AUTORITEIT
PERSOONSGEGEVENS

10 tips voor professionele datalekregistratie

Deze tips zijn zowel van toepassing op het registreren van datalekken die u verplicht bent te melden bij de Autoriteit Persoonsgegevens (AP) als om incidenten die u niet hoeft te melden. De tips vormen een aanvulling op de Q&A's over datalekken op onze website.

Omschrijf incidenten, de gevolgen en de corrigerende maatregelen **duidelijk en volledig.**

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.

Voorkom versnippering van registraties: maak **één overzichtelijke registratie** die voor elk organisatieonderdeel tot op hetzelfde detailniveau wordt ingevuld. Overweeg bijvoorbeeld om de registratie inzichtelijk te maken voor alle medewerkers zodat zij het overzicht kunnen checken voordat zij zelf iets registreren.

Heeft uw organisatie een **functionaris gegevensbescherming** (FG)? Neem dan per incident op of de FG betrokken is en, zo ja, in welke mate.

Neem per incident op of het datalek is **gemeld bij de AP en de betrokken personen** en motiveer waarom dat wel of niet is gebeurd.

Wees **transparant naar de getroffen personen** als er een datalek is geweest. Communiceer hier duidelijk en tijdig over. Bewaar het bewijs van die communicatie en neem deze op in de registratie.

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.

Leg vast welke **andere organisaties** betrokken zijn geweest bij een inbreuk. Bijvoorbeeld medeverwerkingsverantwoordelijken, verwerkers of subverwerkers. Dit is handig als een organisatie nieuwe verwerkersovereenkomsten sluit met de desbetreffende verwerkers.

Overweeg om de datalekken in te delen naar **aard, gevolgen en betrokkenen en mogelijke maatregelen.**

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 of privacycontactpersoon van uw organisatie kan bij deze besprekingen een actieve rol vervullen.

"Van: art 5 1 2e art 5 1-2e
Verzonden: 2020-10-20 15:25:50.070000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: 201019 reactie Jaarverslag Privacy 2019 vs 2 update art 5 1-2e
"
Hey art 5 1-2e

Hierbij onze update/reactie op het AVG stuk.

Met vriendelijke groet,

art 5 1-2e

Hoofd Duurzaam Digitaal Informatiebeheer

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>

Werkdagen: maandag, dinsdag, donderdag en vrijdag

I&A heeft een groep op het Binnenplein! De ‘groep I&A’ biedt nieuws, antwoorden op veelgestelde vragen en geeft tips.
"

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 actueele projectplanning opgesteld. Eind juni is de update gereed en aansluitend zal een projectplan worden opgesteld voor verbeteringen. Update iDMS is het weekend van 17-10-2020 succesvol uitgevoerd. Nu kan er gestart worden met het doorvoeren van vernieuwingen. Dat is een meerjarig traject. PvA 5 okt in MT I&A besproken en memo in PO gedeeld met

		gedeputeerde de Zoete hierover.
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	Borg dat de FG altijd bij de start van een nieuw project wordt geïnformeerd over de intenties van het project, ook wanneer	Advies wordt overgenomen. Het innovatieteam van de provincie heeft hier aandacht voor en

beeld	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.	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. EAA wordt gevraagd te heronderzoeken welk effect de campagne de afgelopen 1,5 jaar heeft gehad tot op heden. Dit is geen afsluiting, maar een 1 meting. FG is

		onderdeel van de werkgroep van deze campagne en doet hierin actief mee.
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	Advies wordt overgenomen. Na de pilot zullen de uitkomsten vergeleken worden met de eisen

	pilot.	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.


provincie
ZUID HOLLAND

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: CONCEPT

Melding gegevens

Naam melder	:	art 5 1-2e EAA)
Registratienummer van het incident	:	n.t.b.
Datum en tijdstip van de melding	:	Maandag 25 maart 10:53
Route van de melding	:	Per e-mail aan de FG

Advies

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

Situatie

(*korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*
De Statengriffie afgelopen mei 2018 begonnen met het weglakken van persoonsgegevens uit ingekomen stukken (alleen die uit het publiek komen) die zij in het Staten Informatie Systeem op internet publiceert. De naam van de inzender wordt niet weggelakt, maar wel de overige contactgegevens (zoals adresgegevens en e-mailadres) en ook eventuele handtekeningen van particulieren.

Gebleken is echter dat door de manier waarop is weggelakt, het toch mogelijk blijkt om er achter te komen welke gegevens er oorspronkelijk onder de zwarte balk staan. Namelijk door de zwarte balk te kopiëren en elders te plakken. Dit werkt overigens alleen bij tekst, maar niet bij weggelakte handtekeningen. Ook zijn de weggelakte tekstuele gegevens vindbaar via zoekmachines als Google. Maar dan moeten al wel bekend zijn bij degene die zoekt.

Melding is gedaan door een inzender van een ingekomen stuk. Het bezwaar werd gemaakt tegen het achterhaalbaar zijn van het e-mailadres, niet tegen het laten staan van de naam van de betrokkene. Ook uit de eigen organisatie is dit gesignaleerd.

Inmiddels is de manier van weglakken aangepast, waardoor nieuwe weglakkingen wel definitief onleesbaar zijn. De reeds gepubliceerde stukken ~~worden~~ zijn gedepubliceerd.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Inschatting op dit moment: ca 20 documenten Per document verschilt het aantal persoonsgegevens. Soms een e-mail met alleen een e-mailadres. Soms gaat het om adresgegevens. De ingekomen stukken gaan over verschillende onderwerpen. Welke precies, wordt nu onderzocht.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend. De documenten zijn gepubliceerd in het provinciale Staten Informatie Systeem, dat via internet toegankelijk is.

Vraag	Antwoord
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Documenten zijn in het Staten Informatie Systeem als PDF gepubliceerd. De documenten kunnen worden gelezen en gekopieerd, maar niet worden gewijzigd of verwijderd.
Welke persoonsgegevens betreft het?	Dat is per brief verschillend; Adresgegevens, e-mailadres.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	~~De eerste inschatting is dat dit niet het geval is.~~ ~~Dit wordt nader onderzocht.~~ Nee. Onderzoek heeft uitgewezen dat het de categorie normale persoonsgegevens betreft (geen bijzondere / hoog risico gegevens).
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Onbekend. De documenten zijn gepubliceerd in het provinciale Staten Informatie Systeem, dat via internet toegankelijk is.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	~~Wordt nader onderzocht door te beoordelen wat de context van de ingekomen stukken zijn.~~ De aard van de persoonsgegevens (e-mailadres en adres) is niet van dien aard dat er sprake is van een risico voor de rechten en vrijheden van betrokken natuurlijke personen. Daarbij is er geen aanleiding om te denken dat er gevoelige gegevens op straat zijn gekomen.
Betreft het een beveiligingsincident?	Ja
Betreft het een datalek?	Ja
Ondernomen beperkende maatregelen.	De stukken ~~worden~~ zijn gedepubliceerd.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Depublicatie. Aanpassing van de wijze waarop vanaf nu wordt weggelakt.

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.

[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.

Conclusie

Dit betreft een voorlopige conclusie. Nog niet alle informatie is op dit moment bekend.
Op dit moment is er geen aanleiding om te denken dat er gevoelige gegevens op straat zijn gekomen. De aard van de persoonsgegevens (e-mailadres en adres) is niet van dien aard dat er sprake is van een een risico voor de rechten en vrijheden van betrokken natuurlijke personen.
~~Om hier een betere inschatting te kunnen maken wordt op dit moment ook de inhoud van de brieven nader bekeken. Een definitief oordeel is daarna pas mogelijk. Gezien de 72 uur termijn wordt dit geval wel als datalek aan de Autoriteit Persoonsgegevens gemeld. Nadere aanvulling op de melding volgt.~~
Onderzoek heeft uitgewezen dat het de categorie normale persoonsgegevens betreft (geen bijzondere / hoog risico gegevens). De aard van de persoonsgegevens (e-mailadres en adres) is niet van dien aard dat er sprake is van een risico voor de rechten en vrijheden van betrokken natuurlijke personen. Daarbij is er is geen aanleiding om te denken dat er gevoelige gegevens op straat zijn gekomen.

Advies

De conclusie is dat er sprake is van een beveiligingslek en dat er 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 meldingsplichtig is bij de Autoriteit Persoonsgegevens.
- er géén 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

"Van: art 5 1-2e
Verzonden: 2019-03-26 12:19:39+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Datalekken: Scans van paspoorten algemeen toegankelijk op IDMS
"
Dag art 5 1-2e

Als ik een zoekterm ingeef in iDMS voor paspoort krijg ik o.a. dit te zien . En ik kan ook daadwerkelijk bij de documenten.

Dat is toch wel een redelijk foute boel.

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/> .
"


Buiten reikwijdte Woo-verzoek


provincie
ZUID HOLLAND

Overleg datalekteam over datalek identiteitsbewijzen

28 maart 2019

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

Bevindingen

Paspoort Jeannette Baljeu – geen probleem

Paspoort art 5 1-2e – geen probleem

- Geplaatst door art 5 1-2e
- Alleen ingezien doo art 5 1-2e

Paspoort art 5 1-2e = directeur Warmteparticipatiefonds

- art 5 1-2e Programma's en Projecten
- **Wie vraagt na?**

Roparun 2014 – 20 paspoorten Gesprek met art 5 1-2e **Actie** art 5 1-2e

art 5 1-2e - 27-03-2019 (heel recent)

- Paspoort art 5 1-2e art 5 1-2e
- Waarom gekeken ?

Prozha 2009 20 stuks – Gesprek met art 5 1-2e **Actie** art 5 1-2e

20 ID's geplaatst in 2009

art 5 1-2e heeft in 22-11-2012 1 week voor uitdiensttreding paspoorten gezipt & gedwonload

- O.a. art 5 1-2e art 5 1-2e
- En de andere waarschijnlijk ook

Verder behandeld in 2009 door een aantal Prozha mensen

Melden aan art 5 1-2e en Jeannette: **Actie** art 5 1-2e **gereed)**

- Informeren art 5 1-2e - **Actie** art 5 1-2e **GEREED)**

Overzicht van identiteitsbewijzen volledig maken – **Actie** art 5 1-2e

- Per ID: wie heeft het benaderd?

"Van: art 5 1-2e
Verzonden: 2019-04-05 13:51:37+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: FW: Onderzoek datalek (reactie art 5 1-2e
"
Deze ook graag op de agenda

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
Verzonden: maandag 1 april 2019 11:29
Aan: art 5 1-2e
Onderwerp: FW: Onderzoek datalek (reactie art 5 1-2e

art 5 1-2e zie onder.

De vraag is inderdaad of de kopie nog nodig is.

Hoe zullen we dat aanpakken?

Van: art 5 1-2e
Verzonden: vrijdag 29 maart 2019 18:52
Aan: art 5 1-2e
Onderwerp: Fwd: Onderzoek datalek

Hoe zit dat? ;)

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

Van: "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Datum: 29 maart 2019 om 15:30:31 CET
Aan: "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Kopie: ""Baljeu, J.N."" <j.baljeu@pzh.nl <mailto:j.baljeu@pzh.nl> >,
"" art 5 1-2e " < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Antw.: Onderzoek datalek

Dnk voor het informeren. Erg zorgelijk en ik hoor graag hoe zeker wordt gesteld dat bij het aantreden van het nieuwe college mijn kopie identiteitsbewijs uit idms wordt verwijderd.

Met vriendelijke groet,

art 5 1-2e

On Thu, Mar 28, 2019 at 4:04 PM +0100, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Geachte art 5 1-2e

Op verzoek van art 5 1-2e maak ik u attent op het onderstaande bericht.

Mocht u naar aanleiding hiervan nog vragen of behoefte aan nadere toelichting hebben, dan hoor ik dat 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

Postbus 90602 | 2509 LP Den Haag

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

Van: art 5 1-2e
Verzonden: donderdag 28 maart 2019 12:55
Aan: art 5 1-2e Baljeu, J.N.
CC: art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: Onderzoek datalek

Beste art 5 1-2e en Jeannette,

Het privacyteam - inclusief FG art 5 1-2e - onderzoekt op dit moment een situatie die we als datalek beschouwen.

Zoals altijd stuur ik jullie z.s.m. het analyse- en adviesrapport.

Omwille van de snelheid informeer ik jullie nu vast per e-mail.

Situatie

Het betreft de aanwezigheid van in totaal 75 kopie identiteitsbewijzen gevonden op 6 locaties in het iDMS.

De eerste documenten zijn in 2009 in iDMS geplaatst.

De toegang tot deze locaties was niet beperkt, zodat alle medewerkers in principe toegang kónden hebben.

Als eerste actie zijn de toegangsrechten tot de iDMS locaties gecorrigeerd, zodat oneigenlijke toegang niet meer mogelijk is.

LET OP! Het betreft ook het paspoort van Jeanette en dat van art 5 1-2e die in de iDMS omgeving van het Nazorgfonds Zuid-Holland staan.

Hiervan konden we vaststellen dat er géén oneigenlijke toegang is geweest en er slechts eén persoon vanuit zijn functie toegang toe heeft gehad. We achten het risico op misbuik hierdoor verwaarloosbaar. De bestanden zijn inmiddels niet meer voor anderen toegankelijk.

Vervolgacties

Belangrijk voor het bepalen van vervolgacties is, dat we de ernst van de situatie kennen.

Een eerste analyse van de iDMS loggegevens toont aan dat we voor 2 van de 6 iDMS locaties op dit moment nader onderzoek willen doen naar de reden waarom enkele personen één of meerdere ID-bestanden hebben geopend.

Vooralsnog beschouwen we dit als een (inmiddels gedicht) datalek.
De kans bestaat dat de in de logging geconstateerde toegang verklaarbaar is, zodat het risico voor betrokkenen klein of verwaarloosbaar is.

De uitkomst van de analyse bepaalt onze verdere acties richting Autoriteit Persoonsgegevens en betrokkenen.

Ik houd jullie op de hoogte.

Voor vragen en nadere toelichting ben ik – of de FG - uiteraard beschikbaar.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Directie Concernzaken | Afdeling I&A

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

Postbus 90602 | 2509 LP Den Haag

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

"


provincie
ZUID HOLLAND


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-04-12 10:34:23.445000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Datalekje???
"
Is duidelijk; ik kan er inderdaad ook bij.

Ben er mee bezig.

Van: art 5 1-2e
Verzonden: donderdag 11 april 2019 16:44
Aan: art 5 1-2e
Onderwerp: Re: Datalekje???
Gevoeligheid: Vertrouwelijk

Ik bel je morgen.

Op 11 apr. 2019 om 13:30 heeft art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl>
> het volgende geschreven:

Hi art 5 1-2e

Misciien iets dat jouw aandacht nodig heeft:

<image001.png>

Met vriendelijke groet,

art 5 1-2e

Tactisch specialist informatieveiligheid

Afdeling Informatisering en Automatisering | bureau Advies en Beleid

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

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: 2019-04-25 15:20:56.690000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: wat aan AP geleverd?
"
Dit was de e-mail aan de AP (excl de bijlagen)

###

Geachte art 5 1-2e

Naar aanleiding van uw verzoek stuur ik u twee overzichten:

- Het logboek datalekken.
Dit is een overzicht met de meest relevante informatie. Per geval is er een achterliggend dossier waarin zich onder meer de analyses, adviesdocumenten, evaluatieverslagen en e-mails bevinden.

- Een overzicht van de via een digitaal formulier gemelde gevallen van vermissing of diefstal van ICT-middelen (sinds april 2017).
Per melding is beoordeeld of er sprake kan zijn van verlies van persoonsgegevens.

De documenten zijn beveiligd met hetzelfde wachtwoord wat ik u separaat per sms toestuur.

Mocht u naar aanleiding hiervan nog aanvullende informatie nodig hebben, dan hoor ik dat graag van u.

Met vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e
Verzonden: donderdag 25 april 2019 13:06
Aan: art 5 1-2e
Onderwerp: wat aan AP geleverd?

Hoi art 5 1-2e

Zou je mij nog even kunnen mailen wat jij destijds aan de AP hebt geleverd n.a.v. hun onderzoek datalek administratie?

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

"Van: art 5 1-2e
Verzonden: 2019-05-17 14:53:23+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Afhandeling datalekken
"
Hoi art 5 1-2e

Ik heb even een stukje ingevuld; deel moet nog worden uitgezocht (maar ik mag eerst even naar de tandarts, zegt mijn agenda).

Volgens mij kan dit dienen als uitgangspunt voor het gesprek van maandag.

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
Verzonden: vrijdag 17 mei 2019 14:31
Aan: art 5 1-2e
Onderwerp: Afhandeling datalekken

""Afhandeling datalekken"" kan via de volgende koppeling worden geopend: http://idms/otcs/llisapi.dll/properties/646462858

Hier staat ook de template voor het adviesdocument. Die tabel moeten we invullen om tot de beoordeling te komen.

MvgEJ
"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Melding gegevens

Naam melder	:
Registratienummer van het incident	:
Datum en tijdstip van de melding	:
Route van de melding	:

Advies

Opgesteld door	:
Datum en tijdstip advies	:
Advies besproken met	:
Advies ter kennisgeving gedeeld met	:

Situatie

(*korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken 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)	In te vullen door art 5 1-2e adhv Excel van art 5 1-2e art 5 1-2e
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	In te vullen door art 5 1-2e
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Mogelijk: inzien, afdrukken, mailen
Welke persoonsgegevens betreft het?	Voornaam, achternaam, functie en organisatie
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?	Waarschijnlijk wel, maar is niet uit te sluiten dat deze ook per mail zijn gedeeld met anderen buiten PZH
Houdt de inbreuk op de persoonsgegevens een hoog risico	Ja, reputatieschade

[1] Zoals: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, werkprestaties, gegevens die betrekking hebben op levensovertuiging, gegevens die betrekking hebben op gezondheid.

Vraag	Antwoord
voor betrokkenen in[2]?	
Betreft het een beveiligingsincident?	Ja
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**; Een strikte interpretatie leidt tot de conclusie dat hier wel inbreuk is in verband met persoonsgegevens en derhalve dat het een datalek betreft.
Ondernomen beperkende maatregelen.	art 5 1-2e
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	m.i. moet er een grondige inventarisatie plaats vinden van de huidige rechtenstructuur van iDMS en zal er veel meer aandacht besteed moeten worden aan het op de juiste wijze plaatsen en beheren van mappen en documenten.

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

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

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 WEL/NIET sprake is van een beveiligingslek en dat er WEL/NIET 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/NIET meldingsplichtig is bij de Autoriteit Persoonsgegevens.
- er WEL/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

Kentallen iDMS

Onderzoek rechtenstructuur

We hebben het onderzoek opgeknipt; op dit moment is gezocht in de ca. 85.000 e-dossiers in primaire en ondersteunende processen, hier verwachten we namelijk grootste risico's. Daarna zal de zoekactie worden herhaald in het organieke deel van iDMS. Tot slot willen we een steekproef doen of de rechten in het digitale archief en op de persoonlijke werkomgevingen in iDMS in orde zijn.

