestuurd, waar nodig zal de AP contact opnemen met overheidsorganisaties (en hun FG) die hun registratie kunnen verbeteren naar aanleiding van deze rapportage.

Tien tips voor een goede registratie

De beoordeling van de registraties leiden tot de volgende lijst met praktische tips voor een goede registratie:

1. Omschrijf incidenten, de gevolgen en de corrigerende maatregelen duidelijk en volledig;
2. Maak expliciet onderscheid tussen corrigerende en preventieve maatregelen. Leg corrigerende maatregelen altijd vast in het datalekregister. Het kan nuttig zijn deze maatregelen mee te nemen in de plan-do-check/learn-act cyclus;
3. Voorkom versnippering van registraties; maak één overzichtelijke registratie die voor elk organisatieonderdeel tot op hetzelfde inhoudelijke detailniveau wordt ingevuld. Overweeg bijvoorbeeld om de registratie inzichtelijk te maken voor alle medewerkers zodat zij het registratieoverzicht kunnen consulteren voordat zij zelf iets registreren;
4. Neem per incident op of de functionaris voor de gegevensbescherming (FG) betrokken is, en zo ja in welke mate. Elke overheidsorganisatie heeft verplicht een FG.
5. Neem per incident op of het datalek is gemeld bij de AP en betrokkenen en motiveer daarbij waarom dat wel of niet is gebeurd;
6. Wees transparant richting getroffen personen als er een datalek is geweest. Communiceer hier doeltreffend en tijdig over. Bewaar het bewijs van die mededeling en neem deze op in de registratie.
7. Stel een handleiding op of verzorg een training voor de medewerkers die de datalekregistratie invullen. Deze instructie kan onderdeel uitmaken van een gedocumenteerde meldingsprocedure voor de meldplicht datalekken.
8. Leg vast welke andere organisaties betrokken zijn geweest bij een inbreuk (bijvoorbeeld medeverwerkingsverantwoordelijken, verwerkers of sub-verwerkers). Dit is handig als een organisatie nieuwe verwerkersovereenkomsten sluit met de desbetreffende verwerkers.
9. Overweeg datalekken in te delen naar aard, gevolgen en betrokkenen en mogelijke maatregelen;
10. Bespreek de datalekregistratie regelmatig op het juiste niveau binnen de organisatie als onderdeel van een plan-do-check/learn-act cyclus. Zo kunnen organisaties leren van fouten. De FG kan bij deze besprekingen een actieve rol vervullen.

AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk
Provincie Zuid-Holland
t.a.v. het college van Gedeputeerde Staten
Postbus 90602
2509 LP Den Haag

Datum
14 maart 2019

Ons kenmerk
Z2018-19205

Contactpersoon
art 5 1-2e

Onderwerp
Publicatie verkennend onderzoek 'registratie van datalekken'

Geacht college,

Graag vragen wij uw aandacht voor het volgende.

Op 13 september 2018 is uw organisatie benaderd om mee te werken aan een verkennend onderzoek naar de registratie van datalekken. Het doel van het onderzoek is om inzicht te krijgen in de wijze waarop overheidsorganisaties invulling geven aan hun registratieverplichting op grond van artikel 33, lid 5, AVG. De provincie Zuid-Holland was een van de 26 organisaties die de Autoriteit Persoonsgegevens (verder: AP) heeft aangeschreven.

Het verkennende onderzoek is thans afgerond. De AP heeft alle registraties bekeken en op basis hiervan een rapportage opgesteld. In deze rapportage zijn de verwerkingsverantwoordelijken niet herleidbaar opgenomen. Via deze weg willen wij u laten weten dat deze rapportage op zondag 17 maart gepubliceerd wordt. Wij nodigen u als verwerkingsverantwoordelijke en uw functionaris gegevensbescherming (FG) uit om kennis te nemen van dit stuk.

We willen u meegeven dat uw registratie niet voldoet aan de eisen neergelegd in artikel 33, vijfde lid, AVG. We verwachten van u, en uw FG, dat op basis van de informatie neergelegd in de rapportage uw registratie zal worden aangepast. Een adequate registratie is namelijk niet alleen verplicht op grond van de AVG, maar kan bijdragen aan vermindering van het aantal inbreuken.

De AP organiseert een rondetafelbijeenkomst voor de FG's van de 26 onderzochte organisaties naar aanleiding van de publicatie. Tijdens deze bijeenkomst wordt gelegenheid geboden om in gesprek te gaan

AUTORITEIT
PERSOONSGEGEVENS

Datum
14-3-2019

Ons kenmerk
Z2018-19205

over best practices, praktische tips en mogelijkheden tot het verbeteren van de registratie van datalekken. Deze sessie zal plaatsvinden op donderdagmiddag 25 april 2019 op ons kantoor in Den Haag. Uw FG ontvangt hier een persoonlijke uitnodiging voor.

Indien u vragen heeft naar aanleiding deze brief, dan kunt u contact opnemen met bovengenoemde contactpersoon.

Hoogachtend,
Autoriteit Persoonsgegevens,
Namens deze,

art 5 1-2e


provincie
ZUID HOLLAND

Van: art 5 1-2e
Verzonden: 2023-09-22 11:41:02.156000+00:00
Aan: art 5 1-2e
CC:
Onderwerp: FW: Vertrouwelijk - update data
"
Ter informatie art 5 1-2e Ik heb art 5 1-2e reeds geïnformeerd, m.u.v. het gegeven dat het script nu loopt. Komt straks tijdens het overleg wel.

Groet,

art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: vrijdag 22 september 2023 11:29
Aan: art 5 1-2e <art 5 1-2e pzh.nl>
CC: art 5 1-2e <art 5 1-2e pzh.nl>
Onderwerp: RE: Vertrouwelijk - update data

Hoi art 5 1-2e

Het script loopt nu. Het draaien duurde vorige keer wel het hele weekend, maar het zou nu iets sneller kunnen gaan omdat er minder items te doorzoeken zijn. art 5 1-2e houdt me op de hoogte.

Groet,

art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 22 september 2023 11:05
Aan: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
CC: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: FW: Vertrouwelijk - update data

Hoi art 5 1-2e

Zie onderstaande mail van mij. Het datalek is in ieder geval minder groot dan wat aanvankelijk als onderzoeksresultaat met jullie is gedeeld.

Groet,

art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 22 september 2023 10:59
Aan: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: Vertrouwelijk - update data

Ha art 5 1-2e

Thanks voor de update. Hopen dat de volgende resultaten meevallen.

Wel goed denk ik om dit ook met art 5 1-2e te delen voordat het overleg start.

Groet,

art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 22 september 2023 10:46
Aan: art 5 1-2e @pzh.nl <mailt o art 5 1-2e pzh.nl> >; art 5 1-2e art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e art 5 1-2e pzh.nl <mailt o art 5 1-2e @pzh.nl> >; art 5 1-2e pzh.nl <mailto art 5 1-2e pzh.nl> >
Onderwerp: Vertrouwelijk - update data

Hoi allen,

Zojuist met datateam en art 5 1-2e de onderzoeksresultaten gevalideerd. Gebleken is dat het script van art 5 1-2e met systeembeheersrechten is uitgevoerd. art 5 1-2e zal het script opnieuw draaien in het weekend i.o.m . art 5 1-2e

In Topdesk in de melding zelf was niet specifiek gevraagd om deze vink uit te schakelen voor het account dat zij voor onderzoeken gebruiken. Deze vink staat standaard aan voor Woo verzoeken. Het account zelf staat overigens standaard uit. Wel stond in de aangehechte mail in Topdesk dat het gaat om publieke rechten, maar dat is bij de verwerking over het hoofd gezien.

We hebben in de resultaten gekeken wat we tegen kwamen en zover zagen we alleen afgeschermde mappen en persoonlijke werkomgevingen. Dat is op zichzelf een opluchting, hoewel het nog steeds mogelijk is dat er honderden tot tienduizenden bestanden in het kader van dit lek onvoldoende zijn afgeschermd.

Er wordt voor volgende week een overleg gepland om de nieuwe resultaten te bekijken.

Met vriendelijke groet,

art 5 1-2e

Functioneel Beheer

art 5 1-2e

"

"Van: art 5 1-2e
Verzonden: 2020-05-28 20:36:40+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e ; art 5 1-2e
Onderwerp: FW: VERTROUWELIJK Concept advies datalek
"
Hallo art 5 1-2e

Nog een paar suggesties in de tekst, verder prima tekst.

Groet,

art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: donderdag 28 mei 2020 18:34
Aan: art 5 1-2e < art 5 1-2e pzh.nl> ; art 5 1-2e
art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: VERTROUWELIJK Concept advies datalek
Urgentie: Hoog

Hallo art 5 1-2e art 5 1-2e en art 5 1-2e

Bijgaand het advies naar aanleiding van het door Tessa gemelde datalek.

Graag jullie aanvullingen cq correcties hierop.

art 5 1-2e kun jij de status weergeven van het verwijderingsverzoek aan Google?

Ik zag dat het stuk rond 18:00 is verwijderd van het archiefweb.

De procedure is dat het advies wordt voorgelegd aan de concerndirecteur die is gemandateerd voor het nemen van een besluit.

Als conform wordt besloten, doe ik daarna de melding aan de Autoriteit Persoonsgegevens.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art 5 1-2e | M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl <http://www.zuid-holland.nl/>
"


provincie
ZUID HOLLAND

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Concept

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	M20 05 02572
Datum en tijdstip van de melding	:	Donderdag 28 mei 2020 15:32 uur
Route van de melding	:	Datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Donderdag 28 mei 2020 18:20 uur
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e privacy jurist)
Strekking advies ter kennisgeving gedeeld met	:	art 5 1-2e

Situatie

Publicatie op de website van de provincie Zuid-Holland van een (geheim) GS besluit met persoonsgegevens van ~~een~~ de burger aan wie het geadresseerd is. Het besluit is gepubliceerd op 13 mei 2020 om 12:00 uur.
Het datalek is ontdekt op 27 mei 2020 om ca 23.00 uur. De advocaat van betrokkene heeft bij de provincie een verzoek tot depublicatie gedaan.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	3 attributen
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend. Het besluit was op het internet gepubliceerd. @Vraag staat uit binnen I&A
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen, kopiëren, afdrukken, e-mailen
Welke persoonsgegevens betreft het?	Naam, adres, woonplaats, bedrag van de vaststelling.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot	Nee. De gegevens zijn gepubliceerd op het internet.

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.

Vraag	Antwoord
personeel van PZH? Zo ja, tot welke gebruikersgroepen?	
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Het is niet uit te sluiten dat de publicatie een risico oplevert voor betrokkene. De advocaat van de betrokkene heeft de provincie op de publicatie van de persoonsgegevens gewezen en een verzoek tot verwijdering gedaan.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja, in relatie tot de vertrouwelijkheid van de betreffende persoonsgegevens.
Betreft het een datalek?	Ja. Persoonsgegevens zijn ten onrechte ~~geopenbaard~~openbaar gemaakt.
Ondernomen beperkende maatregelen.	Het besluit is van de provinciale website verwijderd en ook uit het webarchief (https://zuidholland.archiefweb.eu) van de provincie.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Enkele regels zijn nog zichtbaar in de zoekresultaten van Google. Er wordt gewerkt aan een verwijderingsverzoek..

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.

[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval
Het besluit bevat een aan betrokkene uit te keren schadebedrag. Het openbaar worden van deze informatie in combinatie met de genoemde persoonsgegevens kan een nadelig effect hebben op de persoonlijke levenssfeer van betrokkene. Het is daardoor te kenmerken als persoonsinformatie van gevoelige aard. Door de advocaat van betrokkene is gevraagd om deze gegevens te depubliceren.

Conclusie en advies
Een datalek dient aan de Autoriteit Persoonsgegevens te worden gemeld als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de betrokkenen. Dat is hier naar ons oordeel het geval.

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert het Privacy team om:

- Het datalek te melden bij de Autoriteit Persoonsgegevens.
- De melding en beoordeling zoals gebruikelijk te administreren in het provinciale logboek.

"Van: art 5 1-2e
Verzonden: 2019-07-25 14:25:21+00:00
"Aan: art 5 1-2e
"CC: Baljeu, J.N."
Onderwerp: Fwd: Advies_in_kader_van_meldplicht_datalekken_10_05_2019
"
Dag art 5 1-2e

Dankjewel, ik stem in met je advies.

Hartelijke groet, art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

Van: art 5 1-2e

Verstuurd: donderdag 25 juli 13:56

Onderwerp: Advies_in_kader_van_meldplicht_datalekken_10_05_2019

Aan: art 5 1-2e

Cc: Baljeu, J.N.

Dag art 5 1-2e

Naar aanleiding van het datalek binnen de applicatie Zorg van de Zaak, stuur ik je, bij afwezigheid van art 5 1-2e bijgaand mijn advies.