In totaal zijn er 60 e-dossiers aangetroffen waar iets mee aan de hand is: volgens onze analyse zou de toegang tot deze dossiers beperkt moeten zijn, maar op onderdelen van het dossier kan de hele organisatie meelezen. Van 10 dossier zijn de rechten al gecorrigeerd.

Herstel

Blijven er 50 e-dossiers over waarvan I&A binnenkort de behandelend ambtenaren benadert om te overleggen hoe de rechten moeten staan en deze vervolgens te corrigeren. Te beginnen bij de top 3:

- Grondzaken: 5 e-dossiers
- AO/IC – Jaarrekening: 6 e-dossiers
- Economische Zaken: 5 e-dossiers

Het voorkomen van herhaling

De ontstane problemen zijn veroorzaakt door menselijk handelen. Zowel door iDMS beheerders die geen uniforme werkwijze hanteren bij het beperken van de rechten in iDMS.

- Inventariseren, evalueren en eventueel aanpassen c.q. opstellen aanwezige procedures m.b.t. het verkrijgen van admin rechten of rechten om lokaal autorisatie te wijzigen in iDMS
- Inventariseren wie rechten heeft om rechten te wijzigen en evalueren noodzaak
- Instrueren van beheerders
    - Meekijken met de beheerders die rechten wijzigen
    - Inventariseren welke procedures er vastgelegd moeten zijn
    - Vastleggen procedures
    - Realiseren kennisoverdracht
- Uitvoeren periodieke check op de rechten beperkt toegankelijke locaties
    - Periodiek uitvoeren controlerun en herstel daarop uitvoeren
    - Evalueren procedures volgens plan-do-check-act

Ook komt het voor dat ambtenaren niet weten hoe rechten beperkt kunnen worden en zelf de tekst "(beperkt toegankelijk)" toevoegen aan de dossiernaam in de verwachting dat onbevoegden er niet meer bij kunnen. Hier zullen we de oplossing zoeken in opleiding (we denken aan verplichte iDMS cursus na in diensttreding) en in de bewustwording.

Onderzoek persoonsgegevens (AVG)

De AVG stelt eisen aan de afscherming van persoonsgegevens, ook in iDMS.

Over een concrete zoekmethode zijn we op dit moment nog in gesprek. We moeten rekening houden met de belasting die het zoeken op het systeem legt en de bruikbaarheid van de zoekresultaten.

Analoog aan het afhandelen van het rechtenprobleem, zullen de eigenaren van documenten worden benaderd om documenten met persoonsgegevens op een andere (afgeschermde) plaats op te slaan of te vernietigen.

Anders dan bij het rechtenprobleem, speelt er bij het verkeerd (openbaar) plaatsen van persoonsgegevens in iDMS voornamelijk onwetendheid. Naast het technische spoor (zoeken en herstellen), draagt de aandacht voor persoonsgegevens in de Up-to-data campagne bij tot bewustwording en gevoel verantwoordelijkheid voor het netjes afschermen van persoonsgegevens bij de medewerkers. Mogelijk worden hierbij ook de beoogde privacyofficers in de afdelingen ingezet.

Planning werkzaamheden

De werkdruk op de iDMS beheerders is op dit moment aanzienlijk. Dit neemt niet weg dat het benaderen van behandelend ambtenaren vast van start gaat.
Wel zullen daarom het onderzoek moeten prioriteren ten opzichte van andere werkzaamheden. Daarna kunnen we een planning maken voor de komende periode.

"Van: art 5 1-2e
Verzonden: 2019-07-19 09:34:20.947000+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: FW: melding M19 05 01087
"
Hallo allen,

Graag dinsdag tijdens het privacyteam inhoudelijk bespreken.

Vast een fijn weekend!

Van: art 5 1-2e
Verzonden: vrijdag 19 juli 2019 09:29
Aan: art 5 1-2e <art 5 1-2e pzh.nl>
Onderwerp: FW: melding M19 05 01087

Zullen we deze a.s. dinsdag bespreken?

Van: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 21 juni 2019 15:44
Aan: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: melding M19 05 01087

art 5 1-2e. Mondeling :(uit mijn hoofd gezegd

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
Verzonden: vrijdag 21 juni 2019 15:42
Aan: art 5 1-2e
Onderwerp: RE: melding M19 05 01087

Nee daar heb ik niets aan gedaan.

Lekker melding dit :(

Laten we die dan maar dinsdag tijdens het privacyteam overleg bespreken.

PS: Jij hebt de melding geregistreerd, maar wie heeft het bij jou gemeld?

Van: art 5 1-2e
Verzonden: vrijdag 21 juni 2019 10:19
Aan: art 5 1-2e
Onderwerp: melding M19 05 01087

Goedemorgen art 5 1-2e

Op 13 mei had ik 2 heel verschillende datalekken gemeld. De ene waar we, vooral jij, heel veel werk aan hebben gehad.

Maar ook het datalek met meldingsnummer M19 05 01087.

Kan het zijn dat je die wel opgepakt hebt, maar verder niet afgewerkt hebt?

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

Melden datalek

Aanmelder

Naam	art 5 1-2e
Gebouw	Gebouw C
Telefoonnummer	onbekend
E-mail	art 5 1-2e @pzh.nl
Organisatie-eenheid	Bureau Beleidscoördinatie en Advies
Kostenplaatscode	411
Ruimte (Aanmelder)	C3.51
Specificatie	Kantoor
Plaats	Den Haag

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Afsprakenmails van Zorg van de Zaak zijn naar verkeerde leidinggevenden gestuurd, als gevolg van het wijzigen van de organisatiestructuur. De inbreuk heeft meerdere keren plaats gevonden. Intussen is technisch de inbreuk verholpen. De inbreuk is vandaag gemeld bij de FG.
Wat voor soort incident heeft er plaats gevonden?	Mail naar een verkeerde ontvanger
Wanneer vond de inbreuk plaats? Indien bekend	
Wanneer vond de inbreuk plaats? Indien niet bekend	februari-maart 2019
	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)	werknemers
Schatting van het aantal personen betrokken bij het datalek: minimaal	1
Schatting van het aantal personen betrokken bij het datalek: maximaal	300

"Van: art 5 1-2e
Verzonden: 2019-07-25 14:01:57.377000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: datalek zorg van de zaak is afgehandeld
"
Top, dankjewel.

Succes met het zoeken van een huis!

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 < art 5 1-2e pzh.nl>
Verzonden: donderdag 25 juli 2019 14:00
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: datalek zorg van de zaak is afgehandeld

Hoi art 5 1-2e

Ik zie dat je toch nog op je vrije dag bezig bent geweest .

Dat gevalletje is afgehandeld, ook met art 5 1-2e

Fijne vakantie!

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

"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

"Van: Baljeu, J.N."
Verzonden: 2019-07-25 14:55:29+00:00
"Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: RE: Advies_in_kader_van_meldplicht_datalekken_10_05_2019
"
Dank voor advies, akkoord met advies.

Jeannette

Van: art 5 1-2e
Verzonden: donderdag 25 juli 2019 14:25
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

art 5 1-2e pzh.nl

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

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

"Van: art 5 1-2e
Verzonden: 2019-07-25 17:01:41+00:00
"Aan: art 5 1-2e
"CC: Baljeu, J.N."
Onderwerp: Re: Advies_in_kader_van_meldplicht_datalekken_05_06_2019
"

art 5 1-2e akkoord met je advies, art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Thu, Jul 25, 2019 at 3:08 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

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/> .

"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-08-27 15:25:05+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Fwd: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019
"
Dag art 5 1-2e

Waarschijnlijk een datalek...
Ik zal eerst extra info vragen en haar attenderen op het Loket.

Groet art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

---------- Forwarded message ----------
From: "" art 5 1-2e " < art 5 1-2e pzh.nl
<mailto art 5 1-2e pzh.nl> >
Date: Tue, Aug 27, 2019 at 3:16 PM +0200
Subject: FW: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019
To: "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >

Goedemiddag art 5 1-2e

Zie onderstaand bericht. Kan je mij hierover advies uitbrengen.

De Erfgoedtafel is een netwerkend tafel, die openstaand voor organisaties, belanghebbenden bij de ontwikkeling van de erfgoedlijn. Één van de kernpunten binnen de tafel is samenwerking tussen de deelnemers, in dit geval de deelnemers aan de erfgoedlijn Goeree-Overflakkee. Zo je wenst, kan ik je een toelichting geven op de werking van de tafel.

In afwachting van je reactie.

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: Secretariaat VEERO [mailto art 5 1-2e
Verzonden: dinsdag 27 augustus 2019 11:13
Aan: art 5 1-2e
CC: art 5 1-2e
Onderwerp: Re: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019

Geachte art 5 1-2e beste 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

art 5 1-2e

art 5 1-2e

art 5 1-2e

Op 23 aug. 2019, om 14:42 heeft art 5 1-2e <art 5 1-2e)pzh.nl <mailto art 5 1-2e pzh.nl> > het volgende geschreven:

Goedemiddag allen,

Mede namens uw voorzitter, art 5 1-2e nodig ik u van harte uit voor de bijeenkomst van de erfgoedlijn Goeree-Overflakkee op woensdag 28 augustus a.s. van 10.00 tot 12.30 uur. Aansluitend is er een lunch tot 13.30 uur. Locatie: Museum Ouddorps Raad- en Polderhuis, Raadhuisstraat 4, 3253 AN Ouddorp.

In de bijlagen vindt u het programma en de bijbehorende stukken.

Op het programma staat onder andere besluitvorming over het conceptadvies voor Gedeputeerde Staten over de projectvoorstellen 2020 en de vervolgstappen op de doorontwikkeling van de erfgoedlijn.

De bijeenkomst heeft een bijzonder tintje door de feestelijke onthulling van de touchscreentafel in het museum door onze voorzitter.

Op uw komst wordt gerekend. In verband met de lunch wordt een bericht van verhindering bijzonder op prijs gesteld.

Voor geïnteresseerden in het coalitieakkoord 2019-2023 van het nieuwe provinciaal bestuur; dit is hier te downloaden:
https://www.zuid-holland.nl/overons/coalitieakkoord-2019/
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.zuid-holland.nl%2Foverons%2Fcoalitieakkoord-2019%2F&data=02%7C01 art 5 1-2e
%40pzh.nl%7C82e2b001e8e04dab8b7708d72aced11c
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637024940070381231&sdata=URLsOC0knryN61uPpu1tRosGXdxvnNBgLduPuqM5RfE%3D&reserved=0>

Hartelijke groet, mede namens art 5 1-2e

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 <mailt o art 5 1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <https://eur03.safelin tlook.com/?url=http%3A
%2F%2Fwww.zuid-holland.nl%2F&data=02%7C01 art 5 1-2e 40pzh.nl
%7C82e2b001e8e04dab8b7708d72aced11c
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637024940070391228&sdata=F5jzD%2FvkYcNdHxWn%2BNaaMhttwmehcW%2FJY9btQYNQF%2BE%3D&reserved=0>

-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://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Feformulieren.zuid-holland.nl%2FDefault.aspx%3FscenarioID%3DscContact&data=02%7C01 art 5 1-2e 40pzh.nl
%7C82e2b001e8e04dab8b7708d72aced11c
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637024940070391228&sdata=oyHXK5Y1AU3kHx3jklj1bIRtATMSf67XxARupxei6vM%3D&reserved=0> .
"


provincie
ZUID HOLLAND


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-08-27 15:36:35+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Datalek
"
Dag art 5 1-2e

Helaas, is wel een datalek.
Ik heb gevraagd of art 5 1-2ehet wil melden in het Loket. Vraag is even of het gemeld moet worden bij AP...ga ik nu over nadenken.

Groet art 5 1-2e

Van: loket@pzh.nl
Verzonden: 2019-08-27 15:54:28+00:00
"Aan: art 5 1-2e art 5 1-2e ; art 5 1-2e art 5 1-2e
CC:
Onderwerp: Er is een melding van een Datalek ontvangen. (M19 08 02408)
"

Beste collega,

Er is een melding van een Datalek ontvangen.

Melden datalek: M19 08 02408

Je kunt deze hier <http://loket.pzh.nl/tas/secure/contained/incident?unid=651e470e19454ba9bd54d8a4828d05c9> behandelen.

Met vriendelijke groet,

Het Loket

<HTTP://loket.pzh.nl/tas/images/email_footer.jpg>

Het Loket telefoon 070 4417777 loket.pzh.nl <http://loket.pzh.nl> "

"Van: art 5 1-2e
Verzonden: 2019-08-27 16:34:30.751000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Datalek
"
Ha art 5 1-2e

Eerste reactie.

Of het een datalek is kan ik op basis van het formulier niet bepalen.

Daarvoor is het nodig dat ik art 5 1-2espreek. Ik zal art 5 1-2evragen hierbij aan te schuiven als vervanger van art 5 1-2e

Ik wil de email willen zien die verstuurd is incl adressering. Ook ben ik benieuwd hoe de geadresseerden zich tot elkaar verhouden.

Het betreft een netwerkorganisatie, waar waarschijnlijk contact met anderen een van de gerechtvaardigde doelen is.

Weet ik zo niet, maar zou kunnen

En mogelijk zijn de uitzonderingsgronden uit artikel 9.2 van toepassing. Bijvoorbeeld 9.2.e de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;

De contactgegevens bijvoorbeeld van art 5 1-2e art 5 1-2e (art 5 1-2estaan gewoon op de website van https://www.goeree-overflakkee.nl/portal/overzicht-producten-en-diensten_43368/product/veero-recreatie-en-toerisme_863.html.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

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

art 5 1-2epzh.nl <mailto : art 5 1-2epzh.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 <art 5 1-2epzh.nl>
Verzonden: dinsdag 27 augustus 2019 15:37
Aan: art 5 1-2e <art 5 1-2epzh.nl>
Onderwerp: Datalek

Dag art 5 1-2e

Helaas, is wel een datalek.

Ik heb gevraagd of art 5 1-2e het wil melden in het Loket. Vraag is even of het gemeld moet worden bij AP...ga ik nu over nadenken.

Groet art 5 1-2e

"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-08-27 18:18:13+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Fwd: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019
"
Dag art 5 1-2e

Zie onderstaande mail

Groet art 5 1-2e
Outlook voor Android downloaden <https://aka.ms/ghei36>

---------- Forwarded message ----------
From: "" art 5 1-2e " < art 5 1-2e pzh.nl
<mailto art 5 1-2e zh.n l
Date: Tue, Aug 27, 2019 at 3:32 PM +0200
Subject: FW: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019
To: "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >

Zie onderstaand art 5 1-2een mijn email van zojuist.

Groet

art 5 1-2e

_____

Van: art 5 1-2e
Verzonden: vrijdag, augustus 23, 2019 14:43
Aan: art 5 1-2e
art 5 1-2e

art 5 1-2e

Onderwerp: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019

Goedemiddag allen,

Mede namens uw voorzitter, art 5 1-2e nodig ik u van harte uit voor de bijeenkomst van de erfgoedlijn Goeree-Overflakkee op woensdag 28 augustus a.s. van 10.00 tot 12.30 uur. Aansluitend is er een lunch tot 13.30 uur. Locatie: Museum Ouddorps Raad- en Polderhuis, Raadhuisstraat 4, 3253 AN Ouddorp.

In de bijlagen vindt u het programma en de bijbehorende stukken.

Op het programma staat onder andere besluitvorming over het conceptadvies voor Gedeputeerde Staten over de projectvoorstellen 2020 en de vervolgstappen op de doorontwikkeling van de erfgoedlijn.

De bijeenkomst heeft een bijzonder tintje door de feestelijke onthulling van de touchscreentafel in het museum door onze voorzitter.

Op uw komst wordt gerekend. In verband met de lunch wordt een bericht van verhindering bijzonder op prijs gesteld.

Voor geïnteresseerden in het coalitieakkoord 2019-2023 van het nieuwe provinciaal bestuur; dit is hier te downloaden:https://www.zuid-holland.nl/overons/coalitieakkoord-2019/ <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.zuid-holland.nl%2Foverons%2Fcoalitieakkoord-2019%2F&data=02%7C01 art 5 1-2e %40pzh.nl%7C26f05d5af7b14bbfa67208d727c7ee8c %7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637021611967177592&sdata=vB0%2FBKm 3i7Ne1TT3x4itZ7UZ9Y0%2BmBbkDwfRh6e0P5s%3D&reserved=0>

Hartelijke groet, mede namens art 5 1-2e

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 <mailt o art 5 1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <https://eur03.safeli tlook.com/?url=http%3A
%2F%2Fwww.zuid-holland.nl%2F&data=02%7C01 art 5 1-2e 40pzh.nl
%7C26f05d5af7b14bbfa67208d727c7ee8c
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637021611967177592&sdata=XyPHgakqq
2bVMdrnX7ev6Xo1RUjyWtsHuUaxMCq4w%2B4%3D&reserved=0>

-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 hetcontactformulier
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Feformulieren.zuid-holla .aspx%3FscenarioID
%3DscContact&data=02%7C01 art 5 1-2e %40pzh.nl
%7C26f05d5af7b14bbfa67208d727c7ee8c
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637021611967187583&sdata=udvKqHaQ0
727yvgzJVg%2Fej75t81xoCApLm6ThJX2vTo%3D&reserved=0> .
"


provincie
ZUID HOLLAND


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-08-28 08:14:57+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Datalek
"
Ha art 5 1-2e

Ik heb er een nachtje over geslapen nou ja, kort nachtje werk wel thuis vandaag, maar voordat ik begon moest ik het hele huis nog weer aan de kant maken etc., want vanmiddag komen kijkers (maar dan heb ik een afspraak buiten de deur, dus dat komt goed uit)

Maar terug naar de case:

1. Je geeft aan dat gerechtvaardigd belang mogelijk een grondslag is voor de verwerking (art 6, lid 1 onder f): het vervelende is dat daarbij expliciet wordt een uitzondering wordt gemaakt voor overheidsinstanties, die zich niet op deze grondslag mogen beroepen bij de uitoefening van haar taken.

2. Vervolgens geef je aan dat er mogelijk een escape is ziende op art 9 lid 2 onder e; daar heb ik de volgende opmerkingen bij:

a. Art 9 behandelt de verwerking van bijzondere categorieën van persoonsgegevens; het betreft hier geen bijzondere persoonsgegevens

b. Lid e ziet inderdaad op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt; dat klopt inderdaad voor deze art 5 1-2e maar geldt dat ook voor de anderen?

3. De art 5 1-2e heeft ook in zoverre gelijk dat er tenminste toestemming gegeven had moeten zijn, we kunnen er echter, gelet op de looptijd van dit netwerk, absoluut niet zeker van zijn dat die toestemming expliciet is gegeven.

4. De opmerking van die art 5 1-2e at de adressen allemaal in de BCC geplaatst hadden moeten worden is juist; ik heb toevallig maandag net een blogje geschreven dat nog bij Communicatie ligt ter aanvulling over precies dit onderwerp.

Mijn inziens is het dus wel degelijk een inbreuk in de zin van de AVG; ik betwijfel of het gemeld moet worden aan de AP (ik worstel altijd met het begrip “rechten en vrijheden van natuurlijke personen”, althans met de praktische toepasbaarheid van dat begrip).

Mocht je nog vragen hebben, dan hoor ik het uiteraard 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
Verzonden: dinsdag 27 augustus 2019 16:35
Aan: art 5 1-2e
Onderwerp: RE: Datalek

Ha art 5 1-2e

Eerste reactie.

Of het een datalek is kan ik op basis van het formulier niet bepalen.

Daarvoor is het nodig dat ik art 5 1-2espreek. Ik zal art 5 1-2e vragen hierbij aan te schuiven als vervanger van art 5 1-2e

Ik wil de email willen zien die verstuurd is incl adressering. Ook ben ik benieuwd hoe de geadresseerden zich tot elkaar verhouden.

Het betreft een netwerkorganisatie, waar waarschijnlijk contact met anderen een van de gerechtvaardigde doelen is.

Weet ik zo niet, maar zou kunnen

En mogelijk zijn de uitzonderingsgronden uit artikel 9.2 van toepassing. Bijvoorbeeld 9.2.e de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;

De contactgegevens bijvoorbeeld van art 5 1-2e art 5 1-2e art 5 1-2e , art 5 1-2e staan gewoon op de website van https://www.goeree-overflakkee.nl/portal/overzicht-producten-en-diensten_43368/product/veero-recreatie-en-toerisme_863.html.

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: dinsdag 27 augustus 2019 15:37
Aan: art 5 1-2e
Onderwerp: Datalek

Dag art 5 1-2e

Helaas, is wel een datalek.

Ik heb gevraagd of art 5 1-2ehet wil melden in het Loket. Vraag is even of het gemeld moet worden bij AP...ga ik nu over nadenken.

Groet art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>
"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-08-28 12:39:55.248000+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e art 5 1-2e
Onderwerp: RE: Datalek
"
Hallo art 5 1-2e

Bij afwezigheid van art 5 1-2e wil ik je graag betrekken bij de beoordeling van een melding van een datalek.

* De melding vind je in bijlage 1.
* De mail waar het om gaat vind je in bijlage 2.

De procedure (verkort weergegeven in bijlage 3 en onverkort in bijlage 4) is dat we zo snel mogelijk maar uiterlijk 72 uur na aanmelding komen tot een beoordeling en een advies aan de concerndirecteur.

Voor het advies bestaat een template; die vul ik in als we er samen uit zijn.

In dit geval doen we de beoordeling met 3 man: art 5 1-2e jij en ik.

art 5 1-2een ik werken vandaag huis hebben telefonisch al even afgestemd.

Wij kunnen via de mail afstemmen en als dat handig is vanmiddag even bellen.

De lijn van art 5 1-2een mij op dit moment. Graag jouw mening hierover:

1. art 5 1-2heeft in een e-mail e-mailadressen van relaties opgenomen. Daardoor konden alle ontvangers elkaars e-mailadressen inzien. Omdat betrokkenen hier geen expliciete toestemming voor hebben gegeven en het openbaar maken van de e-mailadressen niet nodig is voor de uitoefening van de betreffende publieke taak (project Erfgoedlijn Goeree-Overflakkee) is er sprake van onrechtmatige verwerking. Dit is een datalek.

   * De emailadressen hadden in de Bcc moeten zitten, zodat ontvangers niet elkaars e-mailadressen kunnen zien
   * Ik wil van art 5 1-2e nog weten of de deelnemers elkaar en elkaars contactgegevens kennen (want uit de mail blijkt dat bijvoorbeeld er een voorzitter is). Dat verandert misschien de situatie.

2. Moet dit datalek gemeld worden bij de AP? => Nee

   * 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.
     In dit geval is dat niet het geval. De inhoud van de mail is een uitnodiging voor een bijeenkomst van project Erfgoedlijn Goeree-Overflakkee waar de geadresseerden bij betrokken zijn.

3. Moet dit datalek gemeld worden aan betrokkenen? => Nee

   * Heeft het datalek ook waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkenen, dan moeten ook deze personen geïnformeerd worden over het datalek.
   * Om bovengenoemde reden is dat hier niet het geval.
   * Wel zou art 5 1-2ein de eerstvolgende e-mail kunnen melden dat de adressen met oog op de AVG voortaan in de Bcc staan. Maar dat is iets anders dan op grond van de AVG melding doen van een datalek.

Graag je 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/>
"

provincie ZUID HOLLAND

Melden datalek

Aanmelder

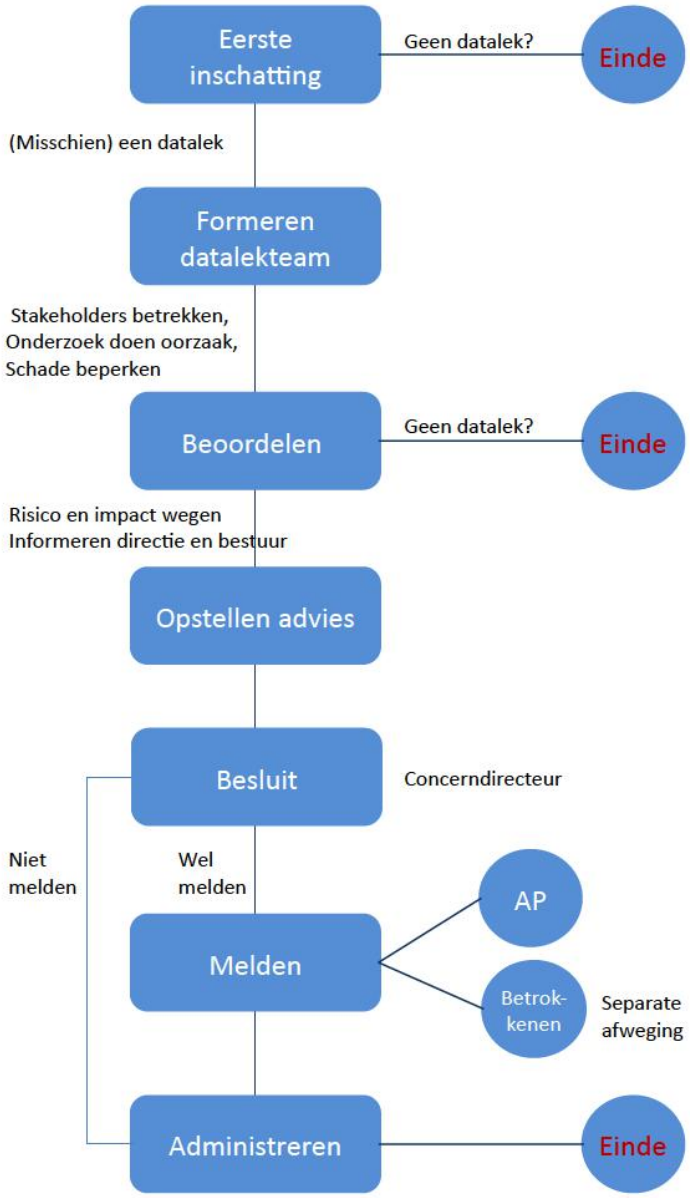
Naam	art 5 1-2e
Telefoonnummer	8331
E-mail	art 5 1-2e @pzh.nl
Organisatie-eenheid	Bureau Cultuur en Vrije tijd
Kostenplaatscode	395

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Een deelnemers aan de erfgoedtafel Goeree-Overflakkee attendeerde me op een mogelijke datalek i.v.m. versturen van de uitnodiging en stukken voor de bijeenkomst erfgoedlijn Goeree-Overflakkee. Dat gebeurt al ruim 7 jaar op deze wijze.
Wat voor soort incident heeft er plaats gevonden?	Anders
Anders? Graag toelichten	Email verstuurd aan deelnemers aan de erfgoedtafel Goeree-Overflakkee. De e-mailadressen staan in het vak 'geadresseerde' en zijn voor een ieder zichtbaar.
Wanneer vond de inbreuk plaats? Indien bekend	23 augustus 2019 14:30
Wanneer vond de inbreuk plaats? Indien niet bekend	Op bovengenoemd moment is de laatste e-mail aan de deelnemers aan de erfgoedtafel verstuurd. Vandaag is het incident gemeld door een deelnemers aan de erfgoedtafel.
	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)	en voor- en achternaam van de deelnemers met meestal de vermelding van de organisatie die zij vertegenwoordigen
Schatting van het aantal personen betrokken bij het datalek: minimaal	45
Schatting van het aantal personen betrokken bij het datalek: maximaal	50

Beoordelen datalekken



In beginsel moet ieder datalek aan de **Autoriteit Persoonsgegevens (AP)** 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.

provincie ZUID HOLLAND

Procedure voor het afhandelen van datalekken

Provincie Zuid-Holland

Mei 2018
Provincie Zuid-Holland
Versie: 1.1

overzicht besluitvorming / bespreking

Documenthistorie

Versie	Datum	Wie	Wijziging
1.0	7 februari 2016	art 5 1-2e	Eerste procedure
1.1	9 mei 2018	art 5 1-2e	Geactualiseerd n.a.v. de AVG

Vastgesteld door concerndirecteur art 5 1-2e op 11 mei 2018.

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Vanaf 1 januari 2016 is de meldplicht Datalekken van kracht. Dit houdt in dat de provincie verplicht is om (potentiële) datalekken te melden aan de landelijke toezichthouder, de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene van wie de gegevens zijn gelekt. Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) formeel van kracht die de huidige Wet bescherming persoonsgegevens (Wbp) vervangt. Ook onder de AVG geldt de meldplicht datalekken.

Er is echter wel een aantal veranderingen ten opzichte van de Wbp, die tot een lichte wijziging in de huidige procedure leidt. Zoals de aanwezigheid in de provincie van een functionaris voor de gegevensbescherming en licht aangepaste terminologie.

1.2 Persoonsgegevens

Een persoonsgegeven is volgens de AVG alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”). Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Er kan een onderscheid worden gemaakt in direct en indirect identificerende gegevens.

Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum.
Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.

Voorbeelden:

- Wanneer bijvoorbeeld een telefoonnummer (indirect identificerend) via een telefoonboek gekoppeld kan worden aan een naam (direct identificerend), dan is het telefoonnummer een persoonsgegeven. Bij de beoordeling of gegevens gekoppeld kunnen worden gaat het niet alleen om de gegevens die de verwerkingsverantwoordelijke in zijn bezit heeft. Ook gegevens die bijvoorbeeld via internet openbaar toegankelijk zijn kunnen worden meegewogen in de beslissing of iemand identificeerbaar is.
- Als door een combinatie van gegevens een dusdanig uniek beeld ontstaat dat de gegevens maar op één persoon betrekking kunnen hebben. Een voorbeeld van een dergelijke spontane identificatie is: ‘een 39-jarige mannelijke jurist woonachtig aan de Oxfordlaan te Leiden’. Het is zeer onwaarschijnlijk dat deze combinatie op meer dan één geïdentificeerde persoon betrekking heeft.

1.3 Datalek

In tegenstelling tot de Wbp, komt in de AVG het letterlijke woord datalek niet voor, maar wordt gesproken over “inbreuk in verband met persoonsgegevens”. Omdat de term datalek echter inmiddels ingeburgerd is, blijven wij (net als de Autoriteit Persoonsgegevens) deze term hanteren.

Bij een datalek is sprake van een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die eventueel zijn getroffen waren niet toereikend om dit te voorkomen.

Voorbeelden van een datalek zijn het verlies van een papieren document of mobiel apparaat waarop gevoelige persoonsgegevens staan. Maar ook computer hacking, besmetting met ransomware, of het technische falen van apparatuur, stroomuitval, wateroverlast kunnen leiden tot een datalek.

1.4 Inhoud meldplicht

De melding moet zo mogelijk gebeuren binnen 72 uur, zonder onderscheid tussen werkdagen, weekenden of feestdagen. Als het incident later dan 72 uur na ontdekking aan de Autoriteit Persoonsgegevens wordt gemeld, dan moet dit worden gemotiveerd. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. De Autoriteit Persoonsgegevens slaat de melding op in een register met alle ontvangen meldingen over datalekken. Dit register is niet openbaar.

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.

1.5 Doel en reikwijdte van deze procedure

Deze procedure beschrijft de wijze waarop binnen de provincie Zuid-Holland wordt omgegaan met de meldplicht datalekken in de zin van de Algemene Verordening Gegevensbescherming (AVG). De procedure is gericht op het beperken van de schade, analyseren van de (ernst van) de situatie en het opstellen van een onderbouwd advies aan de eindverantwoordelijke functionaris binnen de provincie. Dit is de concerndirecteur die gemandateerd is te besluiten om al dan niet melding te doen bij de Autoriteit Persoonsgegevens en betrokkenen (wiens persoonsgegevens het betreft).

De procedure wordt onder coördinatie van de afdeling I&A uitgevoerd, in nauwe samenwerking met de informatiebeheerder van P&O, de privacy jurist van FJZ, de I&A incident manager, een medewerker documentaire informatie van I&A, de functioneel/technisch beheerder van het systeem, betrokken medewerker(s) en diens leidinggevende. Per potentieel datalek wordt op die manier een datalekteam geformeerd.

De functionaris gegevensbescherming (FG) wordt geïnformeerd over het optreden van het potentiële datalek en de afhandeling ervan. De FG kan tijdens de afhandeling gevraagd en ongevraagd adviseren en beoordeelt de correcte uitvoering van de procedure. De FG kan hiertoe per afzonderlijk geval besluiten deel te nemen aan het datalekteam.

Hieronder volgt een nadere uitwerking van deze procedure.

2 Procedurebeschrijving

2.1 Melden incident

2.1.1 Interne medewerkers

De meldplicht datalekken geldt voor de gehele organisatie en iedere medewerker. Iedere medewerker die te maken heeft met vermissing/diefstal van zaken die van de provincie zijn, of met een informatiebeveiligingsincident, dient dit te melden bij het ICT-plein. Dit kan telefonisch via toestelnummer (070) 441 77 77 of via het meldingsformulier in het Loket op Topdesk.
Naam en contactgegevens van de melder worden automatisch in het formulier geregistreerd met de informatie over het incident. De melder kan namelijk gevraagd worden om aanvullende informatie te geven over het incident. Dit is belangrijk voor de goede en snelle afhandeling van het incident en de volledigheid voor een eventuele melding aan de AP.

2.1.2 Verwerkers van persoonsgegevens namens de provincie

Als er externe partijen zijn die in opdracht van de provincie persoonsgegevens verwerken, dan is met deze partijen een verwerkersovereenkomst gesloten, waarin is opgenomen hoe het onderlinge contact verloopt bij mogelijke datalekken. Het betreft dan vaak beveiligingsincidenten met applicaties die in het datacenter van de leverancier draaien.

2.1.3 Derden

Ook burgers of bedrijven kunnen melding doen van een mogelijk datalek bij de provincie. Op verschillende manieren kan zo'n melding de provincie bereiken. Men kan zich via de contactgegevens op de provinciale website wenden tot het Klantcontactcentrum of de provinciale functionaris gegevensbescherming. Ook is het mogelijk dat een burger of bedrijf zich eerst wendt tot de Autoriteit Persoonsgegevens. In dat geval zal de autoriteit contact opnemen met de provinciale functionaris gegevensbescherming.

De FG zal de melding registreren via het meldingsformulier in het Loket op Topdesk.

2.2 Beoordeling of er sprake is van een datalek

2.2.1 Eerste beoordeling

Zo snel mogelijk na de melding van een incident doet de adviseur informatieveiligheid (I&A) een eerste beoordeling of er sprake kan zijn van een datalek dat valt onder de meldplicht van de AVG. Als dit niet kan worden uitgesloten, formeert de adviseur informatieveiligheid het Datalekteam.

2.2.2 Formeren Datalek team

Het Datalekteam bestaat naast de adviseur informatieveiligheid, en afhankelijk van de situatie, uit: de informatiebeheerder van P&O, de privacy jurist van FJZ, de I&A incident manager, een medewerker documentaire informatie van I&A, de functioneel/technisch beheerder van het systeem, betrokken medewerker(s) en diens leidinggevende. Afhankelijk

van de beoordeling van situatie wordt de afdeling Communicatie betrokken in verband met persvoorlichting, interne en/of externe communicatie.

De adviseur informatieveiligheid informeert zo snel mogelijk telefonisch de FG.

2.2.3 Doelen en taken datalekteam

Het Datalekteam heeft als doelstelling:

- Maatregelen (laten) treffen ter beperken van verdere schade;
- Onderzoek te (laten) doen naar de oorzaak van het datalek;
- Gevolgen daarvan voor zowel de provincie Zuid-Holland als de bij het datalek betrokken personen vast te (laten) stellen;
- Acties vast te (laten) stellen voor afhandeling van het datalek en
- Uitgevoerde acties te (laten) controleren

De taken van het Datalekteam zijn:

- Vaststellen van noodzakelijke (directe) acties om de gevolgen van het datalek te beperken en in de toekomst vergelijkbare datalekken te voorkomen;
- Medewerkers van de provincie Zuid-Holland aan te sturen in de uitvoering van de noodzakelijke acties;
- Informeren van directie en bestuur;
- Zorg dragen voor besluitvorming ten aanzien van het datalek;
- (Indien noodzakelijk) interne communicatie rondom het datalek te (laten) verzorgen;
- Vaststellen van de wijze van informeren van betrokkenen (personen waarvan de gegevens bij het incident 'gelekt' zijn).

2.2.4 Beoordelen

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.

2.2.5 Advies

De FG gehoord hebbende stelt het datalekteam een advies op voor de concerndirecteur, belast met de bedrijfsvoering.
De concerndirecteur beoordeelt het incident en het bijgevoegde advies en besluit of er sprake is van een datalek dat gemeld moet worden aan de toezichthouder en eventueel de betrokkene(n).
Een afschrift van het advies wordt aan de FG toegezonden.
De gedeputeerde Middelen wordt geïnformeerd.

2.2.6 Melden

De adviseur informatieveiligheid is er verantwoordelijk voor dat het meldingsformulier van de toezichthouder wordt ingevuld en vervolgens wordt toegestuurd naar de toezichthouder.

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.

2.2.7 Administreren

De adviseur informatieveiligheid houdt een administratie bij waarin alle datalekken die zich voordoen in de organisatie geregistreerd worden. Dit betekent dat ook wanneer een lek niet gemeld hoeft te worden, er een documentatieplicht geldt.
De administratie bevat de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.

In het logboek worden in ieder geval de volgende gegevens vermeld:

a) het onderwerp van het datalek.
b) de datum van het datalek;
c) de duur van het datalek;
d) de aard van de inbreuk;
e) de instanties waar meer informatie over de inbreuk kan worden verkregen;
f) de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk gevolgen te beperken.
g) een beschrijving van de gevolgen voor de verwerkte persoonsgegevens;
h) de maatregelen die de provincie heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen;
i) de kennisgeving aan betrokkenen.

"Van: art 5 1-2e
Verzonden: 2019-08-27 18:18:13+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Fwd: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019
"
Dag art 5 1-2e

Zie onderstaande mail

Groet art 5 1-2e
Outlook voor Android downloaden <https://aka.ms/ghei36>

---------- Forwarded message ----------
From: "" art 5 1-2e " art 5 1-2e pzh.nl
<mailto art 5 1-2e pzh.nl> >
Date: Tue, Aug 27, 2019 at 3:32 PM +0200
Subject: FW: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019
To: "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >

Zie onderstaand art 5 1-2een mijn email van zojuist.