Met vriendelijke groet,

art 5 1-2e
Functionaris voor Gegevensbescherming
M
art 5 1-2e
<mailto: art 5 1-2e pzh.nl>
art 5 1-2e pzh.nl
Provincie Zuid-Holland | Zuid-Hollandplein 1
Postbus 90602 | 2509 LP Den Haag
<http://www.zuid-holland.nl/>
www.zuid-holland.nl


provincie
ZUID HOLLAND


provincie
ZUID HOLLAND

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: DEFINITIEF

Melding gegevens

Naam melder	:	art 5 1-2e
Registratienummer van het incident	:	M19 05 01087
Datum en tijdstip van de melding	:	10 mei 2019
Route van de melding	:	Mondeling gemeld, vervolgens melding in Topdesk aangemaakt door art 5 1-2e

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	25 juli 2019, 12:45 uur
Advies besproken met	:	art 5 1-2e
Advies ter kennisgeving gedeeld met	:	

Situatie

(*korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*
Het betreft een situatie met betrekking tot meldingen vanuit het systeem Zorg van de Zaak omtrent ziekmeldingen van werknemers. Mails met betrekking tot ziekmeldingen of voortgangsgesprekken met ziek gemelde werknemers zijn verstuurd aan de verkeerde leidinggevende. De oorzaak voor het foutief versturen is gelegen in een verandering bij de leverancier. Hierdoor werden mutaties bij medewerkers-leidinggevende relaties niet verwerkt. De inbreuken hebben plaatsgevonden in de periode januari 2019 tot april 2019. Nadat de inbreuken door een voormalig leidinggevende zijn gemeld, zijn er technische maatregelen getroffen. De melding is echter pas in mei 2019 mondeling gedaan bij de FG. Door een ongelukkige samenloop van omstandigheden, de melding van dit datalek viel samen met de datalek melding van het WBR, is deze melding niet opgemerkt door de behandelaren. Op 23 juli 2019 is de melding weer onder de aandacht gekomen van het privacy team. Bij navraag bij P&O bleek dat de inbreuk nog steeds voortduurt. Bij de reparatie-actie in april is wel 95% van alle medewerkers, met hun leidinggevende, dicht gezet, maar per ongeluk is er nog een klein deel vergeten. De technische maatregelen lijken geen effect te hebben gehad. Door de leverancier wordt wederom een poging gedaan om de juiste technische maatregelen door te voeren. Op 24 juli 2019 is ook het resterende deel dichtgezet.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Waarschijnlijk betreft het een beperkte groep ziekgemelde weknemers
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	<10
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen, e-mailen

Vraag	Antwoord
Welke persoonsgegevens betreft het?	Naam, geboortedatum, ID, geslacht, voorletters, adres, telefoonnummer, beperkte medische gegevens
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Beperkte medische gegevens
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja, (oud-)bureauhoofden; voor zover bekend. Het vergt diepgaand onderzoek om te achterhalen, zo dat al mogelijk is, van welke medewerkers de gegevens onterecht zijn verwerkt.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Waarschijnlijk niet, beperkte medische gegevens ingezien door bureauhoofden die uit hoofde van hun functie deze informatie kunnen zien van hun eigen medewerkers.
Betreft het een beveiligingsincident?	Ja Doordat de organisatiewijzigingen niet zijn doorgevoerd, stonden de toegangsrechten niet goed.
Betreft het een datalek?	Ja Er is sprake van ongeoorloofde toegang / inzage in persoonsgegevens
Ondernomen beperkende maatregelen.	Er zijn door de leverancier technische maatregelen genomen, die na de eerste reparatieslag overigens geen effect gesorteerd blijken te hebben.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	De leverancier onderneemt een nieuwe poging om de juiste technische maatregelen door te voeren. Op 24 juli 2019 zijn alle mogelijke mailrelaties naar leidinggevenden afgesloten. In samenspraak met de afdeling I&A, de leverancier en de afdeling P&O wordt gekeken naar een nieuwe oplossing waardoor de leidinggevenden wel weer op de juiste manier van informatie worden voorzien

Afweging

<u>Kaders</u>

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen indien bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse en advies

- Omdat de toegangsrechten het systeem Zorg van de Zaak niet goed aangebracht waren, is er sprake van een beveiligingslek.
- Omdat er persoonsgegevens in de documenten voorkomen, is er sprake van een datalek in de zin van de AVG.
- Gelet op de bevoegdheden die bureauhoofden hebben met betrekking tot inzage in documenten van Zorg van de zaak voor hun eigen medewerkers, is het onwaarschijnlijk dat de inbreuk een groot risico inhoudt voor betrokkenen.

Gezien de afwegingscriteria in de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679[3], komen we tot het oordeel dat:

- het datalek niet gemeld dient te worden bij de Autoriteit Persoonsgegevens.
- er geen melding wordt gedaan bij betrokkenen.

[3] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 – Groep Gegevensbescherming Artikel 29, versie 6 februari 2018

art 5 1-2e

Van: art 5 1-2e
Verzonden: september 2023 16:03
Aan: art 5 1-2e
Onderwerp: en...

Gevoeligheid: Privé

Daar issie!

art 5 1-2e
Hoofd concern- en interne communicatie

provincie Zuid-Holland

art 5 1-2e
art 5 1-2e @pzh.nl
linkedin.com/ art 5 1-2e art 5 1-2e
www.zuid-holland.nl/contact

Werkdagen: ma, di, wo, do, vr

Krachtig Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e zh.nl>
Verzonden: maandag, september 25, 2023 15:21
Aan: art 5 1-2e < art 5 1-2e @p zh.nl>; art 5 1-2e < art 5 1-2e @p zh.nl>; art 5 1-2e < art 5 1-2e @ pzh.nl>; art 5 1-2e < art 5 1-2e @pzh.nl >; art 5 1-2e < art 5 1-2e @p zh.nl>; art 5 1-2e < art 5 1-2e @p zh.nl>; art 5 1-2e < art 5 1-2e @pzh. nl>; art 5 1-2e art 5 1-2e < art 5 1-2e @p zh.nl>; art 5 1-2e < art 5 1-2e @pzh. nl>
Onderwerp: DE vragen...

Dag allemaal,

Deze vragen van de website van de Autoriteit Persoonsgegevens hadden jullie van me tegoed:

- Wat is de oorzaak van het datalek?
- Wanneer is het datalek ontstaan? En is het datalek nog steeds gaande?
- Hoe lang na het ontstaan van het datalek is het ontdekt? En hoe is het ontdekt?
- Wat voor soort persoonsgegevens zijn gelekt? Bijvoorbeeld naam, adres, e-mailadres, creditcardgegevens en/of bijzondere persoonsgegevens.
- Hoeveel persoonsgegevens zijn er (bij benadering) gelekt? Om hoeveel personen gaat het?
- Om wat voor groepen mensen gaat het? Bijvoorbeeld klanten, werknemers, scholieren, patiënten, inwoners etc. Gaat het om kwetsbare groepen? Bijvoorbeeld kinderen, ouderen of mensen met een beperking.
- Hoeveel onbevoegden hadden of hebben bij benadering (mogelijk) toegang tot de gelekte persoonsgegevens?
- Heeft u zicht op wie die onbevoegden zijn? En is het waarschijnlijk dat de onbevoegden kwade bedoelingen hebben met de gegevens? Of gaat het om een bekende, betrouwbare ontvanger?
- Heeft uw organisatie vooraf maatregelen getroffen waardoor de gelekte persoonsgegevens (deels) ontoegankelijk zijn voor onbevoegden? Bijvoorbeeld omdat de gegevens versleuteld zijn?

Tot woensdag,
art 5 1-2e

art 5 1-2e

m unicatie

provincie Zuid-Holland

M art 5 1-2e

art 5 1-2e @ pzh.nl

Werkdagen: maandag, dinsdag, woensdag, donderdag, vrijdag

www.zuid-holland.nl/contact

Krachtig Zuid-Holland.

Van: art 5 1-2e
Verzonden: 2023-04-04 07:35:58+00:00
Aan: art 5 1-2e
CC:
Onderwerp: FW: Conceptadvies datalek A 98259 - Vermissing smartphone
"
Goedemorgen,

art 5 1-2eis akkoord. Zorg jij voor administratieve afhandeling?

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2epzh.nl <mailto : art 5 1-2epzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protect utlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art 5 1-2e art 5 1-2e 40pzh.nl
%7C223a44ca16574840155008db34ce784c
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638161833600437422%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C
%7C&sdata=fIb2z4hDwc3IovSxWjwvVcHIHDRlo5tHasSvHtuPic8%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: maandag 3 april 2023 15:10
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
CC: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Re: Conceptadvies datalek A 98259 - Vermissing smartphone

Akkoord, heeft hij überhaupt iets opgestoken tijdens zijn training voor PA in
2019?

Van: art 5 1-2e
Verzonden: 2023-03-31 15:54:24+00:00
Aan: art 5 1-2e
CC: Willy de Zoete - van der Hout; privacy; art 5 1-2e
Onderwerp: FW: Datalek postkamer - printer print in de nacht bestanden met persoonsgegevens - advies: WEL datalek NIET melden
"
Hoi art 5 1-2e

Ik volg het advies, maar hoor wel graag snel terug hoe dit nou heeft kunnen gebeuren. Klinkt als een soort hack , en dat klinkt dan weer als dat externen bij bestanden kunnen

Hartelijke groet, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: vrijdag 31 maart 2023 15:50
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
CC: Willy de Zoete - van der Hout <wh.de.zoete@pzh.nl>; privacy <privacy@pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Datalek postkamer - printer print in de nacht bestanden met persoonsgegevens - advies: WEL datalek NIET melden

Beste art 5 1-2e

Bijgaand een advies inzake een datalek. De printer in de postkamer heeft buiten openingstijden automatisch bestanden met persoonsgegevens uitgeprint. Op ons verzoek doet I&A onderzoek naar de oorzaak. Ons advies is: niet melden alleen registreren intern.

Volg je het advies?

Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7Cprivacy%40pzh.nl%7Cee4cc5738c9b47ed3f2d08db31ef7016%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638158676672708365%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=NwuOttJpnL%2BMedXgf1D0fgOgc8mH068iIw3f15TMvzY%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.
"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: defintief

Melding gegevens

Aangemeld door	:	art 5 1-2e (Bureau Infrastructuur en Support) (Informatisering en Automatisering))
Registratienummer van het incident	:	M23 03 03583
Datum en tijdstip van de melding	:	29-03-2023, 11.03
Route van de melding	:	melding datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	31 maart 2023 om 14.48 uur,
Advies besproken met	:	Besproken met art 5 1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Gedeeld met eenheid Privacy

Situatie

Melder geeft aan dat een printer in de postkamer (Alleen postkamer medewerkers hebben autorisatie om te printen via deze printer) automatisch bestanden heeft uitgeprint. Dit gebeurde in de nacht van zaterdag 25 maart op zondag 26 maart nadat de zomertijd is ingegaan. Gesproken met art 5 1-2e Xerox) en art 5 1-2e (I&A). Zij hebben in de logboeken gekeken en daaruit valt niet op te maken wie de oorspronkelijke printopdracht naar de postkamer heeft gestuurd. Wel is geconstateerd dat de printopdracht in de nacht van zaterdag op zondag is uitgevoerd. Melder heeft de uitgeprinte stukken achter slot en grendel bewaard. Eenheid Privacy heeft de stukken overgedragen gekregen en deze veiliggesteld. De uitgeprinte stukken bevatten persoonsgegevens. Het zijn o.a. mailwisselingen tussen PZH en de gemeente Leidschendam-Voorburg, bestemmingsplannen, uitgifte van erfpacht en adviesrapportages.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Onbekend.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Waarschijnlijk 0 personen. Het vond plaats buiten de openingstijden van het Provinciehuis. De stukken zijn maandagochtend aangetroffen in de postkamer, waar deze stukken zich horen te bevinden.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen.
Welke persoonsgegevens betreft het?	Normale persoonsgegevens.

Vraag	Antwoord
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Naar alle waarschijnlijkheid wel.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Mogelijk, Informatieveiligheid is ingelicht.
Betreft het een datalek?	Ja.
Ondernomen beperkende maatregelen.	De stukken zijn door melder overgedragen aan Eenheid Privacy. Eenheid Privacy heeft de stukken veiliggesteld.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Verzoek bij art 5 1-2e (coordinator Bureau Infrastructuur en Support) ingediend om verder uit te zoeken hoe dit heeft kunnen gebeuren en dat er maatregelen getroffen worden zodat dit niet nogmaals voorkomt.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

In de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek. Alleen als bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of indien onrechtmatige verwerking redelijkerwijs niet uitgesloten kan worden, is sprake van een datalek. Een zwakke beveiliging levert op zichzelf dus nog geen datalek op.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Om dit te bepalen is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Bij de beoordeling hiervan spelen diverse factoren een rol, zoals:

[1] Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven, strafrechtelijk verleden.
[2] Denk aan: identiteitsfraude, discriminatie, reputatieschade.

- Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals gezondheidsgegevens, gegevens over ras of religie, strafrechtelijke gegevens of bijvoorbeeld financiële gegevens zijn gelekt.
- Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.
- Een gegeven is géén persoonsgegeven als doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. De verordening en de meldplicht datalekken zijn daarom niet van toepassing op anonieme of geanonimiseerde gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
- De AVG en de meldplicht datalekken is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Wanneer is vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient de provincie ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens. Het opstellen van de berichtgeving vindt plaats in nauwe afstemming met de concerndirecteur en de afdeling Communicatie. De gedeputeerde Middelen wordt geïnformeerd.

Analyse van dit specifieke geval

Printer heeft documenten uitgeprint toen er niemand in het PZH pand aanwezig was. Hoe dit heeft kunnen gebeuren is nog niet bekend. Documenten zijn door de melder overgedragen aan Eenheid Privacy. De uitgeprinte stukken bevatten o.a. mailwisselingen tussen PZH en de gemeente Leidschendam-Voorburg, bestemmingsplannen, uitgifte van erfpacht en adviesrapportages. De uitgeprinte stukken zijn door Eenheid Privacy opgeborgen. Het datalek wordt niet gemeld bij de AP en/of betrokkenen, omdat het niet waarschijnlijk is dat het incident een hoog risico vormt voor betrokkenen. De stukken bevatten geen bijzondere en/of gevoelige persoonsgegevens. Op verzoek van Eenheid Privacy onderzoekt I&A dit incident verder. Dit is van belang om soortgelijke incidenten in de toekomst te voorkomen.

Conclusie en advies

De FG gehoord hebbende en gezien de bovengenoemde afwegingskaders en analyse, adviseert de eenheid Privacy als volgt:

- Er is WEL sprake van een datalek in de zin van de AVG.
- Het datalek wordt NIET gemeld bij de Autoriteit Persoonsgegevens of betrokkenen.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.


provincie
Zuid-Holland

"Van: art 5 1-2e
Verzonden: .941000+00:00
"Aan: art 5 1-2e art 5 1-2e ; art 5 1-2e art 5 1-2e
"CC: art 5 1-2e
Onderwerp: FW: privacy
"
Ter info, eind sept zal er dan ongetwijfeld van onze kant weer een reactie worden gevraagd

@art 5 1-2e wil jij dit mee in de gaten houden?