Groet

art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag, augustus 23, 2019 14:43
Aan: art 5 1-2e
art 5 1-2e

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

Onderwerp: Erfgoedlijn Goeree-Overflakkee: bijeenkomst woensdag 28 augustus 2019

Goedemiddag allen,

Mede namens uw voorzitter, art 5 1-2e nodig ik u van harte uit voor de bijeenkomst van de erfgoedlijn Goeree-Overflakkee op woensdag 28 augustus a.s. van 10.00 tot 12.30 uur. Aansluitend is er een lunch tot 13.30 uur. Locatie: Museum Ouddorps Raad- en Polderhuis, Raadhuisstraat 4, 3253 AN Ouddorp.

In de bijlagen vindt u het programma en de bijbehorende stukken.

Op het programma staat onder andere besluitvorming over het conceptadvies voor Gedeputeerde Staten over de projectvoorstellen 2020 en de vervolgstappen op de doorontwikkeling van de erfgoedlijn.

De bijeenkomst heeft een bijzonder tintje door de feestelijke onthulling van de touchscreentafel in het museum door onze voorzitter.

Op uw komst wordt gerekend. In verband met de lunch wordt een bericht van verhindering bijzonder op prijs gesteld.

Voor geïnteresseerden in het coalitieakkoord 2019-2023 van het nieuwe provinciaal bestuur; dit is hier te downloaden:https://www.zuid-holland.nl/overons/coalitieakkoord-2019/ <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.zuid-holland.nl%2Foverons%2Fcoalitieakkoord-2019%2F&data=02%7C01 art 5 1-2e %40pzh.nl%7C26f05d5af7b14bbfa67208d727c7ee8c %7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637021611967177592&sdata=vB0%2FBKm 3i7Ne1TT3x4itZ7UZ9Y0%2BmBbkDwfRh6e0P5s%3D&reserved=0>

Hartelijke groet, mede namens art 5 1-2e

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 <mailt o art 5 1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

www.zuid-holland.nl <https://eur03.safelin tlook.com/?url=http%3A
%2F%2Fwww.zuid-holland.nl%2F&data=02%7C01% art 5 1-2e 40pzh.nl
%7C26f05d5af7b14bbfa67208d727c7ee8c
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637021611967177592&sdata=XyPHgakqq
2bVMdrnX7ev6Xo1RUjyWtsHuUaxMCq4w%2B4%3D&reserved=0>

-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 hetcontactformulier
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Feformulieren.zuid-holland.nl%2FDefault.aspx%3FscenarioID
%3DscContact&data=02%7C01% art 5 1-2e 40pzh.nl
%7C26f05d5af7b14bbfa67208d727c7ee8c
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637021611967187583&sdata=udvKqHaQ0
727yvgzJVg%2Fej75t81xoCApLm6ThJX2vTo%3D&reserved=0> .
"


provincie
ZUID HOLLAND


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-08-28 13:24:13.972000+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e art 5 1-2e
Onderwerp: RE: Datalek
"
Dank. Ik verwerk dit in een adviesje.

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 < art 5 1-2e pzh.nl>
Verzonden: woensdag 28 augustus 2019 13:19
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: Datalek

Beste mensen,

Ik kan de weergegeven gedachtenlijn mede onderschrijven.

Ik zou overigens ook de vraag willen stellen welk type emailadressen het hier betreft. Gaat het om privé-emailadressen?. Of zijn het corporate adressen, zoals bijvoorbeeld @pzh.nl. In dat laatste geval zou nog minder aangenomen kunnen worden dat de persoonlijke levenssfeer van betrokkenen geschaad zou kunnen zijn (hooguit hun zakelijke “levenssfeer”).

En het zou ook de vraag zijn of de deelnemers in het kader van de communicatie over het betreffende project niet juist wenselijk zouden vinden dat men elkaar bereikbaarheidsgegevens kent. Ion plaats van in de eerstvolgende e-mail te melden dat de adressen met oog op de AVG voortaan in de Bcc staan, zou daaraan voorafgaand de vraag gesteld kunnen worden of men bezwaarheeft tegen het onderling mailen met kenbare e-mailadressen.

Maar overall eens: datalek ja, maar gelet op aard, omvang en mate waarin persoonlijke levenssferen geschaad zijn geen melding

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: woensdag 28 augustus 2019 12:40

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 <mailt o art 5 1-2e @pzh.nl> >
Onderwerp: RE: Datalek
Urgentie: Hoog

Hallo art 5 1-2e

Bij afwezigheid van art 5 1-2e wil ik je graag betrekken bij de beoordeling van een melding van een datalek.

* De melding vind je in bijlage 1.
* De mail waar het om gaat vind je in bijlage 2.

De procedure (verkort weergegeven in bijlage 3 en onverkort in bijlage 4) is dat we zo snel mogelijk maar uiterlijk 72 uur na aanmelding komen tot een beoordeling en een advies aan de concerndirecteur.

Voor het advies bestaat een template; die vul ik in als we er samen uit zijn.

In dit geval doen we de beoordeling met 3 man: art 5 1-2e jij en ik.

art 5 1-2een ik werken vandaag huis hebben telefonisch al even afgestemd.

Wij kunnen via de mail afstemmen en als dat handig is vanmiddag even bellen.

De lijn van art 5 1-2een mij op dit moment. Graag jouw mening hierover:

1. art 5 1-2eheeft in een e-mail e-mailadressen van relaties opgenomen. Daardoor konden alle ontvangers elkaars e-mailadressen inzien. Omdat betrokkenen hier geen expliciete toestemming voor hebben gegeven en het openbaar maken van de e-mailadressen niet nodig is voor de uitoefening van de betreffende publieke taak (project Erfgoedlijn Goeree-Overflakkee) is er sprake van onrechtmatige verwerking. Dit is een datalek.

   * De emailadressen hadden in de Bcc moeten zitten, zodat ontvangers niet elkaars e-mailadressen kunnen zien
   * Ik wil van art 5 1-2e nog weten of de deelnemers elkaar en elkaars contactgegevens kennen (want uit de mail blijkt dat bijvoorbeeld er een voorzitter is). Dat verandert misschien de situatie.

2. Moet dit datalek gemeld worden bij de AP? => Nee

o 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.
In dit geval is dat niet het geval. De inhoud van de mail is een uitnodiging voor een bijeenkomst van project Erfgoedlijn Goeree-Overflakkee waar de geadresseerden bij betrokken zijn.

3. Moet dit datalek gemeld worden aan betrokkenen? => Nee

o Heeft het datalek ook waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkenen, dan moeten ook deze personen geïnformeerd worden over het datalek.

o Om bovengenoemde reden is dat hier niet het geval.

o Wel zou art 5 1-2ein de eerstvolgende e-mail kunnen melden dat de adressen met oog op de AVG voortaan in de Bcc staan. Maar dat is iets anders dan op grond van de AVG melding doen van een datalek.

Graag je 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/>
"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-08-28 16:16:00.362000+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e
Onderwerp: RE: Vragen over melding datalek
"
Hallo art 5 1-2e

De lijn van beantwoording wordt: het is een datalek, dat niet aan de Autoriteit Persoonsgegevens en ook niet aan de betrokkenen gemeld hoeft te worden.

Dat zal ik onderbouwen in een advies dat ik je vanmiddag of morgenochtend mail.

Jouw antwoorden geven context aan het advies.

Het advies wordt voor akkoord voorgelegd aan de concerndirecteur en TKN aan gedeputeerde voor bedrijfsvoering Baljeu.

Het is ook goed om de inhoudelijk gedeputeerde te informeren; wie is dat?

En wil jij dat zelf doen of wil je dat ik dat op me neem?

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 art 5 1-2e)pzh.nl>
Verzonden: woensdag 28 augustus 2019 14:19
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
CC: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Re: Vragen over melding datalek

Dag art 5 1-2e

Ik ben extern en heb je bericht afgeluisterd. Ik kom er zsm op terug

Groetjes art 5 1-2e

On Wed, Aug 28, 2019 at 1:45 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Hallo art 5 1-2e

Je hebt een datalek gemeld, waarvan ik de afhandeling verzorg. Ik heb je voicemail ingesproken en ook al met art 5 1-2e gesproken, maar zou graag nog de volgende vragen willen stellen.

In je e-mail nodig je de geadresseerden uit “namens uw voorzitter”.

* Waar is art 5 1-2e voorzitter van en kennen de geadresseerden elkaar?
* Is het in het kader van de communicatie over het betreffende project niet juist wenselijk dat men elkaars bereikbaarheidsgegevens kent? In dat geval zou je in je eerstvolgende e-mail de vraag kunnen stellen of men bezwaar heeft tegen het onderling mailen met kenbare e-mailadressen. Nadeel hiervan is dat je de toestemming (in de vorm van de antwoorden op jouw mail) van de personen moet bewaren, en in de gaten houden dat je niet per ongeluk nieuwe adressen toevoegt zonder dat je daar toestemming voor hebt. Alternatief is om in je eerstvolgende e-mail te vermelden dat je met het oog op de AVG voortaan via de Bcc adresseert.

Ik zou overigens ook de vraag willen stellen welk type emailadressen het hier betreft. Gaat het om privé-emailadressen?. Of zijn het allemaal corporate adressen, zoals bijvoorbeeld @pzh.nl. In dat laatste geval zou nog minder aangenomen kunnen worden dat de persoonlijke levenssfeer van betrokkenen geschaad zou kunnen zijn (hooguit hun zakelijke “levenssfeer”).

art 5 1-2e

Het merendeel van de namen en rollen (niet de e-mailadressen) uit de e-mail staat ook genoemd in een document op internet: Verslag van de werksessie doorontwikkeling kwaliteitsimpuls erfgoedlijn Goeree-Overflakkee

d.d. 30 januari 2019. Voor dat soort publicaties zul je ook de toestemming van de deelnemers moeten hebben. art 5 1-2e kan je hierin adviseren.

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

"Van: art 5 1-2e
Verzonden: 2019-08-29 13:03:03+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e
Onderwerp: RE: Vragen over melding datalek
"
Dag art 5 1-2art 5 1-2e

Fijn dat we met elkaar gesproken hebben.

Ik heb nog even gegoogled op 'werksessie erfgoedlijn Goeree-Overflakkee' met dit als resultaat: https://www.google.com/search?source=hp&ei=X7BnXai8DszhkgXNzpYI&q=werksessie+erfgoedlijn+goeree+overflakkee&oq=werksessie+erfgoedlijn+goeree&gs_l=psy-ab.1.0.33i160.1910.11578..13804...9.0..1.138.2994.34j6......0....1..gws-wiz.......0i131j0j0i10j0i13j0i131i70i256j0i30j0i5i30.WMmRO51kAPc

De dorpsraad Dirksland heeft o.a. het verslag van de werksessie online gezet.

Groet en ik wacht je verdere berichten af

art 5 1-2e

Van: art 5 1-2e
Verzonden: woensdag 28 augustus 2019 16:16
Aan: art 5 1-2e
CC: art 5 1-2e
Onderwerp: RE: Vragen over melding datalek

Hallo art 5 1-2e

De lijn van beantwoording wordt: het is een datalek, dat niet aan de Autoriteit Persoonsgegevens en ook niet aan de betrokkenen gemeld hoeft te worden.

Dat zal ik onderbouwen in een advies dat ik je vanmiddag of morgenochtend mail.

Jouw antwoorden geven context aan het advies.

Het advies wordt voor akkoord voorgelegd aan de concerndirecteur en TKN aan gedeputeerde voor bedrijfsvoering Baljeu.

Het is ook goed om de inhoudelijk gedeputeerde te informeren; wie is dat?

En wil jij dat zelf doen of wil je dat ik dat op me neem?

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: woensdag 28 augustus 2019 14:19
Aan: art 5 1-2e
CC: art 5 1-2e
Onderwerp: Re: Vragen over melding datalek

Dag art 5 1-2e

Ik ben extern en heb je bericht afgeluisterd. Ik kom er zsm op terug

Groetjes art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Wed, Aug 28, 2019 at 1:45 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Hallo art 5 1-2e

Je hebt een datalek gemeld, waarvan ik de afhandeling verzorg. Ik heb je voicemail ingesproken en ook al met art 5 1-2e gesproken, maar zou graag nog de volgende vragen willen stellen.

In je e-mail nodig je de geadresseerden uit “namens uw voorzitter”.

* Waar is art 5 1-2e voorzitter van en kennen de geadresseerden elkaar?
* Is het in het kader van de communicatie over het betreffende project niet juist wenselijk dat men elkaars bereikbaarheidsgegevens kent? In dat geval zou je in je eerstvolgende e-mail de vraag kunnen stellen of men bezwaar heeft tegen het onderling mailen met kenbare e-mailadressen. Nadeel hiervan is dat je de toestemming (in de vorm van de antwoorden op jouw mail) van de personen moet bewaren, en in de gaten houden dat je niet per ongeluk nieuwe adressen toevoegt zonder dat je daar toestemming voor hebt. Alternatief is om in je eerstvolgende e-mail te vermelden dat je met het oog op de AVG voortaan via de Bcc adresseert.

Ik zou overigens ook de vraag willen stellen welk type emailadressen het hier betreft. Gaat het om privé-emailadressen?. Of zijn het allemaal corporate adressen, zoals bijvoorbeeld @pzh.nl. In dat laatste geval zou nog minder aangenomen kunnen worden dat de persoonlijke levenssfeer van betrokkenen geschaad zou kunnen zijn (hooguit hun zakelijke “levenssfeer”).

art 5 1-2e

Het merendeel van de namen en rollen (niet de e-mailadressen) uit de e-mail staat ook genoemd in een document op internet: Verslag van de werksessie doorontwikkeling kwaliteitsimpuls erfgoedlijn Goeree-Overflakkee

d.d. 30 januari 2019. Voor dat soort publicaties zul je ook de toestemming van de deelnemers moeten hebben. art 5 1-2e kan je hierin adviseren.

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

"Van: art 5 1-2e
Verzonden: 2019-08-29 14:04:21+00:00
"Aan: art 5 1-2e art 5 1-2e
"CC: art 5 1-2e
Onderwerp: Re: Datalek
"
Beste allen,

Ik snap de gedachte. Ik heb deze gisteren ook overwogen. Maar ik denk niet dat we daar sluitend mee uitkomen. Het ging hier om een uitnodiging voor een bijeenkomst, als ik het goed begrepen heb. En zo'n boodschap breng je voor elk van de deelnemers ook heel prima over, wanneer alle genodigden in de BCC staan. Ieder krijgt dan toch hetzelfde bericht. Of anders: voor het goed overbrengen van de boodschap is het niet noodzakelijk dat iedereen ieder anders e-mailadres kan zien.

Dus strikt genomen blijft het volgens mij een inbreuk. Alleen is het de vraag hoe ernstig die is, gezien de contekst van de gezamenlijke deelname aan de erfgoedlijn. Maar om die reden ook geen melding. Toch?

Groeten,

art 5 1-2e

On Thu, Aug 29, 2019 at 12:48 PM +0200, "" art 5 1-2e " <art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Nog even tegen jullie aanhouden.

De Erfgoedlijn is een netwerkorganisatie waarvoor art 5 1-2e een voorzitter heeft benoemd. Het doel van de organisatie is samenwerken en kennisdelen. Het is in dat kader nuttig als de deelnemers elkaars contactgegevens kennen.

Moet de redenering niet zijn dat de netwerkorganisatie de uitvoering van een publieke taak is een provinciale taak (grondslag) betreft en dat de het delen van de contactgegevens (doelbinding) daarbij past?

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 < art 5 1-2e pzh.nl>
Verzonden: woensdag 28 augustus 2019 13:19
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: Datalek

Beste mensen,

Ik kan de weergegeven gedachtenlijn mede onderschrijven.

Ik zou overigens ook de vraag willen stellen welk type emailadressen het hier betreft. Gaat het om privé-emailadressen?. Of zijn het corporate adressen, zoals bijvoorbeeld @pzh.nl. In dat laatste geval zou nog minder aangenomen kunnen worden dat de persoonlijke levenssfeer van betrokkenen geschaad zou kunnen zijn (hooguit hun zakelijke “levenssfeer”).

En het zou ook de vraag zijn of de deelnemers in het kader van de communicatie over het betreffende project niet juist wenselijk zouden vinden dat men elkaar bereikbaarheidsgegevens kent. Ion plaats van in de eerstvolgende e-mail te melden dat de adressen met oog op de AVG voortaan in de Bcc staan, zou daaraan voorafgaand de vraag gesteld kunnen worden of men bezwaarheeft tegen het onderling mailen met kenbare e-mailadressen.

Maar overall eens: datalek ja, maar gelet op aard, omvang en mate waarin persoonlijke levenssferen geschaad zijn geen melding

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: woensdag 28 augustus 2019 12:40
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: Datalek
Urgentie: Hoog

Hallo art 5 1-2e

Bij afwezigheid van art 5 1-2e wil ik je graag betrekken bij de beoordeling van een melding van een datalek.

* De melding vind je in bijlage 1.
* De mail waar het om gaat vind je in bijlage 2.

De procedure (verkort weergegeven in bijlage 3 en onverkort in bijlage 4) is dat we zo snel mogelijk maar uiterlijk 72 uur na aanmelding komen tot een beoordeling en een advies aan de concerndirecteur.

Voor het advies bestaat een template; die vul ik in als we er samen uit zijn.

In dit geval doen we de beoordeling met 3 man: art 5 1-2e jij en ik.

art 5 1-2een ik werken vandaag huis hebben telefonisch al even afgestemd.

Wij kunnen via de mail afstemmen en als dat handig is vanmiddag even bellen.

De lijn van art 5 1-2een mij op dit moment. Graag jouw mening hierover:

1. art 5 1-2eheeft in een e-mail e-mailadressen van relaties opgenomen. Daardoor konden alle ontvangers elkaars e-mailadressen inzien. Omdat betrokkenen hier geen expliciete toestemming voor hebben gegeven en het openbaar maken van de e-mailadressen niet nodig is voor de uitoefening van de betreffende publieke taak (project Erfgoedlijn Goeree-Overflakkee) is er sprake van onrechtmatige verwerking. Dit is een datalek.

* De emailadressen hadden in de Bcc moeten zitten, zodat ontvangers niet elkaars e-mailadressen kunnen zien
* Ik wil van art 5 1-2e nog weten of de deelnemers elkaar en elkaars contactgegevens kennen (want uit de mail blijkt dat bijvoorbeeld er een voorzitter is). Dat verandert misschien de situatie.

2. Moet dit datalek gemeld worden bij de AP? => Nee

o 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.
In dit geval is dat niet het geval. De inhoud van de mail is een uitnodiging voor een bijeenkomst van project Erfgoedlijn Goeree-Overflakkee waar de geadresseerden bij betrokken zijn.

3. Moet dit datalek gemeld worden aan betrokkenen? => Nee

o Heeft het datalek ook waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkenen, dan moeten ook deze personen geïnformeerd worden over het datalek.

o Om bovengenoemde reden is dat hier niet het geval.

o Wel zou art 5 1-2e in de eerstvolgende e-mail kunnen melden dat de adressen met oog op de AVG voortaan in de Bcc staan. Maar dat is iets anders dan op grond van de AVG melding doen van een datalek.

Graag je 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/>

"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-08-30 09:38:08.433000+00:00
Aan: art 5 1-2e art 5 1-2e
"CC: art 5 1-2e
Onderwerp: Re: Datalek
"
Dankjewel. Heldere redenering art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Thu, Aug 29, 2019 at 2:04 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Beste allen,

Ik snap de gedachte. Ik heb deze gisteren ook overwogen. Maar ik denk niet dat we daar sluitend mee uitkomen. Het ging hier om een uitnodiging voor een bijeenkomst, als ik het goed begrepen heb. En zo'n boodschap breng je voor elk van de deelnemers ook heel prima over, wanneer alle genodigden in de BCC staan. Ieder krijgt dan toch hetzelfde bericht. Of anders: voor het goed overbrengen van de boodschap is het niet noodzakelijk dat iedereen ieder anders e-mailadres kan zien.

Dus strikt genomen blijft het volgens mij een inbreuk. Alleen is het de vraag hoe ernstig die is, gezien de contekst van de gezamenlijke deelname aan de erfgoedlijn. Maar om die reden ook geen melding. Toch?

Groeten,

art 5 1-2e

On Thu, Aug 29, 2019 at 12:48 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Nog even tegen jullie aanhouden.

De Erfgoedlijn is een netwerkorganisatie waarvoor art 5 1-2e een voorzitter heeft benoemd. Het doel van de organisatie is samenwerken en kennisdelen. Het is in dat kader nuttig als de deelnemers elkaars contactgegevens kennen.

Moet de redenering niet zijn dat de netwerkorganisatie de uitvoering van een publieke taak is een provinciale taak (grondslag) betreft en dat de het delen van de contactgegevens (doelbinding) daarbij past?

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 < art 5 1-2e pzh.nl>
Verzonden: woensdag 28 augustus 2019 13:19
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: Datalek

Beste mensen,

Ik kan de weergegeven gedachtenlijn mede onderschrijven.

Ik zou overigens ook de vraag willen stellen welk type emailadressen het hier betreft. Gaat het om privé-emailadressen?. Of zijn het corporate adressen, zoals bijvoorbeeld @pzh.nl. In dat laatste geval zou nog minder aangenomen kunnen worden dat de persoonlijke levenssfeer van betrokkenen geschaad zou kunnen zijn (hooguit hun zakelijke “levenssfeer”).

En het zou ook de vraag zijn of de deelnemers in het kader van de communicatie over het betreffende project niet juist wenselijk zouden vinden dat men elkaar bereikbaarheidsgegevens kent. Ion plaats van in de eerstvolgende e-mail te melden dat de adressen met oog op de AVG voortaan in de Bcc staan, zou daaraan voorafgaand de vraag gesteld kunnen worden of men bezwaarheeft tegen het onderling mailen met kenbare e-mailadressen.

Maar overall eens: datalek ja, maar gelet op aard, omvang en mate waarin persoonlijke levenssferen geschaad zijn geen melding

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: woensdag 28 augustus 2019 12:40
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 < art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: RE: Datalek
Urgentie: Hoog

Hallo art 5 1-2e

Bij afwezigheid van art 5 1-2e wil ik je graag betrekken bij de beoordeling van een melding van een datalek.

* De melding vind je in bijlage 1.
* De mail waar het om gaat vind je in bijlage 2.

De procedure (verkort weergegeven in bijlage 3 en onverkort in bijlage 4) is dat we zo snel mogelijk maar uiterlijk 72 uur na aanmelding komen tot een beoordeling en een advies aan de concerndirecteur.

Voor het advies bestaat een template; die vul ik in als we er samen uit zijn.

In dit geval doen we de beoordeling met 3 man: art 5 1-2e jij en ik.

art 5 1-2een ik werken vandaag huis hebben telefonisch al even afgestemd.

Wij kunnen via de mail afstemmen en als dat handig is vanmiddag even bellen.

De lijn van art 5 1-2een mij op dit moment. Graag jouw mening hierover:

1. art 5 1-2eheeft in een e-mail e-mailadressen van relaties opgenomen. Daardoor konden alle ontvangers elkaars e-mailadressen inzien. Omdat betrokkenen hier geen expliciete toestemming voor hebben gegeven en het openbaar maken van de e-mailadressen niet nodig is voor de uitoefening van de betreffende publieke taak (project Erfgoedlijn Goeree-Overflakkee) is er sprake van onrechtmatige verwerking. Dit is een datalek.

* De emailadressen hadden in de Bcc moeten zitten, zodat ontvangers niet elkaars e-mailadressen kunnen zien
* Ik wil van art 5 1-2e nog weten of de deelnemers elkaar en elkaars contactgegevens kennen (want uit de mail blijkt dat bijvoorbeeld er een voorzitter is). Dat verandert misschien de situatie.

2. Moet dit datalek gemeld worden bij de AP? => Nee

o 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.
In dit geval is dat niet het geval. De inhoud van de mail is een uitnodiging voor een bijeenkomst van project Erfgoedlijn Goeree-Overflakkee waar de geadresseerden bij betrokken zijn.

3. Moet dit datalek gemeld worden aan betrokkenen? => Nee

o Heeft het datalek ook waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkenen, dan moeten ook deze personen geïnformeerd worden over het datalek.

o Om bovengenoemde reden is dat hier niet het geval.

o Wel zou art 5 1-2e in de eerstvolgende e-mail kunnen melden dat de adressen met oog op de AVG voortaan in de Bcc staan. Maar dat is iets anders dan op grond van de AVG melding doen van een datalek.

Graag je 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/>

"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-08-30 15:08:59.962000+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 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: Secretariaat VEERO [mailto art 5 1-2e
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 beste 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: 2019-08-30 15:38:25+00:00
"Aan: 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
"
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 (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: Secretariaat VEERO [mailto art 5 1-2e
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 beste 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: 2019-08-30 16:36:10+00:00
"Aan: art 5 1-2e
"CC: Baljeu, J.N."
Onderwerp: Re: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Hoi art 5 1-2e

Dankjewel. Ik volg je advies.

Hartelijke groet, art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Fri, Aug 30, 2019 at 3:08 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

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

"Van: art 5 1-2e
Verzonden: 2019-09-03 11:53:08.223000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Hallo art 5 1-2e

Graag gedaan.

Ik zou het advies ook TKN aan jouw gedeputeerde sturen, maar wie is dat ook alweer?

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 < art 5 1-2e pzh.nl>
Verzonden: dinsdag 3 sep :18
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: RE: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Dag art 5 1-2e

Ik ga art 5 1-2e benaderen. Nogmaals dank voor alle inzet en ja, VEERO een beetje flauw hé.

Groet

art 5 1-2e

Van: art 5 1-2e
Verzonden: maandag 2 september 2019 16:29
Aan: art 5 1-2e
Onderwerp: RE: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Hallo art 5 1-2e

art 5 1-2e heeft aangegeven het advies te volgen.

Wat mij betreft kun je VEERO mailen; wellicht dat art 5 1-2e je daarin nog kan

adviseren als je dat wilt.

art 5 1-2e

Wat mij opviel is dat er in het e-mailadres van VEERO geen persoonsgegevens staan

Wel apart dat daar de vraag vandaan komt.

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 < art 5 1-2e)pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: maandag 2 september 2019 11:28
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: FW: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Goedemorgen art 5 1-2e

Ik wil de email van de VEERO beantwoorden over het advies. Kan ik dat al op dit moment? Of wil je dat liever zelf doen?

Groet

art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 30 augustus 2019 19:08
Aan: art 5 1-2e art 5 1-2e art 5 1-2e
CC: art 5 1-2e art 5 1-2e pzh.nl zh.nl>) ; 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 van art 5 1-2e stuur ik je advies bijgaand toe. Wellicht kan je d 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 <mailto : 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 <mailto : art 5 1-2e pzh.nl> >
CC: Baljeu, J.N. <j.baljeu@pzh.nl <mailto: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


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-09-03 12:00:45.589000+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e art 5 1-2e
Onderwerp: TKN: afgehandeld datalek Erfgoedtafel Goeree-Overflakkee
"
Beste Buiten reikwijdte Woo-verzoek

Bijgaand ter kennisname het door art 5 1-2e overgenomen advies over een opgetreden datalek bij de Erfgoedtafel Goeree-Overflakkee.

Voor nadere toelichting ben ik uiteraard beschikbaar.

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 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: Secretariaat VEERO [mailto art 5 1-2e
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 beste 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: 2019-09-13 13:10:57.768000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Datalek?
"
ok

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 < art 5 1-2e pzh.nl>
Verzonden: vrijdag 13 september 2019 13:11
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>
CC: privacy <privacy@pzh.nl>
Onderwerp: Re: Datalek?
Gevoeligheid: Vertrouwelijk

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

Ik bel je om 15.00 uur.

Groet art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Fri, Sep 13, 2019 at 1:07 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> > wrote:

> Hallo allen,
>
> Gevoelige kwestie. Graag jullie reactie.
>
> Ben thuis aan het werk, maar we kunnen bellen.

De Statengriffie gebruikt voor het aanmelden van Statenleden een workflow in Topdesk.

Op basis van de workflow (Topdesk term voor worklow is wijziging) worden onderstaande activiteiten uitgevoerd.

Beoogd resultaat van de complete wijziging:

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

Het vermoeden bestaat dat de collega’s van P&O, I&A en FZ die de bovenstaande activiteiten uitvoeren, toegang hebben tot alle aanvraaggegevens.

De gegevens die bij de aanvraag zitten zijn gevoelig en bijzonder:

* Kopie paspoort
* Verklaring loonheffing
* Opgave loonheffing
* Naam
  Voorletters
  Geboortedatum
  Burgelijke staat
  Adres
  Postcode
  Woonplaats
  BurgerServiceNummer (BSN)
  IBANnummer

1. De I&A collega die het telefoonnummer aanmaakt heeft gemeld dat hij die gegevens niet nodig heeft voor de uitvoering van zijn taak.
2. De toegangsrechten staan te ruim: de gegevens zijn namelijk ook in te zien door Topdesk behandelaars die deze taken niet uitvoeren. Zoals ik; als ik gericht doorklik.
   Gewone gebruikers kunnen er niet bij.

* Ik wil weten hoe de rechten exact staan en ik wil zorgen dat de rechten direct worden gecorrigeerd.
  Helaas kan ik de beheerder van Topdesk niet bereiken. Ben op zoek naar een vervanger.
* Hoe gaan we met deze situatie om?

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

"Van: art 5 1-2e
Verzonden: 2019-09-13 14:41:47.721000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Datalek?
"
Vrijdagmiddag hè

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 art 5 1-2e pzh.nl>
Verzonden: vrijdag 13 september 2019 14:40
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>
CC: privacy <privacy@pzh.nl>
Onderwerp: Re: Datalek?
Gevoeligheid: Vertrouwelijk

Ben nog met een ander spoedje bezig. Meld me straks.

On Fri, Sep 13, 2019 at 1:10 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

> Hoi art 5 1-2e art 5 1-2e
>
> Ik bel je om 15.00 uur.
>
> Groet art 5 1-2e
>
> Outlook voor Android downloaden <https://aka.ms/ghei36>

> On Fri, Sep 13, 2019 at 1:07 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl

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

Hallo allen,

Gevoelige kwestie. Graag jullie reactie.

Ben thuis aan het werk, maar we kunnen bellen.

De Statengriffie gebruikt voor het aanmelden van Statenleden een workflow in Topdesk.

Op basis van de workflow (Topdesk term voor worklow is wijziging) worden onderstaande activiteiten uitgevoerd.

Beoogd resultaat van de complete wijziging:

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

Het vermoeden bestaat dat de collega’s van P&O, I&A en FZ die de bovenstaande activiteiten uitvoeren, toegang hebben tot alle aanvraaggegevens.

De gegevens die bij de aanvraag zitten zijn gevoelig en bijzonder:

* Kopie paspoort
* Verklaring loonheffing
* Opgave loonheffing
* Naam
  Voorletters
  Geboortedatum
  Burgelijke staat
  Adres
  Postcode
  Woonplaats
  BurgerServiceNummer (BSN)
  IBANnummer

1. De I&A collega die het telefoonnummer aanmaakt heeft gemeld dat hij die gegevens niet nodig heeft voor de uitvoering van zijn taak.
2. De toegangsrechten staan te ruim: de gegevens zijn namelijk ook in te zien door Topdesk behandelaars die deze taken niet uitvoeren. Zoals ik; als ik gericht doorklik.
   Gewone gebruikers kunnen er niet bij.

* Ik wil weten hoe de rechten exact staan en ik wil zorgen dat de rechten direct worden gecorrigeerd.
Helaas kan ik de beheerder van Topdesk niet bereiken. Ben op zoek naar een vervanger.
* Hoe gaan we met deze situatie om?

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

"Van: art 5 1-2e
Verzonden: 2019-09-16 07:32:11.841000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Datalek?
"
Nee, ik wil eerst overleggen met het team.

Heb een afspraak ingeschoten voor vanmiddag,

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 < art 5 1-2e pzh.nl>
Verzonden: zondag 15 september 2019 21:14
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Re: Datalek?
Gevoeligheid: Vertrouwelijk

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

Heb je een voorlopige melding aan de AP gedaan?

Groet art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Fri, Sep 13, 2019 at 1:07 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> > wrote:

> Hallo allen,
>
> Gevoelige kwestie. Graag jullie reactie.
>
> Ben thuis aan het werk, maar we kunnen bellen.

De Statengriffie gebruikt voor het aanmelden van Statenleden een workflow in Topdesk.

Op basis van de workflow (Topdesk term voor worklow is wijziging) worden onderstaande activiteiten uitgevoerd.

Beoogd resultaat van de complete wijziging:

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

Het vermoeden bestaat dat de collega’s van P&O, I&A en FZ die de bovenstaande activiteiten uitvoeren, toegang hebben tot alle aanvraaggegevens.

De gegevens die bij de aanvraag zitten zijn gevoelig en bijzonder:

* Kopie paspoort
* Verklaring loonheffing
* Opgave loonheffing
* Naam
  Voorletters
  Geboortedatum
  Burgelijke staat
  Adres
  Postcode
  Woonplaats
  BurgerServiceNummer (BSN)
  IBANnummer

1. De I&A collega die het telefoonnummer aanmaakt heeft gemeld dat hij die gegevens niet nodig heeft voor de uitvoering van zijn taak.
2. De toegangsrechten staan te ruim: de gegevens zijn namelijk ook in te zien door Topdesk behandelaars die deze taken niet uitvoeren. Zoals ik; als ik gericht doorklik.
   Gewone gebruikers kunnen er niet bij.

* Ik wil weten hoe de rechten exact staan en ik wil zorgen dat de rechten direct worden gecorrigeerd.
  Helaas kan ik de beheerder van Topdesk niet bereiken. Ben op zoek naar een vervanger.
* Hoe gaan we met deze situatie om?

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

"Van: art 5 1-2e
Verzonden: 2019-09-16 07:56:33.935000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Topdesk
"
Hallo art 5 1-2e

De aanmeldingen zijn onzichtbaar gemaakt en we zijn bezig met de verdere afhandeling.

Voor de volledigheid van de administratie is het belangrijk dat je melding via het Loket is geregistreerd.

Zou je dit alsnog willen doen?

http://binnenplein.pzh.nl/loket/@12957/datalek/

Vast bedankt.

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 < art 5 1-2e pzh.nl>
Verzonden: donderdag 12 september 2019 09:02
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
CC: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: FW: Topdesk

Hallo art 5 1-2e

Ik heb onderstaande naar art 5 1-2e verzonden maar ik denk dat het jou verantwoordelijkheid is. Dit is namelijk een datalek en moet denk ik snel aangepakt worden.

Met vriendelijke groeten,

art 5 1-2e

Specialist Netwerk en Telecom

Afdeling I&A | bureau Infra & Support

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

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: woensdag 11 september 2019 12:26
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: Topdesk

Hoi art 5 1-2e

Kan jij in Topdesk zoeken op wijzigingsactiviteit met de nummers:

57943

57947

58030

58034

58038

58042

Je moet het filter op Alle zetten. Wanneer je bij deze wijzigingsactiviteiten kan dan kan je ook de gegevens van de pasporten van de Statenleden bekijken.

Met vriendelijke groeten,

art 5 1-2e

Specialist Netwerk en Telecom

Afdeling I&A | bureau Infra & Support

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

art 5 1-2e pzh.nl <mailt o 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> .
"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-09-17 09:18:42.933000+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e
Onderwerp: Advies datalek
"
Beste art 5 1-2e

Het Privacyteam heeft zojuist advies uitgebracht aan art 5 1-2e

Het advies luidt:

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.

We willen de communicatie naar betrokkenen samen met de Griffie en de afdeling Communicatie vormgeven.

Wie kan ik vanuit de Griffie betrekken?

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

"Van: art 5 1-2e
Verzonden: 2019-09-18 14:09:15.866000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Advies DL
"
Hallo art 5 1-2e

Zoals besproken.

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 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.

"Van: art 5 1-2e
Verzonden: 2019-09-18 17:07:59.318000+00:00
"Aan: art 5 1-2e Zoete - van der Hout, WH, de"
CC:
Onderwerp: Melding AP
"
Beste art 5 1-2e en mevrouw De Zoete,

Vanmiddag heb ik melding van het datalek bij de Autoriteit Persoonsgegevens gedaan.

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

Tijdstip ontvangst	18-09-2019 15:07:58
Uniek nummer	art 5 1-2e

"Van: art 5 1-2e
Verzonden: 2019-09-18 17:15:20.939000+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: RE: privacy team vrijdagochtend op de kamer van art 5 1-2e
"
Update:

art 5 1-2e heeft vanmiddag besloten het advies te volgen: 2x melden

art 5 1-2e en ik hebben inmiddels de melding bij de AP gedaan.

Willy de Zoete heeft vandaag in de GS vergadering onderstaande gemeld.

Rondvraag

Gedeputeerde De Zoete meldt een datalek. Maatregelen zijn genomen, Autoriteit Persoonsgegevens wordt geinformeerd en betrokkenen ook. Overleg met de griffie is nodig om te bezien hoe PS wordt geinformeerd.

Afd Communicatie is bezig met een brief.

Ik heb met mijn afdelingshoofd besproken (en telefonisch ingesproken bij art 5 1-2e dat de het zuiverder is als verantwoordelijkheid voor de verdere afhandeling bij afdelingshoofd P&O ligt.

Het gaat dan om brief, informeren PS, woordvoeringslijn bepalen, persvoorlichting, contactpersoon regelen voor vragen, afwegingen over welke vragen van de statenleden wel en niet beantwoord gaan worden vanwege scheiding ambtenarij-politiek, etc.

Ik wil graag helpen etc maar vanuit mijn rol niet de verantwoordelijkheid nemen.

Denk dat we daar in de procedurebeschrijving ook meer helderheid in moeten scheppen.