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: dinsdag 30 juni 2020 10:18
Aan: art 5 1-2e art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
CC: art 5 1-2e pzh.nl> ; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: privacy

Dag art 5 1-2en art 5 1-2e

Bijgaand verslag is met Willy besproken en ze heeft ingestemd met de reactie van de directie daarop. Ik heb haar toegezegd om haar ergens mid oktober te rapporteren over de tussentijdse voortgang. Mag ik jullie vragen zo rond eind september een rondgang te doen ten behoeve van deze update?

Dank alvast, hartelijke groet, art 5 1-2e
"

provincie ZUID HOLLAND

Jaarverslag privacy 2019 PZH

De belangrijkste risico's in beeld

1. Inleiding

Bijna anderhalf jaar na de inwerkingtreding houdt de Algemene verordening gegevensbescherming (AVG) de gemoederen nog flink bezig, binnen de PZH en daarbuiten. In de AVG en de Uitvoeringswet AVG staan nogal wat open normen. Door publicaties van de Autoriteit Persoonsgegevens en door jurisprudentie wordt steeds meer duidelijk hoe deze open normen moeten worden gelezen.

In dit eerste jaarverslag ga ik met name in op de risicogebieden die ik signaleer binnen de PZH bij de verwerking van persoonsgegevens.

De Functionaris voor Gegevensbescherming heeft vanuit de AVG twee taken toebedeeld gekregen:

- Toezicht houden op de naleving van de Algemene verordening gegevensbescherming (AVG) binnen de eigen organisatie
- Advies aan de verwerkingsverantwoordelijke (GS, PS en de CdK) over hun verplichtingen uit de AVG

PZH heeft in 2019 met name op het gebied van bewustwording en het op poten zetten van een privacyorganisatie binnen de provincie goede vooruitgang geboekt.
Iedere afdeling heeft één of meer privacy officers. Zij zijn het eerste aanspreekpunt voor de medewerkers. Ook is er een privacyteam dat de functionaris voor gegevensbescherming (FG) ondersteunt. Dit team beoordeelt datalekken en brengt daarover aan de concerndirectie verslag uit. Sinds 2019 heeft de organisatie verschillende projecten lopen om de bewustwording voor privacy te verhogen. Dit leidt tot meer bewustzijn bij de medewerkers. Daar komen dan weer vragen en acties uit voort die het lerend effect bevorderen.

In 2018 en 2019 is er veel energie gestoken in het contact tussen de ambtelijke organisatie en de FG. In 2020 wil ik meer direct contact hebben met de 3 bestuursorganen, GS, PS en de CdK. Ook hierin vertrouw ik op de ondersteuning van de gedeputeerde mevrouw de Zoete.

De uitdagingen die er nog liggen zijn groot en vragen om een voortvarende aanpak. Voldoen aan de AVG is voor een overheidsorgaan als de provincie natuurlijk een vereiste. De huidige crisis vraagt ook op het gebied van privacy veel inspanningen. Er zal waarschijnlijk voor langere tijd thuis gewerkt worden.
Maar belangrijker nog, we willen de risico's voor burgers en onze organisatie verkleinen.

2. Risicogebieden

a. iDMS: de grootste bron van datalekken
b. Cameratoezicht: te veel verwerking van bijzondere persoonsgegevens
c. Beleid: het ontbreekt aan beleid
d. Innovatieprojecten: feestje, maar privacy blijft te lang buiten beeld
e. Bewustwording: veel te weinig datalekken gemeld
f. Informatieveiligheid: niet onafhankelijk georganiseerd
g. Outlook: onveilig mailen zonder voorbehoud

h. Google Chrome: ongelimiteerd dataverzamelen
i. Topdesk: bedoeld voor het melden van storingen, niet bedoeld voor persoonsgegevens
j. Mobile devices: ongewenst navolgbaar op stap

3. Toelichting per risicogebied

a. iDMS: de grootste bron van datalekken

PZH gebruikt iDMS al 12 jaar als de plaats waar zij al haar documenten opslaat. De kans op datalekken is zeer aanzienlijk. Bij de invoering van het systeemwaren de eisen nog niet zoals die nu zijn, met de AVG. De rechten en rollen zijn niet voldoende uitgewerkt. Daardoor is de kans op datalekken groot. Ook de manier waarop de collega's werken met iDMS is niet betrouwbaar en waterdicht.

Vanuit PZH wordt regelmatig gewezen, met PR-campagnes, op het belang van zorgvuldig werken in iDMS. Toch is het iDMS de voornaamste bron van datalekken. Zodra er een datalek heeft plaatsgevonden wordt er wel een ad hoc oplossing geïmplementeerd, maar structureel blijven er problemen bestaan.

Naar mijn mening wordt er te weinig effort gestoken in het op orde brengen van het iDMS. Ik twijfel er aan of iDMS voldoende technische en organisatorische mogelijkheden kent om het gewenste kwaliteitsniveau te bereiken. Dat kan wel worden bereikt door de vervanging van het iDMS door een ander systeem. Hier wordt al jaren over gesproken. Bij vervanging moet wel worden opgepast dat in een nieuw systeem niet de "chaos" van het huidige systeem wordt meegenomen.

Advies: Zorg op korte termijn dat de rollen en rechten op orde zijn in iDMS. Vervang iDMS en stel daarbij deadlines voor de keuze van een nieuw programma en de implementatie.

b. Cameratoezicht: te veel verwerking van bijzondere persoonsgegevens

PZH gebruikt voor de bewaking van en het toezicht op en in haar gebouwen een camerasysteem. Camerabeelden omvatten veelal persoonsgegevens en zijn een regelmatig punt van discussie. Beeldmateriaal omvat vaak ook bijzondere persoonsgegevens, die in principe niet mogen worden verwerkt, tenzij er een specifieke uitzonderingsgrond bestaat.

Daarom hebben de Europese toezichthouders recent een vernieuwde richtlijn uitgebracht over het gebruik van cameratoezicht in relatie tot de privacywetgeving. De eisen in de nieuwe richtlijn zijn aangescherpt voor het beschermen van de privacy van burgers en medewerkers. PZH voldoet op dit moment niet aan de vereisten.

De afdeling FZ heeft toegezegd dat in 2020 een verbeterslag zal plaatsvinden. De FG zal worden betrokken bij het onderzoek naar de verbeteringen.

c. Beleid: het ontbreekt aan beleid

PZH beschikt niet over een beleid ten aanzien van het omgaan met persoonsgegevens, niet op afdelingsniveau en niet als concern. Er is soms wel wat beleid op deelaspecten. Daarnaast beschikt PZH wel over een privacyverklaring, welke is gepubliceerd op haar website. De AVG vereist echter een beleid op het gebied van privacy waarin ook is vastgelegd op welke wijze de kwaliteit van het omgaan met persoonsgegevens is geborgd.

Er zijn nog maar weinig organisaties die beleid hebben geïmplementeerd dat ook bruikbaar is bij de verwerking van persoonsgegevens in de huidige situatie en in de komende jaren. Vaak komt men niet verder dan op een andere manier opschrijven wat er ook in de AVG staat.

Advies: stel een kader op waarbinnen de afdelingen hun privacybeleid kunnen opstellen. Het beleid van de afdelingen kan vervolgens op concernniveau worden samengevoegd. Het te formuleren beleid biedt ook aanknopingspunten hoe om te gaan met de verwerking van persoonsgegevens in de toekomst.

d. Innovatieprojecten: feestje, maar privacy blijft te lang buiten beeld
PZH wil zich graag een koppositie verwerven bij de digitale transformatie. Onder andere daarvoor zet zij stevig in op innovatieve projecten. Enkele voorbeelden daarvan zijn de deelname aan smart city projecten en smart mobility projecten.
Het is voor de FG moeilijk om inzicht te krijgen in de data die gebruikt (gaan) worden in innovatieprojecten. Het lijkt alsof innovatieprojecten op gespannen voet staan met de AVG.
In deze projecten worden vaak algoritmes en kunstmatige intelligentie (AI) toegepast. Daarbij worden heel grote hoeveelheden gegevens verwerkt (big data) , vaak persoonsgegevens. En door samenvoeging van grote hoeveelheden data kunnen ook nieuwe persoonsgegevens ontstaan, die eerder niet als zodanig herkenbaar waren.
Gelukkig zijn er ook positieve uitzonderingen waarin privacy wel al vanaf het begin wordt meegenomen. Een voorbeeld daarvan is het project SNapp waarin een app zorgt voor de vindbaarheid van bestuurders in Zuid-Holland.

Advies: borg dat de FG altijd bij de start van een nieuw project wordt geïnformeerd over de intenties van het project, ook wanneer niet op voorhand duidelijk is dat er persoonsgegevens zullen worden verwerkt. Daarnaast moeten Privacy by design en Privacy by default een vast gegeven zijn bij innovatieprojecten. Dit zijn beide beginselen die in de AVG zijn vastgelegd.

e. Bewustwording: veel te weinig datalekken gemeld!
“Een datalek is melding van een inbreuk op persoonsgegevens. De verwerkingsverantwoordelijke dient deze meldingen te registreren, te onderzoeken, eventueel passende maatregelen te nemen. Daarnaast dient de verwerkingsverantwoordelijke deze meldingen binnen 72 uur te melden aan de landelijke toezichthouder, de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de betrokkene(n). Mocht dat risico er wel zijn dan zal de verwerkingsverantwoordelijke de inbreuk in sommige gevallen ook moeten melden aan de betrokkene(n).”

In 2019 zijn binnen de PZH in totaal 10 meldingen gemaakt van een datalek.

- In 1 geval betrof het een onterechte melding van een datalek.
- In 5 gevallen betrof het een onterechte inzage in een van de systemen van de PZH, waarbij onbevoegden inzage hadden in persoonsgegevens waartoe zij niet gerechtigd waren op grond van hun functie.
- Bij 2 meldingen betrof het foutief verstuurde e-mails, waarbij persoonsgegevens zijn verzonden naar de verkeerde ontvanger.
- In 1 geval betrof het de onterechte verwerking van bijzondere persoonsgegevens, dat wil zeggen gevoelige persoonsgegevens waarvoor een strenger beveiligingsregime geldt dan voor normale persoonsgegevens.

- In 1 geval betrof het de onterechte toegang tot een van de systemen van PZH, waarbij persoonsgegevens inzichtelijk zijn geweest voor onbevoegden.

Van de bij PZH gemelde datalekken zijn er 4 gemeld aan de AP.

Het lijkt erop dat er veel datalekken niet worden gemeld. Voor een organisatie met zoveel werknemers zijn de aantallen veel te laag in vergelijking met de landelijke cijfers. De oorzaak hiervoor kan onbekendheid zijn met wat een datalek is, maar mogelijk ook schaamtegevoel waardoor er niet gemeld wordt. Een datalek kan veel schade aanbrengen aan de PZH. Enerzijds is daar de imagoschade: het vertrouwen van de burger in een betrouwbare overheid wordt geschaad. Anderzijds kan er ook financiële schade ontstaan. De Autoriteit Persoonsgegevens kan bij een ernstige inbreuk op persoonsgegevens of het niet naleven van de wet, boetes opleggen die kunnen oplopen tot € 20.000.000, -.

Advies: zet ook in 2020 vol in op bewustwording binnen de organisatie door middel van campagnes waarbij het thema datalek centraal staat.

f. Informatieveiligheid: niet onafhankelijk georganiseerd

Bescherming van privacy is nauw verbonden met informatieveiligheid. Het is gebruikelijk dat de FG binnen organisaties zoals PZH een gelijkwaardige collega heeft in de vorm van de CISO (Chief Information Security Officer). De CISO heeft een vergelijkbare en onafhankelijke positie en status binnen de organisatie.

PZH heeft geen CISO, wel een team van 3 informatieveiligheidsadviseurs. Dit team maakt onderdeel uit van de afdeling I&A. Maar door de status en de plaats die dit team heeft zij te weinig slagkracht en bevoegdheden. Dit werkt belemmerend bij het opsporen van datalekken en het implementeren van oplossingen.

Advies: benoem een CISO met een aan de FG vergelijkbare positie. Geef de CISO vergelijkebare bevoegdheden. GS publiceren een reglement voor de CISO zoals dat ook voor de FG is gebeurd.

g. Outlook: onveilig mailen zonder voorbehoud

Het standaardmailprogramma dat door PZH gebruikt wordt is Microsoft Outlook.

De kans is zeer groot dat dagelijks vele malen inbreuk wordt gemaakt op het verwerken van persoonsgegevens bij het gebruik van Outlook. In mail zitten vaak persoonsgegevens. De bijlagen bij mail kunnen uiteraard persoonsgegevens bevatten en ook gevoelige of bijzondere persoonsgegevens. Nu is het zo dat buiten het domein van PZH de mail niet is beschermd door extra maatregelen. Dit betekent dat mail niet voldoet aan een beschermingsniveau zoals dat vereist wordt door de AVG.

Er zijn meerdere oplossingen op de markt verkrijgbaar waardoor het wel mogelijk is om te voldoen aan de vereisten van de AVG.
In 2020 is PZH gestart met een pilot voor een mail-addon die wel veilig mailverkeer mogelijk zou moeten maken. Maar omdat hierbij gebruik gemaakt wordt van een product uit de Verenigde Staten blijft het beveiligd mailen vragen om extra toezicht door de FG.

Advies: houd de eisen voor beveiligd mailen bij PZH nogmaals tegen het licht en vergelijk deze met de uitkomsten uit de pilot.

h. Google Chrome: ongelimiteerd dataverzamelen
PZH heeft in 2019 de keuze gemaakt voor het implementeren van Google Chrome als standaard browser voor de gehele organisatie. Bij de keuze voor deze browser is de FG niet geraadpleegd.