Afdelingshoofd en art 5 1-2e zien elkaar vanavond, dus dan wordt dat hopelijk kortgesloten.

Afdelingshoofd zal ook Afrodite hierover benaderen.

Fijne avond.

Groet, art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: woensdag 18 september 2019 15:52
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: privacy team vrijdagochtend op de kamer van art 5 1-2e

Dag allen,

We kunnen vrijdagochtend weer gebruik maken van de kamer van art 5 1-2e

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

"Van: art 5 1-2e
Verzonden: 2019-09-18 17:17:12.087000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Bevestiging
"
Hallo art 5 1-2e

Zou jij voor in het dossier je besluit nog even willen bevestigen door bijgevoegde mail te beantwoorden?

Vast bedankt!

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

"Van: art 5 1-2e
Verzonden: 2019-09-17 14:28:34.903000+00:00
"Aan: art 5 1-2e Zoete - van der Hout, WH, de"
CC:
Onderwerp: Advies in het kader van de meldplicht datalekken
"

Beste art 5 1-2e mevrouw de Zoete,

Hierbij het advies van het privacyteam over het eerder aangekondigde onderwerp.

art 5 1-2e wil jij hier als gemandateerd concerndirecteur een besluit op nemen?

Mevrouw De Zoete, conform de procedure wordt u geïnformeerd wanneer er een onderzoek start, wanneer er advies is uitgebracht en ook over eventuele vervolgacties die volgen op het besluit.

Voor de volledigheid heb ik de procedure als bijlage 2 bijgevoegd.

Mochten er vragen zijn over de inhoud of de procedure, dan ben ik uiteraard graag bereid een toelichting te geven.

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: maandag 16 september 2019 08:30
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
CC: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl <mailto:wh.de.zoete@pzh.nl>
>
Onderwerp: Vermoeden datalek
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste art 5 1-2e mevrouw De Zoete,

Het privacyteam - inclusief FG art 5 1-2e - onderzoekt op dit moment een situatie die we als datalek in de zin van de Algemene verordening gegevensbescherming beschouwen.

Zoals altijd stuur ik z.s.m. het analyse- en adviesrapport voor besluit aan de concerndirecteur en ter kennisname aan de gedeputeerde.

Situatie

Het betreft het systeem (Topdesk) waarin de Griffie nieuwe statenleden aanmeldt en er vervolgens in diverse ondersteunende afdelingen (P&O, I&A, FZ) taken worden uitgevoerd:

• toegangspas aanmaken

• account aanmaken

• aanmaken telefoonnummer

• OV-abonnement aanmaken

• Gegevens invoeren in Workforce - P&O Salarisadministratie

Het betreft gegevens als:

* kopie paspoort/identeitsbewijs,
* inlichtingenformulier met en zonder BSN-nummer
* loonbelasting verklaring
* verklaring opting-in

Voor de uitvoering hiervan is personeel uit de genoemde afdelingen geautoriseerd.

Niet voor alle taken is het nodig dat geautoriseerd personeel alle gegevens over de statenleden kan inzien.

Geconstateerd is dat dit door een tekortkoming in de software via een omweg in het systeem wel zou kunnen. Een alerte medewerker heeft ons hierop attent gemaakt.

In overleg met de beheerder van het systeem zijn de gegevens alsnog ontoegankelijk gemaakt.

Er is geen aanleiding om te vermoeden dat dit breder het geval is.

In de zin van de AVG wordt een dergelijke situatie wel als datalek gekenmerkt.

Vervolgacties

Vooralsnog beschouwen we dit dan ook als een (inmiddels gedicht) datalek.
De uitkomst van de analyse bepaalt onze verdere acties richting Autoriteit Persoonsgegevens en betrokkenen.

Ik houd jullie op de hoogte.

Voor vragen en nadere toelichting ben ik – of de FG - uiteraard beschikbaar.

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 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.

provincie ZUID HOLLAND

Procedure voor het afhandelen van datalekken

Provincie Zuid-Holland

Mei 2018
Provincie Zuid-Holland
Versie: 1.1

overzicht besluitvorming / bespreking

Documenthistorie

Versie	Datum	Wie	Wijziging
1.0	7 februari 2016	art 5 1-2e	Eerste procedure
1.1	9 mei 2018	art 5 1-2e	Geactualiseerd n.a.v. de AVG

Vastgesteld door concerndirecteur art 5 1-2e op 11 mei 2018.

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Vanaf 1 januari 2016 is de meldplicht Datalekken van kracht. Dit houdt in dat de provincie verplicht is om (potentiële) datalekken te melden aan de landelijke toezichthouder, de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene van wie de gegevens zijn gelekt. Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) formeel van kracht die de huidige Wet bescherming persoonsgegevens (Wbp) vervangt. Ook onder de AVG geldt de meldplicht datalekken.

Er is echter wel een aantal veranderingen ten opzichte van de Wbp, die tot een lichte wijziging in de huidige procedure leidt. Zoals de aanwezigheid in de provincie van een functionaris voor de gegevensbescherming en licht aangepaste terminologie.

1.2 Persoonsgegevens

Een persoonsgegeven is volgens de AVG alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”). Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Er kan een onderscheid worden gemaakt in direct en indirect identificerende gegevens.

Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum.
Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.

Voorbeelden:

- Wanneer bijvoorbeeld een telefoonnummer (indirect identificerend) via een telefoonboek gekoppeld kan worden aan een naam (direct identificerend), dan is het telefoonnummer een persoonsgegeven. Bij de beoordeling of gegevens gekoppeld kunnen worden gaat het niet alleen om de gegevens die de verwerkingsverantwoordelijke in zijn bezit heeft. Ook gegevens die bijvoorbeeld via internet openbaar toegankelijk zijn kunnen worden meegewogen in de beslissing of iemand identificeerbaar is.
- Als door een combinatie van gegevens een dusdanig uniek beeld ontstaat dat de gegevens maar op één persoon betrekking kunnen hebben. Een voorbeeld van een dergelijke spontane identificatie is: ‘een 39-jarige mannelijke jurist woonachtig aan de Oxfordlaan te Leiden’. Het is zeer onwaarschijnlijk dat deze combinatie op meer dan één geïdentificeerde persoon betrekking heeft.

1.3 Datalek

In tegenstelling tot de Wbp, komt in de AVG het letterlijke woord datalek niet voor, maar wordt gesproken over “inbreuk in verband met persoonsgegevens”. Omdat de term datalek echter inmiddels ingeburgerd is, blijven wij (net als de Autoriteit Persoonsgegevens) deze term hanteren.

Bij een datalek is sprake van een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die eventueel zijn getroffen waren niet toereikend om dit te voorkomen.

Voorbeelden van een datalek zijn het verlies van een papieren document of mobiel apparaat waarop gevoelige persoonsgegevens staan. Maar ook computer hacking, besmetting met ransomware, of het technische falen van apparatuur, stroomuitval, wateroverlast kunnen leiden tot een datalek.

1.4 Inhoud meldplicht

De melding moet zo mogelijk gebeuren binnen 72 uur, zonder onderscheid tussen werkdagen, weekenden of feestdagen. Als het incident later dan 72 uur na ontdekking aan de Autoriteit Persoonsgegevens wordt gemeld, dan moet dit worden gemotiveerd. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. De Autoriteit Persoonsgegevens slaat de melding op in een register met alle ontvangen meldingen over datalekken. Dit register is niet openbaar.

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.

1.5 Doel en reikwijdte van deze procedure

Deze procedure beschrijft de wijze waarop binnen de provincie Zuid-Holland wordt omgegaan met de meldplicht datalekken in de zin van de Algemene Verordening Gegevensbescherming (AVG). De procedure is gericht op het beperken van de schade, analyseren van de (ernst van) de situatie en het opstellen van een onderbouwd advies aan de eindverantwoordelijke functionaris binnen de provincie. Dit is de concerndirecteur die gemandateerd is te besluiten om al dan niet melding te doen bij de Autoriteit Persoonsgegevens en betrokkenen (wiens persoonsgegevens het betreft).

De procedure wordt onder coördinatie van de afdeling I&A uitgevoerd, in nauwe samenwerking met de informatiebeheerder van P&O, de privacy jurist van FJZ, de I&A incident manager, een medewerker documentaire informatie van I&A, de functioneel/technisch beheerder van het systeem, betrokken medewerker(s) en diens leidinggevende. Per potentieel datalek wordt op die manier een datalekteam geformeerd.

De functionaris gegevensbescherming (FG) wordt geïnformeerd over het optreden van het potentiële datalek en de afhandeling ervan. De FG kan tijdens de afhandeling gevraagd en ongevraagd adviseren en beoordeelt de correcte uitvoering van de procedure. De FG kan hiertoe per afzonderlijk geval besluiten deel te nemen aan het datalekteam.

Hieronder volgt een nadere uitwerking van deze procedure.

2 Procedurebeschrijving

2.1 Melden incident

2.1.1 Interne medewerkers

De meldplicht datalekken geldt voor de gehele organisatie en iedere medewerker. Iedere medewerker die te maken heeft met vermissing/diefstal van zaken die van de provincie zijn, of met een informatiebeveiligingsincident, dient dit te melden bij het ICT-plein. Dit kan telefonisch via toestelnummer (070) 441 77 77 of via het meldingsformulier in het Loket op Topdesk.
Naam en contactgegevens van de melder worden automatisch in het formulier geregistreerd met de informatie over het incident. De melder kan namelijk gevraagd worden om aanvullende informatie te geven over het incident. Dit is belangrijk voor de goede en snelle afhandeling van het incident en de volledigheid voor een eventuele melding aan de AP.

2.1.2 Verwerkers van persoonsgegevens namens de provincie

Als er externe partijen zijn die in opdracht van de provincie persoonsgegevens verwerken, dan is met deze partijen een verwerkersovereenkomst gesloten, waarin is opgenomen hoe het onderlinge contact verloopt bij mogelijke datalekken. Het betreft dan vaak beveiligingsincidenten met applicaties die in het datacenter van de leverancier draaien.

2.1.3 Derden

Ook burgers of bedrijven kunnen melding doen van een mogelijk datalek bij de provincie. Op verschillende manieren kan zo'n melding de provincie bereiken. Men kan zich via de contactgegevens op de provinciale website wenden tot het Klantcontactcentrum of de provinciale functionaris gegevensbescherming. Ook is het mogelijk dat een burger of bedrijf zich eerst wendt tot de Autoriteit Persoonsgegevens. In dat geval zal de autoriteit contact opnemen met de provinciale functionaris gegevensbescherming.

De FG zal de melding registreren via het meldingsformulier in het Loket op Topdesk.

2.2 Beoordeling of er sprake is van een datalek

2.2.1 Eerste beoordeling

Zo snel mogelijk na de melding van een incident doet de adviseur informatieveiligheid (I&A) een eerste beoordeling of er sprake kan zijn van een datalek dat valt onder de meldplicht van de AVG. Als dit niet kan worden uitgesloten, formeert de adviseur informatieveiligheid het Datalekteam.

2.2.2 Formeren Datalek team

Het Datalekteam bestaat naast de adviseur informatieveiligheid, en afhankelijk van de situatie, uit: de informatiebeheerder van P&O, de privacy jurist van FJZ, de I&A incident manager, een medewerker documentaire informatie van I&A, de functioneel/technisch beheerder van het systeem, betrokken medewerker(s) en diens leidinggevende. Afhankelijk

van de beoordeling van situatie wordt de afdeling Communicatie betrokken in verband met persvoorlichting, interne en/of externe communicatie.

De adviseur informatieveiligheid informeert zo snel mogelijk telefonisch de FG.

2.2.3 Doelen en taken datalekteam

Het Datalekteam heeft als doelstelling:

- Maatregelen (laten) treffen ter beperken van verdere schade;
- Onderzoek te (laten) doen naar de oorzaak van het datalek;
- Gevolgen daarvan voor zowel de provincie Zuid-Holland als de bij het datalek betrokken personen vast te (laten) stellen;
- Acties vast te (laten) stellen voor afhandeling van het datalek en
- Uitgevoerde acties te (laten) controleren

De taken van het Datalekteam zijn:

- Vaststellen van noodzakelijke (directe) acties om de gevolgen van het datalek te beperken en in de toekomst vergelijkbare datalekken te voorkomen;
- Medewerkers van de provincie Zuid-Holland aan te sturen in de uitvoering van de noodzakelijke acties;
- Informeren van directie en bestuur;
- Zorg dragen voor besluitvorming ten aanzien van het datalek;
- (Indien noodzakelijk) interne communicatie rondom het datalek te (laten) verzorgen;
- Vaststellen van de wijze van informeren van betrokkenen (personen waarvan de gegevens bij het incident 'gelekt' zijn).

2.2.4 Beoordelen

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.

2.2.5 Advies

De FG gehoord hebbende stelt het datalekteam een advies op voor de concerndirecteur, belast met de bedrijfsvoering.
De concerndirecteur beoordeelt het incident en het bijgevoegde advies en besluit of er sprake is van een datalek dat gemeld moet worden aan de toezichthouder en eventueel de betrokkene(n).
Een afschrift van het advies wordt aan de FG toegezonden.
De gedeputeerde Middelen wordt geïnformeerd.

2.2.6 Melden

De adviseur informatieveiligheid is er verantwoordelijk voor dat het meldingsformulier van de toezichthouder wordt ingevuld en vervolgens wordt toegestuurd naar de toezichthouder.

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.

2.2.7 Administreren

De adviseur informatieveiligheid houdt een administratie bij waarin alle datalekken die zich voordoen in de organisatie geregistreerd worden. Dit betekent dat ook wanneer een lek niet gemeld hoeft te worden, er een documentatieplicht geldt.
De administratie bevat de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.

In het logboek worden in ieder geval de volgende gegevens vermeld:

a) het onderwerp van het datalek.
b) de datum van het datalek;
c) de duur van het datalek;
d) de aard van de inbreuk;
e) de instanties waar meer informatie over de inbreuk kan worden verkregen;
f) de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk gevolgen te beperken.
g) een beschrijving van de gevolgen voor de verwerkte persoonsgegevens;
h) de maatregelen die de provincie heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen;
i) de kennisgeving aan betrokkenen.

"Van: art 5 1-2e
Verzonden: 2019-09-18 22:33:45+00:00
"Aan: art 5 1-2e Zoete - van der Hout, WH, de"
CC:
Onderwerp: RE: Advies in het kader van de meldplicht datalekken
"
Ha art 5 1-2e

Na consultatie van gedeputeerde De Zoete en haar melding in GS, besluit ik conform je advies. Dankjewel!

Zoals al mondeling met je gedeeld, ontvang ik graag op korte termijn een overzicht van de communicatieve aanpak, ik heb de gedeputeerde toegezegd dat, gezien de gevoeligheid, eerst het haar te delen voordat dit tot uitvoering wordt gebracht.

Hartelijke groet, art 5 1-2e

Van: art 5 1-2e
Verzonden: dinsdag 17 september 2019 14:29
Aan: art 5 1-2e Zoete - van der Hout, WH, de
Onderwerp: Advies in het kader van de meldplicht datalekken
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste art 5 1-2e en mevrouw de Zoete,

Hierbij het advies van het privacyteam over het eerder aangekondigde onderwerp.

art 5 1-2e wil jij hier als gemandateerd concerndirecteur een besluit op nemen?

Mevrouw De Zoete, conform de procedure wordt u geïnformeerd wanneer er een onderzoek start, wanneer er advies is uitgebracht en ook over eventuele vervolgacties die volgen op het besluit.

Voor de volledigheid heb ik de procedure als bijlage 2 bijgevoegd.

Mochten er vragen zijn over de inhoud of de procedure, dan ben ik uiteraard graag bereid een toelichting te geven.

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: maandag 16 september 2019 08:30
Aan: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
CC: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl <mailto:wh.de.zoete@pzh.nl>
>
Onderwerp: Vermoeden datalek
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste art 5 1-2e en mevrouw De Zoete,

Het privacyteam - inclusief FG art 5 1-2e - onderzoekt op dit moment een situatie die we als datalek in de zin van de Algemene verordening gegevensbescherming beschouwen.

Zoals altijd stuur ik z.s.m. het analyse- en adviesrapport voor besluit aan de concerndirecteur en ter kennisname aan de gedeputeerde.

Situatie

Het betreft het systeem (Topdesk) waarin de Griffie nieuwe statenleden aanmeldt en er vervolgens in diverse ondersteunende afdelingen (P&O, I&A, FZ) taken worden uitgevoerd:

• toegangspas aanmaken

• account aanmaken

• aanmaken telefoonnummer

• OV-abonnement aanmaken

• Gegevens invoeren in Workforce - P&O Salarisadministratie

Het betreft gegevens als:

* kopie paspoort/identeitsbewijs,
* inlichtingenformulier met en zonder BSN-nummer
* loonbelasting verklaring
* verklaring opting-in

Voor de uitvoering hiervan is personeel uit de genoemde afdelingen geautoriseerd.

Niet voor alle taken is het nodig dat geautoriseerd personeel alle gegevens over de statenleden kan inzien.

Geconstateerd is dat dit door een tekortkoming in de software via een omweg in het systeem wel zou kunnen. Een alerte medewerker heeft ons hierop attent gemaakt.

In overleg met de beheerder van het systeem zijn de gegevens alsnog ontoegankelijk gemaakt.

Er is geen aanleiding om te vermoeden dat dit breder het geval is.

In de zin van de AVG wordt een dergelijke situatie wel als datalek gekenmerkt.

Vervolgacties

Vooralsnog beschouwen we dit dan ook als een (inmiddels gedicht) datalek.
De uitkomst van de analyse bepaalt onze verdere acties richting Autoriteit Persoonsgegevens en betrokkenen.

Ik houd jullie op de hoogte.

Voor vragen en nadere toelichting ben ik – of de FG - uiteraard beschikbaar.

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

"Van: art 5 1-2e
Verzonden: 2019-09-19 08:57:35.297000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Ter info
"
Ben je ook op de hoogte

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 < art 5 1-2e pzh.nl>
Verzonden: donderdag 19 september 2019 08:35
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>; art 5 1-2e
< art 5 1-2e pzh.nl>
Onderwerp: FW: privacy team vrijdagochtend op de kamer van art 5 1-2e

Beste art 5 1-2e

Ik ben niet bereid hier zomaar de verantwoordelijkheid voor te nemen. Volgens mij komt het lek door outlook en niet door P&O.

Het lijkt mij goed dat betrokkenen geinformeerd worden vanuit een neutraal punt, bv de informatiebeveiligingsfunctionaris.

En denken jullie daar anders over, dan is het tijd voor een goed gesprek daarover.

Gr

art 5 1-2e

Van: art 5 1-2e
Verzonden: donderdag 19 september 2019 08:30
Aan: art 5 1-2e
Onderwerp: FW: privacy team vrijdagochtend op de kamer van art 5 1-2e

Bij deze

Van: art 5 1-2e
Verzonden: woensdag 18 september 2019 17:15
Aan: art 5 1-2e art 5 1-2e art 5 1-2e

Onderwerp: RE: privacy team vrijdagochtend op de kamer van art 5 1-2e

Update:

art 5 1-2e heeft vanmiddag besloten het advies te volgen: 2x melden

art 5 1-2e en ik hebben inmiddels de melding bij de AP gedaan.