Google is een van de grootste verwerkers van persoonsgegevens. De bescherming van de grondrechten van burgers staat daarbij veelal niet voorop. Het gevolg daarvan is dat zij al meerdere, heel hoge, boetes opgelegd heeft gekregen door de EU als gevolg van de schending van de Europese privacywetten. Ook nu nog is Google onderworpen aan onderzoeken door de EU.

Er zijn alternatieven voor het gebruik van Google Chrome die veel meer gericht zijn op de bescherming van persoonsgegevens.
Advies: implementeer een privacyvriendelijk alternatief als standaard browser.

i. Topdesk: bedoeld voor het melden van storingen, niet bedoeld voor persoonsgegevens
Topdesk is van oorsprong een ticketsysteem dat is bedoeld voor het melden van ICT-storingen. Binnen PZH is het echter uitgegroeid tot een systeem waarin heel veel meldingen worden verwerkt. Hierbij zitten ook meldingen en workflows waarin (gevoelige) persoonsgegevens worden verwerkt. Dit oneigenlijke gebruik van Topdesk baart mij als FG grote zorgen omdat door het gebruik van Topdesk ook al datalekken zijn veroorzaakt. Wat ook zorgen baart is de wijze waarop en het gebrek aan snelheid waarmee PZH omgaat met gemelde problemen rond Topdesk.

Advies: onderzoek de processen in Topdesk op nut en noodzaak en neem daarbij de bescherming van persoonsgegevens als uitgangspunt. Implementeer een goed en transparant model voor het analyseren en oplossen van zulke problemen.

j. Mobile devices: ongewenst navolgbaar op stap
PZH stelt aan haar medewerkers mobile devices ter beschikking in de vorm van smartphones, tablets en laptops. Dit vergemakkelijkt o.a. het plaats- en tijdongebonden werken.

Maar het gebruik van dergelijke devices legt een zware verplichting op PZH ten aanzien van de beveiliging en daarmee de bescherming van persoonsgegevens. Ik heb geconstateerd dat het Mobile Device Management niet voor alle devices op dezelfde wijze is geconfigureerd. Bovendien voldoet dat niet aan de vereisten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is een norm die is opgelegd aan de overheid. Het tekort aan beveiligingsmaatregelen zorgt voor een permanente inbreuk op persoonsgegevens.

Advies: breng op korte termijn de beveiligingsmaatregelen op een voldoende niveau te voor alle mobile devices. Schakel standaard de locatieinstellingen uit.

4. Rechten van betrokkenen (burgers en medewerkers): hoe vaak is er een beroep op gedaan?
In de AVG wordt in Hoofdstuk III aandacht besteed aan de rechten van betrokkenen, degenen van wie informatie wordt verwerkt. In de artikelen 15 t/m 22 AVG worden deze rechten expliciet omgezet naar de vormen van verzoek die een betrokkene kan doen aan de verwerkingsverantwoordelijke.

In 2019 is driemaal een verzoek geweest tot inzage ex art. 15 AVG (verzoek om inzage). Van de overige rechten is in 2019 geen gebruik gemaakt. De drie verzoeken zijn gehonoreerd en afgehandeld binnen de termijn die de AVG geeft.

Tot slot: waarop focust de Autoriteit Persoonsgegevens en hoe raakt dat PZH?
De Autoriteit Persoonsgegevens heeft in haar toekomstvisie "Focus AP: Dataprotectie in een digitale samenleving" aangegeven waar wat haar betreft de prioriteiten liggen in het toezicht op de verwerking en bescherming van persoonsgegevens. De overheid is een van de sectoren die verscherpt in de gaten wordt gehouden. Inhoudelijk gaat de AP vooral inzetten op de volgende drie gebieden:

- *Datahandel*
  Dit speelt in zoverre een rol voor PZH dat hieronder o.a. valt de verkoop van data. PZH heeft in haar innovatieve projecten te maken met de verkoop van data, te denken valt hierbij aan de data die gegenereerd worden in bijvoorbeeld de smart city en smart mobility projecten, zoals in de keten van gegevens uit de intelligente verkeersregelinstallaties (iVri's).
- *Digitale overheid*
  Dat dit van belang is voor PZH spreekt voor zich.
- *Artificiële intelligentie & algoritmes*
  Ook PZH zal in toenemende mate gebruik maken van AI en algoritmes, waarbij ook grote hoeveelheden persoonsgegevens worden verwerkt. De bedoeling is om dit jaar een kennisbijeenkomst te organiseren rondom AI en algoritmes in het licht van de AVG voor juristen en FG's in de provincie Zuid-Holland.

art 5 1-2e
Functionaris voor Gegevensbescherming PZH

provincie ZUID HOLLAND

Reactie Directieteam op Jaarverslag privacy 2019 PZH van de Functionaris voor Gegevensbescherming PZH

Privacy krijgt de laatste jaren steeds meer aandacht. Ontwikkelingen rondom Tech-reuzen als Facebook en Google hebben laten zien hoe belangrijk het is dat persoonsgegevens veilig worden beheerd. We moeten ons echter ook realiseren dat in het recente verleden bij de ontwikkeling van IT systemen andere uitgangspunten centraler stonden. Denk aan efficiency, kostenreductie, betrouwbaarheid en veiligheid.

De PZH heeft mede daarom toentertijd gekozen voor samenwerking met onder andere Microsoft. Dat levert op dit moment grote voordelen. Zo is er sprake van een hoge betrouwbaarheid van het netwerk en is het mogelijk gebleken om een snelle ontwikkeling door te maken op het gebied van data gedreven werken waarbij algoritmen een belangrijke rol spelen. Ook is het gelukt om bij de Coronacrisis snel op te schalen om betrouwbaar thuis te kunnen werken en vanuit huis samen te werken (Microsoft Teams).

Maar zoals gezegd met de jaren is echter ook geconstateerd dat er wel erg makkelijk met privacy gevoelige gegevens werd omgegaan. We moeten leren dat zorgvuldiger te doen. Innovatie, aanschaf van nieuwe systemen, datagebruik moeten hand in hand gaan met het zorgvuldig bewaken van gevoelige gegevens. Met de aanstelling van de functionaris voor gegevensbescherming (FG) in 2018 hebben we bij de PZH daar een adviseur/toezichthouder voor, die ons daarin helpt maar ook controleert.

In zijn eerste jaarverslag wijst de FG ons op de risicogebieden die hij signaleert binnen de PZH bij de verwerking van persoonsgegevens. De belangrijkste risico’s worden zo in beeld gebracht en van zijn advies voorzien. Daar zijn wij hem erkentelijk voor. Onderstaand geven wij aan wat wij ondernemen op basis van zijn advies.

Tabel 1

Door FG gesignaleerd risicogebied	Door FG gegeven advies	Onze reactie
a. iDMS: de grootste bron van datalekken	Zorg op korte termijn dat de rollen en rechten op orde zijn in iDMS. Vervang iDMS en stel daarbij deadlines voor de keuze van een nieuw programma en de implementatie.	Deels overgenomen. Inrichting rechten en rollen is onderdeel van het project Identity en Access Management (IAM). In dit project is reeds de basis gelegd voor een goede inrichting van rechten en rollen in diverse applicaties. Tot dat toekennen en ontnemen van rechten en rollen sterk verbeterd en waar mogelijk geautomatiseerd kan verlopen, zal I&A extra toezien op de handmatige verwerking. Op dit moment wordt iDMS geupdate, vernieuwd en zullen diverse verbeteringen worden doorgevoerd. Waarbij één van de doelstellingen is om de applicatie meer AVG-proof te maken. Belangrijkste hierbij blijft wel hoe de gebruikers omgaan met systemen en informatie. Van zowel IAM als de aanpassing iDMS wordt een actueel projectplanning opgesteld. Eind juni is de update gereed en aansluitend zal een projectplan worden opgesteld voor verbeteringen.

b. Cameratoezicht: te veel verwerking van bijzondere persoonsgegevens	PZH voldoet op dit moment niet aan de vereisten.	De afdeling FZ heeft toegezegd dat in 2020 een verbeterslag zal plaatsvinden. De FG zal worden betrokken bij het onderzoek naar de verbeteringen. Planning 4e kwartaal.
c. Beleid: het ontbreekt aan beleid	PZH beschikt niet over een beleid ten aanzien van het omgaan met persoonsgegevens, niet op afdelingsniveau en niet als concern. Er is soms wel wat beleid op deelaspecten. Daarnaast beschikt PZH wel over een privacyverklaring, welke is gepubliceerd op haar website. De AVG vereist echter een beleid op het gebied van privacy waarin ook is vastgelegd op welke wijze de kwaliteit van het omgaan met persoonsgegevens is geborgd.	Beleid wordt ontwikkeld Het privacy team van de PZH is op dit moment aan de slag met de opdrachtformulering privacy beleid n.a.v. het jaarverslag FG. Dat document zou richtinggevend moeten zijn voor de komende 3 tot 5 jaar en in ieder geval antwoord moeten geven op: wat willen we, met welke middelen en binnen welke kaders, bereiken en wie spelen daar een rol bij. Oplevering eind 4e kwartaal 2020.
d. Innovatieprojecten: feestje, maar privacy blijft te lang buiten beeld	Borg dat de FG altijd bij de start van een nieuw project wordt geïnformeerd over de intenties van het project, ook wanneer niet op voorhand duidelijk is dat er	Advies wordt overgenomen.

	persoonsgegevens zullen worden verwerkt. Daarnaast moeten Privacy by design en Privacy by default een vast gegeven zijn bij innovatieprojecten. Dit zijn beide beginselen die in de AVG zijn vastgelegd.	Het innovatieteam van de provincie heeft hier aandacht voor en wijst hen die innovaties ontwikkelen op het belang van de beginselen van de AVG I&A heeft nauwelijks eigen innovatie projecten, wel werkt men aan innovaties bij digitaal Zuid Holland en het Innovatieteam. Bij digitaal Zuid Holland wordt bij de experimenten juist ook ethische aspecten in beschouwing genomen. In geval van innovaties bij I&A zal al in een vroeg stadium de FG worden geïnformeerd over toekomstige projecten.
e. Bewustwording: veel te weinig datalekken gemeld	Zet ook in 2020 vol in op bewustwording binnen de organisatie door middel van campagnes waarbij het thema datalek centraal staat.	Advies wordt overgenomen. Bewustwording is een gedragscomponent die een lange adem vereist De huidige bewustwordingscampagne is een meerjarig traject, waar de AVG 1 van de 5 onderwerpen is naast informatiebeheer, informatieveiligheid, integriteit, data- en informatiekwaliteit. Daarnaast heeft de FG een eigen campagne lopen met communicatie waarin aandacht wordt gevraagd voor AVG.

f. Informatieveiligheid: niet onafhankelijk georganiseerd	Benoem een CISO met een aan de FG vergelijkbare positie. Geef de CISO vergelijkbare bevoegdheden. GS publiceren een reglement voor de CISO zoals dat ook voor de FG is gebeurd.	Advies wordt niet opgevolgd. De aanstelling van een CISO valt onder de verantwoordelijkheid van de directie / het bestuur. Tot op heden heeft de organisatie er overigens bewust niet voor gekozen om een functionaris als CISO, CIO, CDO of controller aan te stellen. De achterliggende gedachte daarbij is dat met het aanstellen van dergelijke functionarissen ook de eigen verantwoordelijkheid minder wordt. Bij I&A vinden relatief veel audits plaats op het gebied van veiligheid. De aanbevelingen worden niet altijd even snel opgevolgd. Een oorzaak hiervan was de bureaustructuur waarbij eigen prioriteiten konden worden gesteld. Inmiddels stuurt het MT op een andere manier en vanuit gemeenschappelijke prioriteiten. Op deze manier wordt het onderliggende probleem opgelost en is de vraag of het instellen van een functionaris die toezicht, met ambtelijke interacties tot gevolg, wel nodig is en niet juist de noodzaak tot verbetering afzwakt .
g. Outlook: onveilig mailen zonder voorbehoud	Houd de eisen voor beveiligd mailen bij PZH nogmaals tegen het licht en vergelijk deze met de uitkomsten uit de pilot.	Advies wordt overgenomen. Na de pilot zullen de uitkomsten vergeleken worden met de eisen voor beveiligd mailen.

h. Google Chrome: ongelimiteerd dataverzamelen	Implementeer een privacy vriendelijk alternatief als standaard browser.	Advies wordt niet overgenomen. Veel applicaties die in gebruik zijn bij PZH ondersteunen alleen de browsers Google Chroom en/of Microsoft Edge. Voor de nu gebruikte browsers zal een audit plaats vinden op de instellingen gericht op de privacy en data uitwisseling. Daarnaast zal onderzocht worden hoe om te gaan met het beheer van data en algoritmes.
i. Topdesk: bedoeld voor het melden van storingen, niet bedoeld voor persoonsgegevens	Onderzoek de processen in Topdesk op nut en noodzaak en neem daarbij de bescherming van persoonsgegevens als uitgangspunt. Implementeer een goed en transparant model voor het analyseren en oplossen van zulke problemen.	Het systeem wordt niet alleen ingezet om storing bij I&A te melden, maar ook voor aanvragen voor de gehele bedrijfsvoering. Voor deze aanvragen zijn nu eenmaal persoonsgegevens nodig. Aan risicobeheersing inzake vertrouwelijke gegevens is opgepakt. Ook hier geldt een eigen verantwoordelijkheid voor de gebruiker van het systeem. Daarover wordt gecommuniceerd.
j. Mobile devices: ongewenst navolgbaar op stap	Breng op korte termijn de beveiligingsmaatregelen op een voldoende niveau voor alle mobile devices. Schakel standaard de locatie instellingen uit.	Advies wordt overgenomen. Beveiligingsmaatregelen zullen tegen het licht gehouden worden en waar mogelijk worden aangepast en op een hoger niveau worden gebracht. Waar mogelijk zullen locatie instellingen standaard uitgezet worden.

"Van: art 5 1-2e
Verzonden: 2020-05-12 16:20:14.037000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: FW: Reactie op het jaarverslag privacy
"
In onze bila even goed afstemmen. Met art 5 1-2e wel wat leuke denklijnen net besproken.

Oa CT mede-eigenaar/ of minimaal deelgenoot maken.

Maar ook hoe we hier nou handig mee omgaan. Bv Discussie over aanzetten smart UI vond ik vorige week niet heel sterk in de stuurgroep.

We moeten echt een grotere opzet gaan regelen, het wordt steeds urgenter.

Via de aangeleverde input richting staten gelukkig ook weer even goed onder de aandacht gebracht. Maar we moeten echt met de goede dingen komen. Ook bv xECM en inzet van externe partijen ed.

We zijn goed bezig, wel nog concreter maken langs het MT en dus ook CT. Etc

We kunnen hier echt een wat grotere broek in aantrekken.

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: dinsdag 12 mei 2020 13:42
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e p z art 5 1-2e
van < art 5 1-2e pzh.nl > art 5 1-2e pzh.nl> ; art 5 1-2e
art 5 1-2e)pzh.nl>
Onderwerp: RE: Reactie op het jaarverslag privacy

Hierbij mijn reactie art 5 1-2e Die mbt IAM had ik gisteren in MT aan de orde willen stellen, ben ik vergeten. Bij deze dan.

Groeten,
art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 12 mei 2020 11:05
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e , art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> > ; art 5 1-2e
<aj.boere@pzh.nl <mailto art 5 1-2e ozh.nl> >; art 5 1-2e
< art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> > ; art 5 1-2e
art 5 1-2e pzh.nl <mailt o art 5 1-2e)pzh.nl> >
Onderwerp: Reactie op het jaarverslag privacy

Dag allen,

Bijgaand ontvangen jullie onze reactie op het jaarverslag Privacy.

Willen jullie hier nog even naar kijken of het zo klopt?

Overigens heb ik een stukje geel gemarkeerd, omdat daar een datum moet staan van de projectplanning idms.

Ik hoor graag wat de datum is.

Groeten,

art 5 1-2e

Reactie I&A op jaarverslag privacy 2019 PZH

Algemene reactie

Privacy krijgt de laatste jaren steeds meer aandacht. Terecht, maar bedacht moet worden dat bij de ontwikkeling van de IT systemen andere uitgangspunten centraler stonden zoals efficiency, kostenreductie, betrouwbaarheid en veiligheid. Daarbij is gekozen voor samenwerking met onder andere Microsoft. Dat levert op dit moment grote voordelen. Zo is er sprake van een hoge betrouwbaarheid van het netwerk en is het mogelijk gebleken om een snelle ontwikkeling door te maken op het gebied van datagedreven werken waarbij algoritmen een belangrijke rol spelen (Azure). Ook is het gelukt om bij de Coronacrisis snel op te schalen om betrouwbaar thuis te kunnen werken en vanuit huis samen te werken (Microsoft Teams). Naast deze voordelen komen er nu ook steeds meer de nadelen aan het licht: privacy en afhankelijkheid. Uiteraard heeft I&A hier oog voor en zal serieus werk maken van de aanbevelingen (hierover later meer). Maar volledig opheffen van de nadelen is niet mogelijk en kan alleen als de organisatie kiest voor een andere koers en de gevolgen accepteert met betrekking tot financiën, personeel en gebruiksgemak. Het lijkt ons goed de aanbevelingen ook in deze context te plaatsen zodat een realistisch beeld ontstaat over wat I&A kan doen.

Specifieke reactie

a. iDMS de grootste bron van datalekken

Inrichting rechten en rollen is onderdeel van het project Identity en Access Management (IAM). In dit project is reeds de basis gelegd voor een goede inrichting van rechten en rollen in diverse applicaties. Tot dat toekennen en ontnemen van rechten en rollen sterk verbeterd en waar mogelijk geautomatiseerd kan verlopen, zal I&A extra toezien op de handmatige verwerking. Op dit moment wordt iDMS ~~geupdate~~geüpdatet, vernieuwd en zullen diverse verbeteringen worden doorgevoerd. Waarbij één van de doelstellingen is om de applicatie meer AVG-proof te maken. Belangrijkste hierbij blijft wel hoe de gebruikers omgaan met systemen en informatie. Van zowel IAM als de aanpassing iDMS wordt een actueel projectplanning opgesteld welke …..gereed is. Aandachtspunt op dit moment zijn het beschikbare budget en de beschikbare personele capaciteit (mede vanwege restricties aan de inhuur).

b. Cameratoezicht: te veel verwerking van bijzondere persoonsgegevens

Reactie vanuit afdeling FZ.

c. Beleid: het ontbreekt aan beleid

Primair dient eerst concernbreed beleid opgesteld te worden, waarna I&A deze kan verbijzonderen voor de informatisering- en automatiseringsaspecten.

d. Innovatieprojecten: feestje, maar privacy blijft te lang buiten beeld

I&A heeft nauwelijks eigen innovatie projecten, wel werken we mee aan innovaties bij digitaal Zuid Holland en het Innovatieteam. In geval van innovaties bij I&A zal al in een vroeg stadium de FG worden geïnformeerd over toekomstige projecten.

e. Bewustwording: veel te weinig datalekken gemeld

De huidige bewustwordingscampagne is een meerjarig traject, waar de AVG ~~één~~ 1 van de 5 onderwerpen is naast informatiebeheer, informatieveiligheid, integriteit, data- en informatiekwaliteit. Daarnaast heeft de FG een eigen campagne lopen met communicatie waarin aandacht wordt gevraagd voor AVG. Daarin speelt I&A verder geen rol.

Zie verder opmerking onder algemeen.

f. Informatieveiligheid: niet onafhankelijk georganiseerd

De aanstelling van een CISO valt onder de verantwoordelijkheid van de directie / het bestuur. Tot op heden heeft de organisatie er overigens bewust niet voor gekozen om een functionaris als CISO, CIO, CDO of controller aan te stellen. De achterliggende gedachte daarbij is dat met het aanstellen van dergelijke functionarissen ook de eigen verantwoordelijkheid minder wordt. Bij I&A vinden relatief veel audits plaats op het gebied van veiligheid. De aanbevelingen worden niet altijd even snel opgevolgd. Een oorzaak hiervan was de bureaustructuur waarbij eigen prioriteiten konden worden gesteld. Inmiddels stuurt het MT op een andere manier en vanuit gemeenschappelijke prioriteiten. Op deze manier wordt het onderliggende probleem opgelost en is de vraag of het instellen van een functionaris die toezicht, met ambtelijke interacties tot gevolg, wel nodig is.

g. Outlook: onveilig mailen zonder voorbehoud

Advies wordt overgenomen: na de pilot zullen de uitkomsten vergeleken worden met de eisen voor beveiligd mailen.

h. Google Chrome: ongelimiteerd data verzamelen

Veel applicaties die in gebruik zijn bij PZH ondersteunen alleen de browsers Google Chroom en/of Microsoft Edge. Browsers die bekend staan om een meer privacy vriendelijk alternatief wordt veelal niet ondersteund en geven veel technische problemen waardoor deze niet kunnen worden ingezet. Voor de nu gebruikte browsers zal een audit plaats vinden op de instellingen gericht op de privacy en data uitwisseling.

De provincie ~~Zuid-holland~~Zuid-Holland gaat steeds meer data gedreven werken. Algoritmes kunnen worden gebruikt om bepaalde beslissingen (deels) te automatiseren. Daar moet verantwoording over afgelegd kunnen worden. Een algoritme kan daardoor onder de werking van de Archiefwet vallen. Er moet nagedacht worden over hoe om te gaan met het beheer van data en algoritmes. Het is raadzaam om ook omtrent dit onderwerp kennisbijeenkomsten te organiseren.

i. Topdesk: bedoeld voor het melden van storingen, niet bedoeld voor persoonsgegevens

Een systeem dat niet bedoeld is voor vertrouwelijke gegevens en risico's heeft bij verkeerd gebruik. Deze risico's zullen zo veel als mogelijk worden beheerst. Op dit moment wordt hier aan gewerkt.

j. Mobile devices: ongewenst navolgbaar op stap

Advies wordt overgenomen. Beveiligingsmaatregelen zullen tegen het licht gehouden worden en waar mogelijk worden aangepast en op een hoger niveau worden gebracht. Waar mogelijk zullen locatie instellingen standaard uitgezet worden.

"Van: art 5 1-2e , art 5 1-2e
Verzonden: 2020-05-12 .278000+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: RE: Reactie op het jaarverslag privacy
"
Een datum voor iDMS is ook nog niet te geven. We moeten eerst de upgrade erdoor hebben, daar wordt nu 'driftig' op getest. En we zijn bezig al wat zaken uit te zoeken voor de verbeteringen daarna en welke mogelijkheden er zijn.

Ik zal het projectplan binnenkort een keer agenderen in kleiner comité.

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: dinsdag 12 mei 2020 13:42
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e , art 5 1-2e van < art 5 1-2e pzh.nl>; art 5 1-2e pzh.nl> ; art 5 1-2e art 5 1-2e pzh.nl>
Onderwerp: RE: Reactie op het jaarverslag privacy

Hierbij mijn reactie art 5 1-2e Die mbt IAM had ik gisteren in MT aan de orde willen stellen, ben ik vergeten. Bij deze dan.

Groeten,
art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 12 mei 2020 11:05
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e , art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> > ; art 5 1-2e <aj.boere@pzh.nl <mailto:aj.boere@pzh.nl> >; art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> > ; art 5 1-2e art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: Reactie op het jaarverslag privacy

Dag allen,

Bijgaand ontvangen jullie onze reactie op het jaarverslag Privacy.

Willen jullie hier nog even naar kijken of het zo klopt?

Overigens heb ik een stukje geel gemarkeerd, omdat daar een datum moet staan van de projectplanning idms.

Ik hoor graag wat de datum is.

Groeten,

art 5 1-2e
"

Van: art 5 1-2e
Verzonden: 2023-09-28 14:38:23.096000+00:00
Aan: art 5 1-2e
CC:
Onderwerp: FW: stand van zaken privacy
"

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: maandag 5 oktober 2020 11:35
Aan: art 5 1-2e < art 5 1-2e pzh.nl> ; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e pzh.nl>
Onderwerp: Fwd: stand van zaken privacy

Van: art 5 1-2e art 5 1-2e)pzh.nl <mailt o art 5 1-2e)pzh.nl> >
Verstuurd: maandag 5 oktober 2020 10:19
Aan: art 5 1-2e
Onderwerp: stand van zaken privacy

Ollah,

N.a.v. het jaarverslag van de FG hebben we Willy bericht over de acties die wij op dat gebied ondernemen. Willy is door art 5 1-2e toegezegd dat hij eind oktober hierop terug zou komen. Dat hoeft natuurlijk niet een ellenlang verhaal te zijn, maar een paar regels met een soort stand van zaken zou wel fijn zijn. Kunnen jullie mij die svp aanleveren voor de onderdelen waar jullie aan verbonden? Zou dat voor 22 oktober kunnen?

Ik heb het rapport van de FG en onze reactie daarop nog even toegevoegd.

Thx vast.

Met groet,

art 5 1-2e

"

provincie ZUID HOLLAND

Jaarverslag privacy 2019 PZH

De belangrijkste risico's in beeld

1. Inleiding

Bijna anderhalf jaar na de inwerkingtreding houdt de Algemene verordening gegevensbescherming (AVG) de gemoederen nog flink bezig, binnen de PZH en daarbuiten. In de AVG en de Uitvoeringswet AVG staan nogal wat open normen. Door publicaties van de Autoriteit Persoonsgegevens en door jurisprudentie wordt steeds meer duidelijk hoe deze open normen moeten worden gelezen.

In dit eerste jaarverslag ga ik met name in op de risicogebieden die ik signaleer binnen de PZH bij de verwerking van persoonsgegevens.

De Functionaris voor Gegevensbescherming heeft vanuit de AVG twee taken toebedeeld gekregen:

- Toezicht houden op de naleving van de Algemene verordening gegevensbescherming (AVG) binnen de eigen organisatie
- Advies aan de verwerkingsverantwoordelijke (GS, PS en de CdK) over hun verplichtingen uit de AVG

PZH heeft in 2019 met name op het gebied van bewustwording en het op poten zetten van een privacyorganisatie binnen de provincie goede vooruitgang geboekt.
Iedere afdeling heeft één of meer privacy officers. Zij zijn het eerste aanspreekpunt voor de medewerkers. Ook is er een privacyteam dat de functionaris voor gegevensbescherming (FG) ondersteunt. Dit team beoordeelt datalekken en brengt daarover aan de concerndirectie verslag uit. Sinds 2019 heeft de organisatie verschillende projecten lopen om de bewustwording voor privacy te verhogen. Dit leidt tot meer bewustzijn bij de medewerkers. Daar komen dan weer vragen en acties uit voort die het lerend effect bevorderen.

In 2018 en 2019 is er veel energie gestoken in het contact tussen de ambtelijke organisatie en de FG. In 2020 wil ik meer direct contact hebben met de 3 bestuursorganen, GS, PS en de CdK. Ook hierin vertrouw ik op de ondersteuning van de gedeputeerde mevrouw de Zoete.

De uitdagingen die er nog liggen zijn groot en vragen om een voortvarende aanpak. Voldoen aan de AVG is voor een overheidsorgaan als de provincie natuurlijk een vereiste. De huidige crisis vraagt ook op het gebied van privacy veel inspanningen. Er zal waarschijnlijk voor langere tijd thuis gewerkt worden.
Maar belangrijker nog, we willen de risico's voor burgers en onze organisatie verkleinen.