Willy de Zoete heeft vandaag in de GS vergadering onderstaande gemeld.

Rondvraag

Gedeputeerde De Zoete meldt een datalek. Maatregelen zijn genomen, Autoriteit Persoonsgegevens wordt geinformeerd en betrokkenen ook. Overleg met de griffie is nodig om te bezien hoe PS wordt geinformeerd.

Afd Communicatie is bezig met een brief.

Ik heb met mijn afdelingshoofd besproken (en telefonisch ingesproken bij art 5 1-2e dat de het zuiverder is als verantwoordelijkheid voor de verdere afhandeling bij afdelingshoofd P&O ligt.

Het gaat dan om brief, informeren PS, woordvoeringslijn bepalen, persvoorlichting, contactpersoon regelen voor vragen, afwegingen over welke vragen van de statenleden wel en niet beantwoord gaan worden vanwege scheiding ambtenarij-politiek, etc.

Ik wil graag helpen etc maar vanuit mijn rol niet de verantwoordelijkheid nemen.

Denk dat we daar in de procedurebeschrijving ook meer helderheid in moeten scheppen.

Afdelingshoofd en art 5 1-2e zien elkaar vanavond, dus dan wordt dat hopelijk kortgesloten.

Afdelingshoofd zal ook art 5 1-2e hierover benaderen.

Fijne avond.

Groet, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: woensdag 18 september 2019 15:52
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: privacy team vrijdagochtend op de kamer van art 5 1-2e

Dag allen,

We kunnen vrijdagochtend weer gebruik maken van de kamer van art 5 1-2e

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

Geachte heer/mevrouw, [personaliseren]

Onlangs 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.

Aanleiding
Sinds vorig jaar mei is de Algemene Verordening Gegevensbescherming (AVG) van kracht. Deze verordening voorziet in een versterking van de privacyrechten en bescherming van ~~data~~persoonsgegevens. We hebben naar aanleiding van deze verordening onder meer een functionaris voor gegevensbescherming aangesteld en het toezicht op de verwerking van ~~(~~persoons~~)~~gegevens verder aangescherpt. Doordat wij onze bestaande werkwijzen en processen nu meer dan vroeger kritisch tegen het licht houden komen zwakke plekken sneller in beeld – ook voordat er daadwerkelijk misbruik gemaakt wordt van de gegevens - en kunnen we snel en direct 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 datalek
Voor het aanmelden van nieuwe statenleden en fractiemedewerkers maakt de provincie gebruik van een IT-systeem. ~~Hierbij~~ 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.

Afhandeling/maatregelen
Na constatering is het lek direct gedicht. Uw persoonsgegevens zijn uit het systeem verwijderd en de werkwijze is aangepast, zodat dit niet opnieuw kan gebeuren. De functionaris voor gegevensbescherming en de concerndirectie zijn op de hoogte gesteld. Er is ook een officiële melding gedaan bij de Autoriteit Persoonsgegevens. Gedeputeerde Staten licht Provinciale Staten binnenkort in over dit incident.

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. Uw gegevens zijn niet inzichtelijk geweest voor anderen dan een groep provincieambtenaren. ~~Al onze collega's leggen een ambtseed af en wij verwachten integer gedrag van ze.~~ 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……
Ook is onze functionaris gegevensbescherming, 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

art 5 1-2e
Statengriffier

"Van: art 5 1-2e
Verzonden: 2019-09-20 13:47:55.926000+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: Nieuwe versie.
"
Nieuw voorstel

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

Geachte heer/mevrouw, [personaliseren]

Op 11 september is een datalek geconstateerd in één van onze systemen. Door dit lek zijn persoonlijke gegevens van u tijdelijk onvoldoende beschermd geweest. Met deze brief informeerenik wij u graag verder.

Aanleiding
Sinds vorig jaar mei is de Algemene Verordening Gegevensbescherming (AVG) van kracht. Deze verordening voorziet in een versterking van de privacyrechten en bescherming van data. We hebben naar aanleiding van deze verordening onder meer een Functionaris Gegevensbescherming aangesteld en het toezicht op de verwerking van (persoons)gegevens verder aangescherpt. Doordat wij onze bestaande werkwijzen en processen nu meer dan vroeger kritisch tegen het licht houden komen zwakke plekken sneller in beeld – ook voordat er daadwerkelijk misbruik gemaakt wordt van de gegevens - en kunnen we snel en direct gepaste maatregelen nemen. Dat is ook nu het geval. Een alerte medewerker heeft opgemerkt dat hij meer gegevens kon inzien dan hij nodig heeft voor het uitoefenen van zijn functie en. Hij heeft daar melding van gemaakt bij..

Toelichting: aard en omvang datalek
Voor het aanmelden van nieuwe Statenleden en fractiemedewerkers maakt de Statengriffie gebruik van het programma Topdesk. Wanneer een nieuw Statenlid of een fractiemedewerker wordt aangemeld, worden persoonsgegevens als een kopie van het identiteitsbewijs, de burgerlijke staat, een handtekening, een Burgerservicenummer (BSN) en een IBAN-nummer opgenomen in de administratie. Een aantal medewerkers kan deze gegevens inzien voor zijn of haar werk.

Gedurende de periode tussen 16 februari 2016 en 11 september 2019 had daarnaast een aantal andere medewerkers ook toegang tot deze gegevens. Het gaat dan bijvoorbeeld om collega's die een toegangspas aanmaken of een telefoon regelen. Deze collega's zien in Topdesk dat er een nieuwe medewerker is. Dat is voor hun werk voldoende informatie. Via een omweg *konden* deze medewerkers echter ook persoonlijke gegevens inzien die ze niet nodig hebben voor hun werk. In totaal gaat het om ongeveer 400 medewerkers. Daarmee is sprake van een datalek.

Na statenverkiezingen wordt een grote groep nieuwe statenleden en fractiemedewerkers in de provinciale administratie opgenomen met oog op de salarisverwerking en het verstrekken van toegangspassen en IT-middelen. Personele wisselingen die na die tijd plaatsvinden worden op een andere manier verwerkt. Dit gebeurt door daartoe aangewezen medewerkers van ondersteunende afdelingen. Hierbij worden in een IT-systeem de persoonsgegevens opgenomen die u de provincie heeft verstrekt. De genoemde medewerker 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 zien. We hebben geen aanwijzing dat dit daadwerkelijk is gebeurd, maar kunnen dit helaas niet uitsluiten.

Afhandeling/maatregelen
Na constatering is het lek direct gedicht. Alle aanvragen Uw persoonsgegevens zijn uit in het systeem zijn geblokkeerd verwijderd en de werkwijze is aangepast, zodat dit niet opnieuw kan gebeuren. Dde Functionaris Gegevensbescherming en de concerndirectie zijn op de hoogte gesteld. Er zijn procesafspraken gemaakt tussen P&O en de Statengriffie over een alternatieve werkwijze. Er is ook een

officiële melding gedaan bij de Autoriteit Persoonsgegevens. Gedeputeerde Staten licht Provinciale Staten binnenkort in over dit incident.

Wat betekent dit voor u?

Wij~~Ik~~ begrijpen dat 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. Uw gegevens zijn niet inzichtelijk geweest voor anderen dan een groep provincieambtenaren. Al onze collega's leggen een ambtseed af en wij verwachten integer gedrag van ze. De provincie heeft veel aandacht voor veilige omgang met persoonsgegevens en provinciemedewerkers zijn hier in toenemende mate alert op. Helaas hebben we ~~kunnen we~~ in dit geval niet kunnen uitsluiten dat mensen die geen toegang hoorden te hebben tot uw gegevens ze wel hebben gezien. Daarom vinden wij ~~ik~~ het van belang u dit bericht te sturen. Niettemin raden wij u aan om alert te zijn op signalen van identiteitsfraude of ander misbruik van uw persoonsgegevens.

Vragen?

Wij kunnen ons ~~Ik kan me~~ voorstellen dat er bij u nog vragen leven als het gaat om uw persoonlijke situatie. U kunt hiervoor contact opnemen met……
Ook is onze functionaris gegevensbescherming, art 5 1-2e beschikbaar voor om uw vragen te beantwoorden. U kunt hem bereiken per e-mail via fg@pzh.nl of telefonisch o art 5 1-2e

Gedeputeerde Staten, namens deze,

art 5 1-2e
Statengriffier

"Van: art 5 1-2e
Verzonden: 2019-09-20 17:46:48.563000+00:00
"Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: FW: Concept tekst
"
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 20 september 2019 17:46
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>;
art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e
<j. art 5 1-2e pzh.nl>
Onderwerp: Concept tekst
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste art 5 1-2e

Op verzoek van art 5 1-2e mail ik je onze concept tekst voor het informeren van de statenleden en fractiemedewerkers.

Aandachtspunt: in de tekst staat genoemd dat GS PS zullen informeren, maar dat is geloof ik nog onderwerp van gesprek.

Voel je vrij om aanpassingen in de tekst aan te brengen.

Mocht je over de inhoud willen afstemmen dan kun je mij of een van de andere uiteraard daarover bereiken.

art 5 1-2e e namen en adressen worden nog geverifieerd tegen de basisregistatie en kan
e maandag mailen.

Vast een fijn weekend.

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

Geachte heer/mevrouw, [personaliseren]

Onlangs 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.

Aanleiding
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 – ook voordat er daadwerkelijk misbruik gemaakt wordt van de gegevens - en kunnen we snel en direct 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 datalek
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.

Afhandeling/maatregelen
Na constatering is het lek direct gedicht. Uw persoonsgegevens zijn uit het systeem verwijderd en de werkwijze is aangepast, zodat dit niet opnieuw kan gebeuren. De functionaris voor gegevensbescherming en de concerndirectie zijn op de hoogte gesteld. Er is ook een officiële melding gedaan bij de Autoriteit Persoonsgegevens. Gedeputeerde Staten licht Provinciale Staten binnenkort in over dit incident.

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. Uw gegevens zijn niet inzichtelijk geweest voor anderen dan een groep provincieambtenaren. 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……

Ook is onze functionaris gegevensbescherming, 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

art 5 1-2e
Statengriffier

Geachte heer/mevrouw, [personaliseren]

Onlangs 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.

Aanleiding
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 – ook voordat er daadwerkelijk misbruik gemaakt wordt van de gegevens - en kunnen we snel en direct 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 datalek
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.

Afhandeling/maatregelen
Na constatering is het lek direct gedicht. Uw persoonsgegevens zijn uit het systeem verwijderd en de werkwijze is aangepast, zodat dit niet opnieuw kan gebeuren. De functionaris voor gegevensbescherming en de concerndirectie zijn op de hoogte gesteld. Er is ook een officiële melding gedaan bij de Autoriteit Persoonsgegevens. Gedeputeerde Staten licht Provinciale Staten binnenkort in over dit incident.

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. Uw gegevens zijn niet inzichtelijk geweest voor anderen dan een groep provincieambtenaren. 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……

Ook is onze functionaris gegevensbescherming, 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

art 5 1-2e
Statengriffier

"Van: art 5 1-2e
Verzonden: 2019-09-23 13:40:12.818000+00:00
"Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: Re: Concept tekst
"
Hoi, ik lig met griep in bed.

Ik weet niet wat er vanochtend is afgesproken maar misschien goed om aanpassingen met art 5 1-2e op te nemen.

Gr art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Mon, Sep 23, 2019 at 10:38 AM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Eens met voorstel van art 5 1-2e

Van: art 5 1-2e
Verzonden: maandag 23 september 2019 10:19
Aan: art 5 1-2e
CC: art 5 1-2e
Onderwerp: FW: Concept tekst
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

art 5 1-2e

Ad Toelichting: aard en omvang datalek

Ik vraag me af of het voldoende helder is dat het om tussentijdse wijzigingen gaat. De afsluitende zin zegt dat wil, maar de eerste bepaald niet.

Vandaar de suggestie om ook in de eerste zin al “tussentijdse” in te voegen.

Verder nog meervoud bij GS.

Groet,

art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: vrijdag 20 september 2019 17:47
Aan: art 5 1-2e art 5 1-2e pzh.nl>; art 5 1-2e
< art 5 1-2e pzh.nl>
Onderwerp: FW: Concept tekst
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

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 20 september 2019 17:46
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> >; 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 <j . art 5 1-2e pzh.nl
<mailto:j. art 5 1-2e pzh.nl> >
Onderwerp: Concept tekst
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste art 5 1-2e

Op verzoek van art 5 1-2e mail ik je onze concept tekst voor het informeren van de statenleden en fractiemedewerkers.

Aandachtspunt: in de tekst staat genoemd dat GS PS zullen informeren, maar dat is geloof ik nog onderwerp van gesprek.

Voel je vrij om aanpassingen in de tekst aan te brengen.

Mocht je over de inhoud willen afstemmen dan kun je mij of een van de andere uiteraard daarover bereiken.

art 5 1-2e e namen en adressen worden nog geverifieerd tegen de basisregistatie en kan ik je maandag mailen.

Vast een fijn weekend.

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

"Van: art 5 1-2e
Verzonden: 2019-09-24 16:49:31+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Tot slot
"

met vriendelijke groet,

art 5 1-2e

Senior Functioneel Specialist

Procesmanager CHM

Plv. teamcoördinator

Afdeling I&A | Bureau Bedrijfsinformatie

T 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/>

"

Actie:
Beste art 5 1-2e

Naar aanleiding van je melding, stuur ik je het volgende antwoord:
Het is niet mogelijk om vanuit TOPdesk te achterhalen, wie welke kaart heeft geopend en alleen maar bekeken heeft.

Ik verwacht hiermee uw vraag te hebben beantwoord. Mocht dit echter niet het geval zijn, neem dan gerust telefonisch contact met ons op.


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-09-25 13:24:44.217000+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: RE: Data lek opgepikt door omroep West
"
Hallo allen,

In het artikel op de website wordt gerefereerd aan statenvraag 3543 van de PVV waarvan de beantwoording gisteren in de GS-vergadering conform is vastgesteld.

In die statenvraag zijn grote zorgen geuit over de veiligheid van 'de ICT-systemen van de provincie'.

Die vraag is gesteld n.a.v. een op internet gepubliceerde lijst met overheidswebsites (met de naam 'Faalkaart'), waarin staat vermeld in welke mate die voldoen aan een aantal beveiligingsstandaarden. Van de provincies stond PZH op de derde plaats van onderen.

Ongelukkige samenloop van omstandigheden, maar belangrijk is dat deze websites volledig los staan van het interne IT-systeem waarin het datalek is geconstateerd.

Inhoudelijk verwijs ik naar de beantwoording in de bijlage.

Mochten er toelichting nodig zijn, dan hoor ik dat 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/>

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: woensdag 25 september 2019 12:34
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>; 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 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>
Onderwerp: Fwd: Data lek opgepikt door omroep West

Ter informatie

art 5 1-2e is contactpersoon als iemand benaderd wordt door journalisten.

Hartelijke groet,

art 5 1-2e

M art 5 1-2e

E art 5 1-2e pzh.nl

Provincie Zuid-Holland

---------- Forwarded message ----------
From: "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Date: Wed, Sep 25, 2019 at 12:13 PM +0200
Subject: Data lek opgepikt door omroep West
To: ""Zoete - van der Hout, WH, de"" <wh.de.zoete@pzh.nl
<mailto: art 5 1-2e pzh.nl> >, " " art 5 1-2e " art 5 1-2e pzh.nl
<mailto:dh.bennink@pzh.nl> >, "" art 5 1-2e " < art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> >

Datalek provincie: 'Persoonlijke gegevens politici onvoldoende beschermd'
#omroepwest

https://www.omroepwest.nl/nieuws/3906177/Datalek-provincie-Zuid-Holland-
Persoonlijke-gegevens-politici-onvoldoende-beschermd

Outlook voor Android downloaden <https://aka.ms/ghei36>
"


provincie
ZUID HOLLAND

ANTWO

VAN GEDEPUTEERDE STATEN OP VRAGEN VAN

J. Mooiman (PVV)
(d.d. 23 augustus 2019)

Nummer
3543

Onderwerp
Grote zorgen veiligheid ICT systemen Provincie Zuid-Holland

Aan de leden van Provinciale Staten

Toelichting vragensteller
Uit een bericht van Binnenlands Bestuur (*) komt naar voren dat uit de op basisbeveiliging.nl staande Faalkaart blijkt dat het over het algemeen slecht is gesteld met de veiligheid van ICT van Nederlandse gemeenten en provincies.

Tot schrik van de PVV zijn de resultaten voor de Provincie Zuid-Holland zwaar onvoldoende. 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. (**)

Het doel van de genoemde website is om de beveiliging en privacy voor o.a. provincies te verbeteren, en hoogleraa art 5 1-2e *(Universiteit Twente) is van mening dat de Faalkaart een goed instrument kan zijn om de overheids-ICT te verbeteren. De waarde van de Faalkaart wordt ook door het SIDN fonds onderschreven, opgericht door de Stichting Internet Domeinregistratie Nederland, de autoriteit die het .nl domein beheert.*

Hoogleraar art 5 1-2e *toonde onlangs ook al aan dat de cruciale digitale infrastructuur van Nederland kwetsbaar is en dat o.a. het kennisniveau van Nederlandse politici over ICT tekort schiet. (***)*

De PVV Zuid-Holland maakt zich grote zorgen over de staat waarin de veiligheid van de Zuid-Hollandse ICT zich bevindt met alle gevolgen van dien voor onze burgers, ondernemers en provinciale overheid en stellen daarom de volgende vragen aan Gedeputeerde Staten:

1. *Bent u bekend met de zogenoemde Faalkaart en deelt u de mening dat de resultaten voor de Provincie Zuid-Holland zéér zorgwekkend zijn? Zo nee, waarom niet?*

Antwoord
GS hebben kennisgenomen van de Faalkaart, vinden het belangrijk dat tekortkomingen waar nodig worden gerepareerd, maar zijn niet van mening dat de

resultaten zéér zorgwekkend zijn voor de veiligheid van de IT systemen van de provincie.

De provinciale ‘corporate’ website

De Faalkaart heeft betrekking op provinciale websites. De primaire ‘corporate’ website van de provincie Zuid-Holland is www.zuid-holland.nl. Via deze website wordt belangrijke informatie over de provincie verstrekt. Ook de besluiten van PS en GS zijn hierop te vinden. Deze website is een zogenaamde *transactiewebsite*. Als enige provinciale website vindt hier interactie met burgers en bedrijven plaats in de vorm van digitale contact- en aanvraagformulieren. Deze formulieren worden vanaf de website geautomatiseerd verwerkt naar de interne ICT-systemen van de provincie. Mede door deze koppeling is het risicoprofiel voor deze website hoger dan voor andere provinciale websites

De veiligheid van de corporate website wordt jaarlijks op een aantal manieren getoetst. Ten eerste laat de afdeling Informatisering en Automatisering van de provincie jaarlijks beveiligingsonderzoeken op deze website uitvoeren. Daarnaast toetst het Forum Standaardisatie jaarlijks of deze website aan verplichte beveiligingsstandaarden voor de publieke sector voldoet. Het Forum Standaardisatie is opgericht door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en onderhoudt de lijst met verplichte open standaarden voor de publieke sector en toetst de toepassing ervan. In de meest recente meting van maart 2019 is geconstateerd dat www.zuid-holland.nl aan alle verplichte internetstandaarden voldoet.
NB: In onderstaande tabel wordt ook het www.pzh.nl vermeld. Dit is echter geen publiek toegankelijke webadres. De bezoeker die dit webadres intypt, wordt naar de veilige zuid-holland.nl website geleid. In de volgende paragraaf wordt uitgelegd waarom dit bij een geautomatiseerde test tot verkeerde constateringen kan leiden.