2. Risicogebieden

a. iDMS: de grootste bron van datalekken
b. Cameratoezicht: te veel verwerking van bijzondere persoonsgegevens
c. Beleid: het ontbreekt aan beleid
d. Innovatieprojecten: feestje, maar privacy blijft te lang buiten beeld
e. Bewustwording: veel te weinig datalekken gemeld
f. Informatieveiligheid: niet onafhankelijk georganiseerd
g. Outlook: onveilig mailen zonder voorbehoud

h. Google Chrome: ongelimiteerd dataverzamelen
i. Topdesk: bedoeld voor het melden van storingen, niet bedoeld voor persoonsgegevens
j. Mobile devices: ongewenst navolgbaar op stap

3. Toelichting per risicogebied

a. iDMS: de grootste bron van datalekken

PZH gebruikt iDMS al 12 jaar als de plaats waar zij al haar documenten opslaat. De kans op datalekken is zeer aanzienlijk. Bij de invoering van het systeemwaren de eisen nog niet zoals die nu zijn, met de AVG. De rechten en rollen zijn niet voldoende uitgewerkt. Daardoor is de kans op datalekken groot. Ook de manier waarop de collega's werken met iDMS is niet betrouwbaar en waterdicht.

Vanuit PZH wordt regelmatig gewezen, met PR-campagnes, op het belang van zorgvuldig werken in iDMS. Toch is het iDMS de voornaamste bron van datalekken. Zodra er een datalek heeft plaatsgevonden wordt er wel een ad hoc oplossing geïmplementeerd, maar structureel blijven er problemen bestaan.

Naar mijn mening wordt er te weinig effort gestoken in het op orde brengen van het iDMS. Ik twijfel er aan of iDMS voldoende technische en organisatorische mogelijkheden kent om het gewenste kwaliteitsniveau te bereiken. Dat kan wel worden bereikt door de vervanging van het iDMS door een ander systeem. Hier wordt al jaren over gesproken. Bij vervanging moet wel worden opgepast dat in een nieuw systeem niet de "chaos" van het huidige systeem wordt meegenomen.

Advies: Zorg op korte termijn dat de rollen en rechten op orde zijn in iDMS. Vervang iDMS en stel daarbij deadlines voor de keuze van een nieuw programma en de implementatie.

b. Cameratoezicht: te veel verwerking van bijzondere persoonsgegevens

PZH gebruikt voor de bewaking van en het toezicht op en in haar gebouwen een camerasysteem. Camerabeelden omvatten veelal persoonsgegevens en zijn een regelmatig punt van discussie. Beeldmateriaal omvat vaak ook bijzondere persoonsgegevens, die in principe niet mogen worden verwerkt, tenzij er een specifieke uitzonderingsgrond bestaat.

Daarom hebben de Europese toezichthouders recent een vernieuwde richtlijn uitgebracht over het gebruik van cameratoezicht in relatie tot de privacywetgeving. De eisen in de nieuwe richtlijn zijn aangescherpt voor het beschermen van de privacy van burgers en medewerkers. PZH voldoet op dit moment niet aan de vereisten.

De afdeling FZ heeft toegezegd dat in 2020 een verbeterslag zal plaatsvinden. De FG zal worden betrokken bij het onderzoek naar de verbeteringen.

c. Beleid: het ontbreekt aan beleid

PZH beschikt niet over een beleid ten aanzien van het omgaan met persoonsgegevens, niet op afdelingsniveau en niet als concern. Er is soms wel wat beleid op deelaspecten. Daarnaast beschikt PZH wel over een privacyverklaring, welke is gepubliceerd op haar website. De AVG vereist echter een beleid op het gebied van privacy waarin ook is vastgelegd op welke wijze de kwaliteit van het omgaan met persoonsgegevens is geborgd.

Er zijn nog maar weinig organisaties die beleid hebben geïmplementeerd dat ook bruikbaar is bij de verwerking van persoonsgegevens in de huidige situatie en in de komende jaren. Vaak komt men niet verder dan op een andere manier opschrijven wat er ook in de AVG staat.

Advies: stel een kader op waarbinnen de afdelingen hun privacybeleid kunnen opstellen. Het beleid van de afdelingen kan vervolgens op concernniveau worden samengevoegd. Het te formuleren beleid biedt ook aanknopingspunten hoe om te gaan met de verwerking van persoonsgegevens in de toekomst.

d. Innovatieprojecten: feestje, maar privacy blijft te lang buiten beeld
PZH wil zich graag een koppositie verwerven bij de digitale transformatie. Onder andere daarvoor zet zij stevig in op innovatieve projecten. Enkele voorbeelden daarvan zijn de deelname aan smart city projecten en smart mobility projecten.
Het is voor de FG moeilijk om inzicht te krijgen in de data die gebruikt (gaan) worden in innovatieprojecten. Het lijkt alsof innovatieprojecten op gespannen voet staan met de AVG.
In deze projecten worden vaak algoritmes en kunstmatige intelligentie (AI) toegepast. Daarbij worden heel grote hoeveelheden gegevens verwerkt (big data) , vaak persoonsgegevens. En door samenvoeging van grote hoeveelheden data kunnen ook nieuwe persoonsgegevens ontstaan, die eerder niet als zodanig herkenbaar waren.
Gelukkig zijn er ook positieve uitzonderingen waarin privacy wel al vanaf het begin wordt meegenomen. Een voorbeeld daarvan is het project SNapp waarin een app zorgt voor de vindbaarheid van bestuurders in Zuid-Holland.

Advies: borg dat de FG altijd bij de start van een nieuw project wordt geïnformeerd over de intenties van het project, ook wanneer niet op voorhand duidelijk is dat er persoonsgegevens zullen worden verwerkt. Daarnaast moeten Privacy by design en Privacy by default een vast gegeven zijn bij innovatieprojecten. Dit zijn beide beginselen die in de AVG zijn vastgelegd.

e. Bewustwording: veel te weinig datalekken gemeld!
“Een datalek is melding van een inbreuk op persoonsgegevens. De verwerkingsverantwoordelijke dient deze meldingen te registreren, te onderzoeken, eventueel passende maatregelen te nemen. Daarnaast dient de verwerkingsverantwoordelijke deze meldingen binnen 72 uur te melden aan de landelijke toezichthouder, de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de betrokkene(n). Mocht dat risico er wel zijn dan zal de verwerkingsverantwoordelijke de inbreuk in sommige gevallen ook moeten melden aan de betrokkene(n).”

In 2019 zijn binnen de PZH in totaal 10 meldingen gemaakt van een datalek.

- In 1 geval betrof het een onterechte melding van een datalek.
- In 5 gevallen betrof het een onterechte inzage in een van de systemen van de PZH, waarbij onbevoegden inzage hadden in persoonsgegevens waartoe zij niet gerechtigd waren op grond van hun functie.
- Bij 2 meldingen betrof het foutief verstuurde e-mails, waarbij persoonsgegevens zijn verzonden naar de verkeerde ontvanger.
- In 1 geval betrof het de onterechte verwerking van bijzondere persoonsgegevens, dat wil zeggen gevoelige persoonsgegevens waarvoor een strenger beveiligingsregime geldt dan voor normale persoonsgegevens.

- In 1 geval betrof het de onterechte toegang tot een van de systemen van PZH, waarbij persoonsgegevens inzichtelijk zijn geweest voor onbevoegden.

Van de bij PZH gemelde datalekken zijn er 4 gemeld aan de AP.

Het lijkt erop dat er veel datalekken niet worden gemeld. Voor een organisatie met zoveel werknemers zijn de aantallen veel te laag in vergelijking met de landelijke cijfers. De oorzaak hiervoor kan onbekendheid zijn met wat een datalek is, maar mogelijk ook schaamtegevoel waardoor er niet gemeld wordt. Een datalek kan veel schade aanbrengen aan de PZH. Enerzijds is daar de imagoschade: het vertrouwen van de burger in een betrouwbare overheid wordt geschaad. Anderzijds kan er ook financiële schade ontstaan. De Autoriteit Persoonsgegevens kan bij een ernstige inbreuk op persoonsgegevens of het niet naleven van de wet, boetes opleggen die kunnen oplopen tot € 20.000.000, -.

Advies: zet ook in 2020 vol in op bewustwording binnen de organisatie door middel van campagnes waarbij het thema datalek centraal staat.

f. Informatieveiligheid: niet onafhankelijk georganiseerd

Bescherming van privacy is nauw verbonden met informatieveiligheid. Het is gebruikelijk dat de FG binnen organisaties zoals PZH een gelijkwaardige collega heeft in de vorm van de CISO (Chief Information Security Officer). De CISO heeft een vergelijkbare en onafhankelijke positie en status binnen de organisatie.

PZH heeft geen CISO, wel een team van 3 informatieveiligheidsadviseurs. Dit team maakt onderdeel uit van de afdeling I&A. Maar door de status en de plaats die dit team heeft zij te weinig slagkracht en bevoegdheden. Dit werkt belemmerend bij het opsporen van datalekken en het implementeren van oplossingen.

Advies: benoem een CISO met een aan de FG vergelijkbare positie. Geef de CISO vergelijkebare bevoegdheden. GS publiceren een reglement voor de CISO zoals dat ook voor de FG is gebeurd.

g. Outlook: onveilig mailen zonder voorbehoud

Het standaardmailprogramma dat door PZH gebruikt wordt is Microsoft Outlook.

De kans is zeer groot dat dagelijks vele malen inbreuk wordt gemaakt op het verwerken van persoonsgegevens bij het gebruik van Outlook. In mail zitten vaak persoonsgegevens. De bijlagen bij mail kunnen uiteraard persoonsgegevens bevatten en ook gevoelige of bijzondere persoonsgegevens. Nu is het zo dat buiten het domein van PZH de mail niet is beschermd door extra maatregelen. Dit betekent dat mail niet voldoet aan een beschermingsniveau zoals dat vereist wordt door de AVG.

Er zijn meerdere oplossingen op de markt verkrijgbaar waardoor het wel mogelijk is om te voldoen aan de vereisten van de AVG.
In 2020 is PZH gestart met een pilot voor een mail-addon die wel veilig mailverkeer mogelijk zou moeten maken. Maar omdat hierbij gebruik gemaakt wordt van een product uit de Verenigde Staten blijft het beveiligd mailen vragen om extra toezicht door de FG.

Advies: houd de eisen voor beveiligd mailen bij PZH nogmaals tegen het licht en vergelijk deze met de uitkomsten uit de pilot.

h. Google Chrome: ongelimiteerd dataverzamelen
PZH heeft in 2019 de keuze gemaakt voor het implementeren van Google Chrome als standaard browser voor de gehele organisatie. Bij de keuze voor deze browser is de FG niet geraadpleegd.

Google is een van de grootste verwerkers van persoonsgegevens. De bescherming van de grondrechten van burgers staat daarbij veelal niet voorop. Het gevolg daarvan is dat zij al meerdere, heel hoge, boetes opgelegd heeft gekregen door de EU als gevolg van de schending van de Europese privacywetten. Ook nu nog is Google onderworpen aan onderzoeken door de EU.

Er zijn alternatieven voor het gebruik van Google Chrome die veel meer gericht zijn op de bescherming van persoonsgegevens.
Advies: implementeer een privacyvriendelijk alternatief als standaard browser.

i. Topdesk: bedoeld voor het melden van storingen, niet bedoeld voor persoonsgegevens
Topdesk is van oorsprong een ticketsysteem dat is bedoeld voor het melden van ICT-storingen. Binnen PZH is het echter uitgegroeid tot een systeem waarin heel veel meldingen worden verwerkt. Hierbij zitten ook meldingen en workflows waarin (gevoelige) persoonsgegevens worden verwerkt. Dit oneigenlijke gebruik van Topdesk baart mij als FG grote zorgen omdat door het gebruik van Topdesk ook al datalekken zijn veroorzaakt. Wat ook zorgen baart is de wijze waarop en het gebrek aan snelheid waarmee PZH omgaat met gemelde problemen rond Topdesk.

Advies: onderzoek de processen in Topdesk op nut en noodzaak en neem daarbij de bescherming van persoonsgegevens als uitgangspunt. Implementeer een goed en transparant model voor het analyseren en oplossen van zulke problemen.

j. Mobile devices: ongewenst navolgbaar op stap
PZH stelt aan haar medewerkers mobile devices ter beschikking in de vorm van smartphones, tablets en laptops. Dit vergemakkelijkt o.a. het plaats- en tijdongebonden werken.

Maar het gebruik van dergelijke devices legt een zware verplichting op PZH ten aanzien van de beveiliging en daarmee de bescherming van persoonsgegevens. Ik heb geconstateerd dat het Mobile Device Management niet voor alle devices op dezelfde wijze is geconfigureerd. Bovendien voldoet dat niet aan de vereisten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is een norm die is opgelegd aan de overheid. Het tekort aan beveiligingsmaatregelen zorgt voor een permanente inbreuk op persoonsgegevens.

Advies: breng op korte termijn de beveiligingsmaatregelen op een voldoende niveau te voor alle mobile devices. Schakel standaard de locatieinstellingen uit.

4. Rechten van betrokkenen (burgers en medewerkers): hoe vaak is er een beroep op gedaan?
In de AVG wordt in Hoofdstuk III aandacht besteed aan de rechten van betrokkenen, degenen van wie informatie wordt verwerkt. In de artikelen 15 t/m 22 AVG worden deze rechten expliciet omgezet naar de vormen van verzoek die een betrokkene kan doen aan de verwerkingsverantwoordelijke.

In 2019 is driemaal een verzoek geweest tot inzage ex art. 15 AVG (verzoek om inzage). Van de overige rechten is in 2019 geen gebruik gemaakt. De drie verzoeken zijn gehonoreerd en afgehandeld binnen de termijn die de AVG geeft.

Tot slot: waarop focust de Autoriteit Persoonsgegevens en hoe raakt dat PZH?
De Autoriteit Persoonsgegevens heeft in haar toekomstvisie "Focus AP: Dataprotectie in een digitale samenleving" aangegeven waar wat haar betreft de prioriteiten liggen in het toezicht op de verwerking en bescherming van persoonsgegevens. De overheid is een van de sectoren die verscherpt in de gaten wordt gehouden. Inhoudelijk gaat de AP vooral inzetten op de volgende drie gebieden:

- *Datahandel*
  Dit speelt in zoverre een rol voor PZH dat hieronder o.a. valt de verkoop van data. PZH heeft in haar innovatieve projecten te maken met de verkoop van data, te denken valt hierbij aan de data die gegenereerd worden in bijvoorbeeld de smart city en smart mobility projecten, zoals in de keten van gegevens uit de intelligente verkeersregelinstallaties (iVri's).
- *Digitale overheid*
  Dat dit van belang is voor PZH spreekt voor zich.
- *Artificiële intelligentie & algoritmes*
  Ook PZH zal in toenemende mate gebruik maken van AI en algoritmes, waarbij ook grote hoeveelheden persoonsgegevens worden verwerkt. De bedoeling is om dit jaar een kennisbijeenkomst te organiseren rondom AI en algoritmes in het licht van de AVG voor juristen en FG's in de provincie Zuid-Holland.

art 5 1-2e
Functionaris voor Gegevensbescherming PZH

provincie ZUID HOLLAND

Reactie Directieteam op Jaarverslag privacy 2019 PZH van de Functionaris voor Gegevensbescherming PZH

Privacy krijgt de laatste jaren steeds meer aandacht. Ontwikkelingen rondom Tech-reuzen als Facebook en Google hebben laten zien hoe belangrijk het is dat persoonsgegevens veilig worden beheerd. We moeten ons echter ook realiseren dat in het recente verleden bij de ontwikkeling van IT systemen andere uitgangspunten centraler stonden. Denk aan efficiency, kostenreductie, betrouwbaarheid en veiligheid.

De PZH heeft mede daarom toentertijd gekozen voor samenwerking met onder andere Microsoft. Dat levert op dit moment grote voordelen. Zo is er sprake van een hoge betrouwbaarheid van het netwerk en is het mogelijk gebleken om een snelle ontwikkeling door te maken op het gebied van data gedreven werken waarbij algoritmen een belangrijke rol spelen. Ook is het gelukt om bij de Coronacrisis snel op te schalen om betrouwbaar thuis te kunnen werken en vanuit huis samen te werken (Microsoft Teams).

Maar zoals gezegd met de jaren is echter ook geconstateerd dat er wel erg makkelijk met privacy gevoelige gegevens werd omgegaan. We moeten leren dat zorgvuldiger te doen. Innovatie, aanschaf van nieuwe systemen, datagebruik moeten hand in hand gaan met het zorgvuldig bewaken van gevoelige gegevens. Met de aanstelling van de functionaris voor gegevensbescherming (FG) in 2018 hebben we bij de PZH daar een adviseur/toezichthouder voor, die ons daarin helpt maar ook controleert.

In zijn eerste jaarverslag wijst de FG ons op de risicogebieden die hij signaleert binnen de PZH bij de verwerking van persoonsgegevens. De belangrijkste risico’s worden zo in beeld gebracht en van zijn advies voorzien. Daar zijn wij hem erkentelijk voor. Onderstaand geven wij aan wat wij ondernemen op basis van zijn advies.

provincie ZUID HOLLAND

Tabel 1

Door FG gesignaleerd risicogebied	**Door FG gegeven advies**	**Onze reactie**
a. iDMS: de grootste bron van datalekken	Zorg op korte termijn dat de rollen en rechten op orde zijn in iDMS. Vervang iDMS en stel daarbij deadlines voor de keuze van een nieuw programma en de implementatie.	Deels overgenomen. Inrichting rechten en rollen is onderdeel van het project Identity en Access Management (IAM). In dit project is reeds de basis gelegd voor een goede inrichting van rechten en rollen in diverse applicaties. Tot dat toekennen en ontnemen van rechten en rollen sterk verbeterd en waar mogelijk geautomatiseerd kan verlopen, zal I&A extra toezien op de handmatige verwerking. Op dit moment wordt iDMS geupdate, vernieuwd en zullen diverse verbeteringen worden doorgevoerd. Waarbij één van de doelstellingen is om de applicatie meer AVG-proof te maken. Belangrijkste hierbij blijft wel hoe de gebruikers omgaan met systemen en informatie. Van zowel IAM als de aanpassing iDMS wordt een actueel projectplanning opgesteld. Eind juni is de update gereed en aansluitend zal een projectplan worden opgesteld voor verbeteringen.
b. Cameratoezicht: te veel verwerking van bijzondere	PZH voldoet op dit moment niet aan de vereisten.	De afdeling FZ heeft toegezegd dat in 2020 een verbeterslag zal plaatsvinden. De FG zal worden betrokken bij het onderzoek naar

persoonsgegevens		de verbeteringen. Planning 4e kwartaal.
c. Beleid: het ontbreekt aan beleid	PZH beschikt niet over een beleid ten aanzien van het omgaan met persoonsgegevens, niet op afdelingsniveau en niet als concern. Er is soms wel wat beleid op deelaspecten. Daarnaast beschikt PZH wel over een privacyverklaring, welke is gepubliceerd op haar website. De AVG vereist echter een beleid op het gebied van privacy waarin ook is vastgelegd op welke wijze de kwaliteit van het omgaan met persoonsgegevens is geborgd.	Beleid wordt ontwikkeld Het privacy team van de PZH is op dit moment aan de slag met de opdrachtformulering privacy beleid n.a.v. het jaarverslag FG. Dat document zou richtinggevend moeten zijn voor de komende 3 tot 5 jaar en in ieder geval antwoord moeten geven op: wat willen we, met welke middelen en binnen welke kaders, bereiken en wie spelen daar een rol bij. Oplevering eind 4e kwartaal 2020.
d. Innovatieprojecten: feestje, maar privacy blijft te lang buiten beeld	Borg dat de FG altijd bij de start van een nieuw project wordt geïnformeerd over de intenties van het project, ook wanneer niet op voorhand duidelijk is dat er persoonsgegevens zullen worden verwerkt. Daarnaast moeten Privacy by	Advies wordt overgenomen. Het innovatieteam van de provincie heeft hier aandacht voor en wijst hen die innovaties ontwikkelen op het belang van de beginselen van de AVG I&A heeft nauwelijks eigen innovatie projecten, wel werkt men aan

	design en Privacy by default een vast gegeven zijn bij innovatieprojecten. Dit zijn beide beginselen die in de AVG zijn vastgelegd.	innovaties bij digitaal Zuid Holland en het Innovatieteam. Bij digitaal Zuid Holland wordt bij de experimenten juist ook ethische aspecten in beschouwing genomen. In geval van innovaties bij I&A zal al in een vroeg stadium de FG worden geïnformeerd over toekomstige projecten.
e. Bewustwording: veel te weinig datalekken gemeld	Zet ook in 2020 vol in op bewustwording binnen de organisatie door middel van campagnes waarbij het thema datalek centraal staat.	Advies wordt overgenomen. Bewustwording is een gedragscomponent die een lange adem vereist De huidige bewustwordingscampagne is een meerjarig traject, waar de AVG 1 van de 5 onderwerpen is naast informatiebeheer, informatieveiligheid, integriteit, data- en informatiekwaliteit. Daarnaast heeft de FG een eigen campagne lopen met communicatie waarin aandacht wordt gevraagd voor AVG.
f. Informatieveiligheid: niet onafhankelijk georganiseerd	Benoem een CISO met een aan de FG vergelijkbare positie. Geef de CISO vergelijkbare bevoegdheden. GS publiceren een reglement voor de CISO zoals dat ook voor de FG is gebeurd.	Advies wordt niet opgevolgd. De aanstelling van een CISO valt onder de verantwoordelijkheid van de directie / het bestuur. Tot op heden heeft de organisatie er overigens bewust niet voor gekozen om een functionaris als CISO, CIO, CDO of controller aan te stellen. De achterliggende gedachte

		daarbij is dat met het aanstellen van dergelijke functionarissen ook de eigen verantwoordelijkheid minder wordt. Bij I&A vinden relatief veel audits plaats op het gebied van veiligheid. De aanbevelingen worden niet altijd even snel opgevolgd. Een oorzaak hiervan was de bureaustructuur waarbij eigen prioriteiten konden worden gesteld. Inmiddels stuurt het MT op een andere manier en vanuit gemeenschappelijke prioriteiten. Op deze manier wordt het onderliggende probleem opgelost en is de vraag of het instellen van een functionaris die toezicht, met ambtelijke interacties tot gevolg, wel nodig is en niet juist de noodzaak tot verbetering afzwakt .
g. Outlook: onveilig mailen zonder voorbehoud	Houd de eisen voor beveiligd mailen bij PZH nogmaals tegen het licht en vergelijk deze met de uitkomsten uit de pilot.	Advies wordt overgenomen. Na de pilot zullen de uitkomsten vergeleken worden met de eisen voor beveiligd mailen.
h. Google Chrome: ongelimiteerd dataverzamelen	Implementeer een privacy vriendelijk alternatief als standaard browser.	Advies wordt niet overgenomen. Veel applicaties die in gebruik zijn bij PZH ondersteunen alleen de browsers Google Chroom en/of Microsoft Edge. Voor de nu gebruikte browsers zal een audit plaats vinden op de instellingen gericht op de privacy en data uitwisseling.

		Daarnaast zal onderzocht worden hoe om te gaan met het beheer van data en algoritmes.
i. Topdesk: bedoeld voor het melden van storingen, niet bedoeld voor persoonsgegevens	Onderzoek de processen in Topdesk op nut en noodzaak en neem daarbij de bescherming van persoonsgegevens als uitgangspunt. Implementeer een goed en transparant model voor het analyseren en oplossen van zulke problemen.	Het systeem wordt niet alleen ingezet om storing bij I&A te melden, maar ook voor aanvragen voor de gehele bedrijfsvoering. Voor deze aanvragen zijn nu eenmaal persoonsgegevens nodig. Aan risicobeheersing inzake vertrouwelijke gegevens is opgepakt. Ook hier geldt een eigen verantwoordelijkheid voor de gebruiker van het systeem. Daarover wordt gecommuniceerd.
j. Mobile devices: ongewenst navolgbaar op stap	Breng op korte termijn de beveiligingsmaatregelen op een voldoende niveau voor alle mobile devices. Schakel standaard de locatie instellingen uit.	Advies wordt overgenomen. Beveiligingsmaatregelen zullen tegen het licht gehouden worden en waar mogelijk worden aangepast en op een hoger niveau worden gebracht. Waar mogelijk zullen locatie instellingen standaard uitgezet worden.

art 5 1-2e

Van: art 5 1-2e
Verzonden: ptember 2023 09:53
Aan: art 5 1-2e
Onderwerp: ED: Datalek EasyFunders

Ik wordt zo geopereerd en misschien dat art 5 1-2e pas later dan 1030 beschikbaar Verder dan in de matrix beschreven heeft niemand toegang Dit heb ik al trouwens erg duidelijk gemaakt in de mailwisseling Afschermen tegen schermafdruk weerhoudt iemand er niet van om het bsn nr op te schrijven Ik zou verder contact opnemen met art 5 1-2e

PROVINCIAAL BESTUUR VAN ZUID-HOLLAND

Besluitenlijst (middels de zgn 4-parafenprocedure) van de vergadering van Gedeputeerde Staten van 21 april 2020

Van: art 5 1-2e
Verzonden: 2023-05-24 08:23:18+00:00
Aan: art 5 1-2e
CC:
Onderwerp: Re: Definitief RE: Conceptadvies datalek A99581
"
Akkoord.

<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAAb9ysg&data=05%7C01% art 5 1-2e 40pzh.nl%7C824cc1ab188e4856a9e008db5c1f5d3d%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015609209%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=TxqLnDfXYRAovX9tfWEt6PwnBkdcFWTWdQ%2BOdbwHQlw%3D&reserved=0> Met

vriendelijke groet,

art 5 1-2e

Functionaris voor Gegevensbescherming

Gerechtelijk Deskundige

<olm://attachment/AQADAAAAyQAAAAAAAAAAM74HAAAAAAAA1AAAAAAABD9sAAAAAAAHvjMAAAAAAAQ_bAMAAIAAAAAAJW5lLmJvbnNAcHpoLm5sX0FjdGl2ZVN5bmNFeGNoYW5nZV9IeFM%3D/AQADAAABagAAAAAAAAAPL4HAAAAAAABZwAAAAAABD1TAAAAAAAHvjwAAAAAAAQ9UwMAAIAAAAAAJW5lLmJvbnNAcHpoLm5sX0FjdGl2ZVN5bmNFeGNoYW5nZV9IeFM%3D>

M art 5 1-2e

art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e 40pzh.nl%7C824cc1ab188e4856a9e008db5c1f5d3d%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015609209%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=akyvDHFfWTEqGof3VvwEUTJhU6tJPjSCgWEa8Ls0Afk%3D&reserved=0>

Werkdagen: ma, di, wo, do,

vr

Elke dag beter. Zuid-

Holland.

Outlook voor Android <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAAb9ysg&data=05%7C01% art 5 1-2e 40pzh.nl%7C824cc1ab188e4856a9e008db5c1f5d3d%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015609209%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=TxqLnDfXYRAovX9tfWEt6PwnBkdcFWTWdQ%2BOdbwHQlw%3D&reserved=0> downloaden
_____

From: art 5 1-2e pzh.nl>
Sent: Wednesday, May 24, 2023 8:21:14 AM
To: art 5 1-2e pzh.nl>
Cc: art 5 1-2e pzh.nl>
Subject: FW: Definitief RE: Conceptadvies datalek A99581

Akkoord?

Met vriendelijke

groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e pzh.nl

<mailto art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7 art 5 1-2e 40pzh.nl
%7C824cc1ab188e4856a9e008db5c1f5d3d
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015765475%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=U39IC7m1rce8rWPx00tDV3LE0%2BjDXxY%2FraqBX1nE27o
%3D&reserved=0>

Werkdagen: ma, di, wo, do,

vr

Elke dag beter. Zuid-

Holland.

Van: art 5 1-2e pzh.nl>
Verzonden: dinsdag 23 mei 2023 17:26
Aan: art 5 1-2e pzh.nl>
Onderwerp: Definitief RE: Conceptadvies datalek A99581

Dit is

‘m.

Met vriendelijke

groet,

art 5 1-2e

Privacy Officer

Eenheid Privacy

M art 5 1-2e pzh.nl

<mailto art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e 40pzh.nl%7C824cc1ab188e4856a9e008db5c1f5d3d%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015765475%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=U39IC7m1rce8rWPx00tDV3LE0%2BjDXxY%2FraqBX1nE27o%3D&reserved=0>

Werkdagen: ma, di, do,

vr

Elke dag beter. Zuid-

Holland.

Van: art 5 1-2e pzh.nl> >
Verzonden: dinsdag 23 mei 2023 16:12
Aan: art 5 1-2e pzh.nl> >
Onderwerp: RE: Conceptadvies datalek A99581

Hi art 5 1-2e

Check nog even de slotparagraaf. Dat loopt niet helemaal lekker mbt tot de wipeactie van de servicedesk. Met vriendelijke groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e pzh.nl

<m

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7 art 5 1-2e 0pzh.nl

%7C824cc1ab188e4856a9e008db5c1f5d3d
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015765475%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=U39IC7m1rce8rWPx00tDV3LE0%2BjDXxY%2FraqBX1nE27o
%3D&reserved=0>

Werkdagen: ma, di, wo, do,

vr

Elke dag beter. Zuid-

Holland.

Van: art 5 1-2e pzh.nl <mailt o art 5 1-2e)pzh.nl> >
Verzonden: maandag 22 mei 2023 13:05
Aan: art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Conceptadvies datalek A99581

Hi art 5 1-2e

Hopelijk is het vorige bericht succesvol ingetrokken Ik heb de collega gesproken en het conceptadvies aangevuld. Zie bijlage. Met vriendelijke groet,

art 5 1-2e

Privacy Officer

Eenheid Privacy

M art 5 1-2e pzh.nl

<mailto: art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7 art 5 1-2e 40pzh.nl
%7C824cc1ab188e4856a9e008db5c1f5d3d
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638205062015765475%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=U39IC7m1rce8rWPx00tDV3LE0%2BjDXxY%2FraqBX1nE27o
%3D&reserved=0>

Werkdagen: ma, di, do,

vr Elke dag beter. Zuid-

Holland.

provincie
Zuid-Holland

provincie
Zuid-Holland

Van: art 5 1-2e
Verzonden: 2023-04-04 07:35:58+00:00
Aan: art 5 1-2e
CC:
Onderwerp: FW: Conceptadvies datalek A 98259 - Vermissing smartphone
"
Goedemorgen,

art 5 1-2e s akkoord. Zorg jij voor administratieve

afhandeling?

Met vriendelijke

groet

art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e pzh.nl

<mailto: art 5 1-2e @pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e 40pzh.nl
%7C223a44ca16574840155008db34ce784c
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638161833600437422%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C
%7C&sdata=fIb2z4hDwc3IovSxWjwvVcHIHDRlo5tHasSvHtuPic8%3D&reserved=0>

Werkdagen: ma, di, wo, do,

vr

Elke dag beter. Zuid-

Holland.

Van: art 5 1-2e pzh.nl>
Verzonden: maandag 3 april 2023 15:10
Aan: art 5 1-2e pzh.nl>
CC: art 5 1-2e pzh.nl>
Onderwerp: Re: Conceptadvies datalek A 98259 - Vermissing smartphone

Akkoord, heeft hij überhaupt iets opgestoken tijdens zijn training voor PA in 2019?

Met vriendelijke groet,

art 5 1-2e

Functionaris voor Gegevensbescherming

<olm://attachment/AQADAAAAyQAAAAAAAAAM74HAAAAAAAA1AAAAAAABD9sAAAAAAAHvjMAAAAAAAQ_bAMAAIAAAAAAJW5lLmJvbnNAcHpoLm5sX0FjdGl2ZVN5bmNFeGNoYW5nZV9IeFM%3D/AQADAAABagAAAAAAAAAPL4HAAAAAAABZwAAAAAABD1TAAAAAAAHvjwAAAAAAAQ9UwMAAIAAAAAAJW5lLmJvbnNAcHpoLm5sX0FjdGl2ZVN5bmNFeGNoYW5nZV9IeFM%3D>

M art 5 1-2e

art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e 40pzh.nl%7C223a44ca16574840155008db34ce784c%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638161833600437422%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=fIb2z4hDwc3IovSxWjwvVcHIHDRlo5tHasSvHtuPic8%3D&reserved=0>

Werkdagen: ma, di, wo, do,

vr

Elke dag beter. Zuid-

Holland.

Outlook voor Android <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAAb9ysg&data=05%7C01% art 5 1-2e 40pzh.nl%7C223a44ca16574840155008db34ce784c%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638161833600437422%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=fVG3mh%2BNqd0n7fnJFGmEyPm3vVLDpX11CHueaiqom5U%3D&reserved=0> downloaden

---

From: art 5 1-2e pzh.nl> >
Sent:
To: art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >
Cc: art 5 1-2e pzh.nl <mail t art 5 1-2e pzh.nl> >
Subject: FW: Conceptadvies datalek A 98259 - Vermissing smartphone

Akkoord? Check de melder

Met vriendelijke

groet art 5 1-2e

Privacy jurist

Eenheid Privacy

M art 5 1-2e pzh.nl

<mailto art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protec .com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C0 art 5 1-2e 40pzh.nl
%7C223a44ca16574840155008db34ce784c
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638161833600437422%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C
%7C&sdata=fIb2z4hDwc3IovSxWjwvVcHIHDRlo5tHasSvHtuPic8%3D&reserved=0>

Werkdagen: ma, di, wo, do,

vr

Elke dag beter. Zuid-

Holland.

Van: art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: maandag 3 april 2023 11:00
Aan: art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: Conceptadvies datalek A 98259 - Vermissing smartphone

Hi art 5 1-2e

Bijgaand het aangepaste conceptadvies voor A

98259.

Met vriendelijke

groet,

art 5 1-2e

Junior Privacy Officer

Eenheid Privacy

M art 5 1-2e

E art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>
www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7 art 5 1-2e 40pzh.nl
%7C223a44ca16574840155008db34ce784c
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638161833600593690%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=a%2F6dG6CzXhlR2gTjYVFV09wg%2FgaF4azvmd%2ByuqkdqVI
%3D&reserved=0>

Werkdagen: ma, di, do,

vr

Elke dag beter. Zuid-
Holland.

"


provincie
Zuid-Holland


provincie
Zuid-Holland

Van: art 5 1-2e
Verzonden: 2022-11-28 15:36:32+00:00
Aan: art 5 1-2e
CC:
Onderwerp: RE: Melding mogelijk datalek A 94293
"
Hoi,

Morgenmiddag pakken art 5 1-2e en ik deze op.

Het is de eerste datalek voor art 5 1-2e

Ik heb morgenmiddag een afspraak ingepland en dan kunnen we met zijn tweeën alles fysiek even doornemen.

Vriendelijke groet,

art 5 1-2e

Coördinator eenheid & Privacy Officer

Eenheid Privacy

art 5 1-2e pzh.nl
<mailto:aa.damhuis@pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2F&data=05%7C01% art 5 1-2e 40pzh.nl%7C9c4623348d634d9d0ba108dad14df1b3%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638052429938884371%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=e7%2BrtIP%2FhYc5wufO%2FWeASJ2MPIsVHlgWHXI%2Fw5d60M0%3D&reserved=0>

Van: art 5 1-2e pzh.nl>
Verzonden: maandag 28 november 2022 15:30
Aan: art 5 1-2e pzh.nl> ; art 5 1-2e pzh.nl>; art 5 1-2e pzh.nl> ; art 5 1-2e pzh.nl>
Onderwerp: RE: Melding mogelijk datalek A 94293

Lekker op tijd gemeld

Met vriendelijke groet,

art 5 1-2e

Functionaris voor Gegevensbescherming

M art 5 1-2e

E art 5 1-2e)pzh.nl <mailto : art 5 1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art 5 1-2e 40pzh.nl%7C9c4623348d634d9d0ba108dad14df1b3%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638052429938884371%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=ScYJBXmtpH%2FIhmVO7fBnsZD%2B4ddU0V2B3nEGOYMeJOU%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art 5 1-2e)pzh.nl <mailt o art 5 1-2e @pzh.nl> >
Verzonden: maandag 28 november 2022 15:27
Aan: art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >; art 5 1-2e art 5 1-2e pzh.nl <mailt o art 5 1-2e)pzh.nl> > art 5 1-2e art 5 1-2e pzh.nl art 5 1-2e @pzh.nl> > ; art 5 1-2e pzh.nl @pzh.nl> >
Onderwerp: FW: Melding mogelijk datalek A 94293

Van: loket@pzh.nl <mailto:loket@pzh.nl> <loket@pzh.nl <mailto:loket@pzh.nl> >
Verzonden: maandag 28 november 2022 15:26:49 (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
art 5 1-2e

Onderwerp: Melding mogelijk datalek A 94293

Beste collega,

Er is een melding gedaan van een mogelijk datalek:

Zie voor meer informatie:
Activiteitnummer: A 94293
Wijzigingsnummer: W22 11 00349

Hier kan je de activiteit <https://eur03.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fpvzh.topdesk.net%2Ftas%2Fsecure%2Fcontained%2Fchangeactivity
%3Funid%3Da6506357e41d4c63b809565f4f1aa31e&data=05%7C01% art 5 1-2e 40pzh.nl
%7C9c4623348d634d9d0ba108dad14df1b3%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638052429938884371%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=0bR9C7Ce1mx3pS%2BvI9j0tIyHtK3bZ8RVI80uxJXzQ0k
%3D&reserved=0> bekijken.

Met vriendelijke groet,

<HTTPS://pvzh.topdesk.net/tas/images/email_footer.jpg>

Het Loket telefoon 070 4417777 pvzh.topdesk.net
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Fpvzh.topdesk.net%2F&data=05%7C01% art 5 1-2e 40pzh.nl
%7C9c4623348d634d9d0ba108dad14df1b3%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638052429938884371%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=e8tE%2F%2FPKT%2FZIti1NrL7pq4wtFmV8hrnWBEFNxn5HZ8M
%3D&reserved=0>

"


provincie
Zuid-Holland

provincie Zuid-Holland

Van: art 5 1-2e
Verzonden: 2023-09-21 16:57:09.039000+00:00
Aan: art 5 1-2e
CC:
Onderwerp: RE: Spoedoverleg datalek
"
Voor onze afspraak morgen kunnen ook uitgenodigd worden:

* Functioneel beheer IDMS - art 5 1-2e
* BI team - art 5 1-2e

Groet,

art 5 1-2e

-----Oorspronkelijke afspraak-----
Van: art 5 1-2e)pzh.nl>
Verzonden: donderdag 21 september 2023 11:40
art 5 1-2e art 5 1-2e
Onderwerp: Spoedoverleg datalek
Tijd: donderdag 21 september 2023 14:00-14:45 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
Locatie: Microsoft Teams-vergadering
Urgentie: Hoog
Gevoeligheid: Privé

In overleg met art 5 1-2e)verleg vindt plaats via ms teams, duur +/- 30-45 min.

art 5 1-2e 1-09-2023

Microsoft Teams-vergadering

Neem deel vanaf uw computer, mobiele app of apparaat voor vergaderruimte

Klik hier om deel te nemen aan de vergadering
<https://teams.microsoft.com/l/meetup-join/19%3ameeting_MWVjZmNjZmMtMjhiYS00NjIwLTk1NTAtZDc1MjFhMWJiOTM2%40thread.v2/0?context=%7b%22Tid%22%3a%226d99bc28-8f28-4a73-a501-63a8e1eb3040%22%2c%22Oid%22%3a%2260ca2822-a24e-466f-858d-0b2687af1079%22%7d>

Vergadering-id: 392 270 975 314
Wachtwoordcode: zrL98A

Teams downloaden <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.microsoft.com%2Fen-us%2Fmicrosoft-teams%2Fdownload-app&data=05%7C01% art 5 1-2e 0pzh.nl%7Ce9c99ffefa2b4360d9ab08dbba86b084%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638308859871201611%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=s0PhX0K6ioqKkZH926MZoGqfuJoT7cOgAj00pC0DLBA%3D&reserved=0> | Deelnemen op het web <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.microsoft.com%2Fmicrosoft-teams%2Fjoin-a-meeting&data=05%7C01%7Cmhe.nijenkamp%40pzh.nl

%7Ce9c99ffefa2b4360d9ab08dbba86b084%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638308859871201611%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=RNjQ5HnnnDDsuRxIVhF8tXTbGigYre7eb9zjaUZAvOw
%3D&reserved=0>

Meer informatie <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Faka.ms%2FJoinTeamsMeeting&data=05%7C01%7 art 5 1-2e 40pzh.nl
%7Ce9c99ffefa2b4360d9ab08dbba86b084%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638308859871201611%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=35%2FTSpqXg
%2FG9pI0efLjbGBIC5wl3CoMR22RYz2IRXW4%3D&reserved=0> | Opties voor vergadering
<https://teams.microsoft.com/meetingOptions/?organizerId=60ca2822-a24e-466f-
858d-0b2687af1079&tenantId=6d99bc28-8f28-4a73-a501-
63a8e1eb3040&threadId=19_meeting_MWVjZmNjZmMtMjhiYS00NjIwLTk1NTAtZDc1MjFhMWJiOTM
2@thread.v2&messageId=0&language=nl-NL>

"