Resultaten web provincies

Domeinnaam	DNSSEC	HSTS	HTTPS Afgedwongen	TLS	TLS NCSC
provincie.drenthe.nl	WAAR	WAAR	ONWAAR	WAAR	WAAR
www.bij12.nl	WAAR	ONWAAR	WAAR	WAAR	WAAR
www.brabant.nl	WAAR	ONWAAR	WAAR	WAAR	ONWAAR
www.drenthe.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.flevoland.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.fryslan.frl	WAAR	WAAR	WAAR	WAAR	WAAR
www.fryslan.nl	WAAR	ONWAAR	ONWAAR	ONWAAR	ONWAAR
www.gelderland.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.ipo.nl	ONWAAR	ONWAAR	WAAR	WAAR	WAAR
www.limburg.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.noord-holland.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.overijssel.nl	WAAR	WAAR	ONWAAR	WAAR	WAAR
www.provincie-utrecht.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.provinciegroningen.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.prvlimburg.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.pzh.nl	WAAR	ONWAAR	ONWAAR	ONWAAR	ONWAAR
www.zeeland.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.zuid-holland.nl	WAAR	WAAR	WAAR	WAAR	WAAR

M
eting informatieveiligheidstandaarden maart 2019

Tot slot zijn alle organisaties die DigiD op hun website gebruiken – waaronder de provincie – verplicht te voldoen aan een zware beveiligingsnorm. Via een jaarlijks ICT-beveiligingsassessment ziet Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, hierop toe. Ook in 2019 heeft Logius aan onze provincie goedkeuring verleend.

Overige provinciale websites

Naast de corporate website beschikt de provincie over een veelvoud van andere websites die divers van aard zijn. Hierop wordt informatie verstrekt over specifieke onderwerpen (zoals het coalitieakkoord, de begroting en archeologie) en er worden bijvoorbeeld filmpjes, foto's of kaarten getoond. Kenmerkend is dat er geen transacties plaatsvinden, er wordt geen DigiD gebruikt en er bestaat geen verbinding tussen de website en de interne ICT-systemen in de provinciale datacenters. Het risicoprofiel van dit soort websites is lager.

Om die reden zijn binnen de overheid de streefbeeldafspraken over de toepassing van de informatieveiligheidsstandaarden voor websites de afgelopen jaren juist gericht geweest op de transactiewebsites van de overheid (zoals www.zuid-holland.nl). Dit zijn afspraken die in het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) zijn vastgesteld en die jaarlijks worden getoetst door het Forum Standaardisatie.
Desalniettemin is de afspraak op dit moment dat (sinds einde 2018) álle overheidswebsites moeten voldoen aan een aantal beveiligingsstandaarden. De Faalkaart laat zien dat dit voor deze categorie provinciale websites nog niet in alle gevallen zo is.

Duiding
Op dit moment heeft de provincie veel verschillende websites. Dit compliceert om consistentie te krijgen in haar digitale uitingen en ook om alle websites op hetzelfde kwaliteitsniveau te brengen. De provincie heeft hier aandacht en streeft ernaar om alle websites te laten voldoen aan het hierboven genoemde afsprakenstelsel.

Er is vanuit de Faalkaart geen contact met de provincie Zuid-Holland geweest over de wijze van testen en het beoordelen van de resultaten. Dit maakt het voor de provincie lastig om de in de Faalkaart genoemde tekortkomingen exact te duiden. Dit komt omdat er meerdere redenen kunnen zijn waarom een dergelijke geautomatiseerde test bij een website een foutmelding oplevert en daardoor plaatsing op de Faalkaart. Een eerste controle (na de publicatie van de Faalkaart) van de testresultaten door de afdeling Informatisering & Automatisering van de province, laat zien dat bij circa een kwart van de websites de genoemde tekortkomingen niet (meer) worden aangetroffen of dat een andere oorzaak heeft geleid tot een vermelding op de Faalkaart.

2. *Wat is en wordt door de provincie ondernomen om de ICT-omgeving zo veilig mogelijk te maken voor onze burgers, ondernemers en provinciale overheid? Graag een gemotiveerd antwoord.*

Antwoord
Op dit moment heeft de provincie veel verschillende websites. Dit compliceert om consistentie te krijgen in haar digitale uitingen en ook om alle websites op hetzelfde kwaliteitsniveau te brengen.
Daarom is binnen onze provincie de ambitie ‘corporate website, tenzij’ geformuleerd, waarbij de corporate website altijd het eerste uitgangspunt is, tenzij het om een project gaat waar de provincie een van de vele deelnemers is en niet de trekker. Dit wordt verder uitgewerkt bij de vernieuwing van het digitaal platform Zuid-Holland, waarbij de provincie streeft naar kwaliteit op het gebied van informatieveiligheid, gebruiksvriendelijkheid, actualiteit, toegankelijkheid, leesbaarheid en vindbaarheid.

3. *Welke (aanvullende) maatregelen mogen wij van u verwachten n.a.v. de bijzonder zorgwekkende cijfers voor de Provincie Zuid-Holland? Graag een gemotiveerd antwoord.*

Antwoord
De provincie is voornemens om in 2023 aantoonbaar te voldoen aan de ISO27001 norm voor beheersing van informatieveiligheid met risicomanagement als vertrekpunt. In de tweede helft van 2019 worden hiervoor de eerste plannen gemaakt en concrete stappen gezet.

4. *Wat wordt door de Provincie en eventuele partners ondernomen om het kennisniveau inzake ICT veiligheid van de provinciale overheid (politici, bestuurders, ambtenaren en gezien haar rol ook de griffie) op pijl te houden en waar mogelijk verder te vergroten?*

Antwoord
Informatieveiligheid is een onderwerp dat regelmatig op de agenda staat van het portefeuilleoverleg met de gedeputeerde. Voor de provinciale organisatie is begin 2019 een bewustwordingscampagne (Up-to-data) gestart met informatie en activiteiten rond informatieveiligheid, privacy en informatiebeheer. Vorige week onder meer een bijeenkomst met een hacker. De bewustwordingscampagne heeft een continu karakter en zal de komende jaren voortduren.

Uit een bericht van Trouw (****) blijkt dat de gemeente Den Haag eind november 2018 een wedstrijd met prijzenpot organiseerde voor ethische hackers om een dag lang de Haagse systemen te hacken.

De hackers vonden maar liefst 62 zwakke plekken in de Haagse systemen, waarvan 10 vielen in de categorie "hoge impact" en 1 zelfs zo ernstig was dat een systeem direct moest worden uitgezet. De wedstrijd was daarmee erg "succesvol" en goedkoper dan het inhuren van een bedrijf om hetzelfde werk te doen.

5. *Deelt u de mening dat het regelmatig controleren van de provinciale systemen op zwakke plekken van groot belang is om de veiligheid van gevoelige informatie zo goed mogelijk op peil te houden? Zo ja, bent u bereid in navolging van de gemeente Den Haag een soortgelijke activiteit te organiseren voor ethische hackers? Zo nee, waarom niet?*

Antwoord
Ja, wij zijn van mening dat regelmatige controle belangrijk is. De in de Faalkaart genoemde websites maken echter een beperkt deel uit van de provinciale informatiesystemen en bevatten openbare informatie. Er is hier geen sprake van bedreiging van de veiligheid van gevoelige informatie.
De provincie neemt continu maatregelen om de veiligheid van de informatie¬voorziening te waarborgen en net als de gemeente den Haag maakt de provincie gebruik van ethische hackers. De provincie zet hen al enige jaren in op contractbasis.

Den Haag, 24 september 2019

Gedeputeerde Staten van Zuid-Holland,
secretaris, voorzitter,

drs. H.M.M. Koek drs. J. Smit

BRON

(*) https://www.binnenlandsbestuur.nl/digitaal/nieuws/faalkaart-toont-kwetsbaarheid-ict-overheden.10559222.lynkx

(**) https://basisbeveiliging.nl/#report-zuid-holland

(***) https://www.binnenlandsbestuur.nl/digitaal/nieuws/belangrijke-nederlandse-ict-infrastructuur-is.10414668.lynkx

(****) https://www.trouw.nl/nieuws/den-haag-laat-zich-bewust-hacken-een-stuk-goedkoper-dan-een-bedrijf-inhuren~bd68f62c/?referer=https%3A%2F%2Fwww.google.nl%2F

"Van: art 5 1-2e
Verzonden: 2019-09-25 14:03:55.833000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Data lek opgepikt door omroep West
"
Matig. Ben nog thuis maar hou mijn mail in de gaten.

Morgen kom ik weer naar Den Haag.

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 < art 5 1-2e pzh.nl>
Verzonden: woensdag 25 september 2019 14:02
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Re: Data lek opgepikt door omroep West

Ben je weer beter?

M art 5 1-2e

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

Provincie Zuid-Holland

On Wed, Sep 25, 2019 at 1:24 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Hallo allen,

In het artikel op de website wordt gerefereerd aan statenvraag 3543 van de PVV waarvan de beantwoording gisteren in de GS-vergadering conform is vastgesteld.

In die statenvraag zijn grote zorgen geuit over de veiligheid van ‘de ICT-systemen van de provincie’.

Die vraag is gesteld n.a.v. een op internet gepubliceerde lijst met overheidswebsites (met de naam ‘Faalkaart’), waarin staat vermeld in welke mate die voldoen aan een aantal beveiligingsstandaarden. Van de provincies stond PZH op de derde plaats van onderen.

Ongelukkige samenloop van omstandigheden, maar belangrijk is dat deze websites volledig los staan van het interne IT-systeem waarin het datalek is geconstateerd.

Inhoudelijk verwijs ik naar de beantwoording in de bijlage.

Mochten er toelichting nodig zijn, dan hoor ik dat 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/>

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: woensdag 25 september 2019 12:34
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 <j. art 5 1-2e pzh.nl <mailto:j . 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> > ; 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> >
Onderwerp: Fwd: Data lek opgepikt door omroep West

Ter informatie

art 5 1-2e s contactpersoon als iemand benaderd wordt door journalisten.

Hartelijke groet,

art 5 1-2e

M art 5 1-2e

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

Provincie Zuid-Holland

---------- Forwarded message ----------
From: "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Date: Wed, Sep 25, 2019 at 12:13 PM +0200
Subject: Data lek opgepikt door omroep West
To: ""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> >

Datalek provincie: 'Persoonlijke gegevens politici onvoldoende beschermd'
#omroepwest

https://www.omroepwest.nl/nieuws/3906177/Datalek-provincie-Zuid-Holland-
Persoonlijke-gegevens-politici-onvoldoende-beschermd

Outlook voor Android downloaden <https://aka.ms/ghei36>

"


provincie
ZUID HOLLAND

art 5 1-2e

Van: art 5 1-2e
Verzonden: 5 september 2019 16:06
Aan: art 5 1-2e
Onderwerp: pt tekst

Gevoeligheid: Vertrouwelijk

Ha art 5 1-2e
Dankjewel, dat denk ik ook.
Fijne vakantie!

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 p zh.nl

Provincie Zuid-Holland
Zuid-Hollandplein 1, 2596 AW
Postbus 90602, 2509 LP
Den Haag
www.zuid-holland.nl

Van: art 5 1-2e <j. art 5 1-2e @pzh.nl >
Verzonden: woensdag 25 september 2019 15:56
Aan: 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 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 < art 5 1-2e @pzh. nl>; art 5 1-2e < art 5 1-2e @pzh.nl >
Onderwerp: RE: Concept tekst
Gevoeligheid: Vertrouwelijk

Dag allemaal,

Het lijkt me goed om dit datalek nog even te evalueren alleen sta ik nu ook op het punt om met vakantie te gaan. Mochten jullie tijdnes mijn vakantie willen evalueren, dan zou ik in elk geval graag willen meegeven dat we wat mij betreft duidelijke afspraken moeten maken over 'wie hem is'. Waar begint de rol van de FG en waar houdt hij op? Wie doet daarna wat? Ik denk er winst te behalen is in de definitie van het eigenaarschap.

Veel groeten en tot eind oktober!!
art 5 1-2e

Van: art 5 1-2e < art 5 1-2e @pzh. nl>
Verzonden: maandag 23 september 2019 14:05
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.n l>; 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>; art 5 1-2e < art 5 1-2e @pzh.nl >; art 5 1-2e <j. art 5 1-2e @pzh. nl>
Onderwerp: Re: Concept tekst
Gevoeligheid: Vertrouwelijk

Beste mensen,
De een is ziek, de ander vrij, een derde op vakantie, kortom, Ik heb zojuis art 5 1-2e gevraa gd de coördinatie op zich te nemen, zij is daartoe gelukkig bereid! Haar eerste ac et art 5 1-2e sparren over onderstaande mail.
Hartelijke groet, art 5 1-2e

Outlook voor Android downloaden

Van: art 5 1-2e
Verstuurd: maandag 23 september 13:39
Onderwerp: RE: Concept tekst
Aan: 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

Ha art 5 1-2e

Ik snap, denk ik, wat je bedoelt: zelfs als GS PS informeren moet er ook aanvullend nog een bericht naar de betrokkenen die dan niet worden bereikt (oud-Statenleden en -fractiemedewerkers). Toch?

Dit neemt echter niet weg dat ik dan nog steeds wel eerst moet weten of GS het nu wel of niet gaan doen (PS informeren).
Een eventuele tekst van mij moet op dit punt kloppen uiteraard.
En bovendien, als GS dat wel doen ligt het voor de hand dat ik uitga van die GS-tekst en daar dan begeleidend tekstje bij doe, meer niet.
Kortom, het blijft voor mij relevant.
Wanneer wordt dit duidelijk? Morgen na GS?

Ander praktisch puntje nog: hoe bereik ik oud-Statenleden en oud-fractiemedewerkers?
Voor zover wij (griffie) hier nog (mail-)adressen hebben van deze personen, is de kans reëel dat die intussen niet meer actueel zijn.

Kortom, we zijn er nog niet, volgens mij…

Vriendelijke groet,

art 5 1-2e

Van: art 5 1-2e
Verzonden: maandag 23 september 2019 08:33
Aan: 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
Onderwerp: Re: Concept tekst
Gevoeligheid: Vertrouwelijk

Dag art 5 1-2e
Zonder de lijst in detail te kennen, kunnen er ook voormalig statenleden tussen zitten of oud-fractiemedewerkers. Het is daarom alleen al wenselijk een eensluidende brief aan alle betrokkenen te sturen.
Met vriendelijke groet art 5 1-2e Pr ovincie Zuid-Holland
Outlook voor Android downloaden

On Mon, Sep 23, 2019 at 7:05 AM +0200, " art 5 1-2e art 5 1-2e zh.nl > wrote:
Beste art 5 1-2e en ande ren,
Als inderdaad nog onderwerp van gesprek is of GS PS zullen informeren, moet de uitkomst daarvan hoe dan ook worden afgewacht, zou ik zeggen.
Op de eerste plaats zou een tekst die ik verstuur, uiteraard ook wat dat betreft moeten kloppen. Maar los daarvan, een tekst als deze wordt toch ook overbodig als GS PS informeren?
Of zie ik dat verkeerd?
Vr.gr.,
art 5 1-2e
Outlook voor Android downloaden

On Fri, Sep 20, 2019 at 5:46 PM +0200, "art 5 1-2e < art 5 1-2e pzh.nl > wrote:
Beste art 5 1-2e

Op verzoek van art 5 1-2e mail ik je on ze concept tekst voor het informeren van de statenleden en fractiemedewerkers.
Aandachtspunt: in de tekst staat genoemd dat GS PS zullen informeren, maar dat is geloof ik nog onderwerp van gesprek.
Voel je vrij om aanpassingen in de tekst aan te brengen.
Mocht je over de inhoud willen afstemmen dan kun je mij of een van de andere uiteraard daarover bereiken.

art 5 1-2e De namen en adressen worden nog geverifieerd tegen de basisregistatie en kan ik je maandag mailen.
Vast een fijn weekend.

Met vriendelijke groet,

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

Provincie Zuid-Holland

Zuid-Hollandplein 1, 2596 AW

Postbus 90602, 2509 LP

Den Haag

www.zuid-holland.nl

"Van: art 5 1-2e
Verzonden: 2019-09-26 15:24:40.196000+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e
Onderwerp: FW: memo voor MT - aanbevelingen startnotitie iDMS
"
Hoi art 5 1-2e

Bijgaand de definitieve stukken.

De versie die art 5 1-2eeerder stuurde mag je vergeten.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

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

art 5 1-2epzh.nl <mailto :art 5 1-2epzh.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 <art 5 1-2epzh.nl>
Verzonden: donderdag 26 september 2019 15:18
Aan: art 5 1-2e <art 5 1-2epzh.nl>
Onderwerp: RE: memo voor MT - aanbevelingen startnotitie iDMS

Hierbij art 5 1-2e

Groeten,
art 5 1-2e

Van: art 5 1-2e
Verzonden: donderdag 26 september 2019 14:17
Aan: art 5 1-2e <art 5 1-2epzh.nl <mailto :art 5 1-2epzh.nl> >
CC: art 5 1-2e <art 5 1-2epzh.nl <mailto :art 5 1-2epzh.nl> >
Onderwerp: memo voor MT - aanbevelingen startnotitie iDMS

Ha art 5 1-2e

Bijgevoegd de door mij aangekondigde memo voor agendering MT a.s. maandag. In de memo is verwezen naar een bijlage (de startnotitie iDMS). art 5 1-2emailt je deze vanmiddag.

Groeten,
art 5 1-2e
"

provincie ZUID HOLLAND

Memo

Contact
art 5 1-2e
art 5 1-2e
art 5 1-2e @pzh.nl

Datum
26 september 2019

Aan
Leden MT I&A

Kopie aan
team informatieveiligheid

Onderwerp
aanbevelingen startnotitie iDMS

N
aar aanleiding een beveiligingsincident in iDMS waarbij delen van beperkt toegankelijk gemaakte dossier bereed toegankelijk waren (geheime documenten waren te openen waarin zich ook gevoelige persoonsgegevens bevinden) heeft onder coördinatie van informatieveiligheid een onderzoek plaatsgevonden. Dit heeft geresulteerd in een startnotitie (zie bijlage).

Hieronder volgen de geformuleerde actie(s) een aanbevelingen uit de startnotitie.

Actie

- *Vervuiling:*
  Zet slimme ai-zoekmogelijkheden om te zoeken naar duplicaten, hernoemde kopieën, eerdere werkversies van documenten. Benader eigenaren en ruim op. Instrueer en communiceer.
- *Persoonsgegevens (AVG)*: idem.
- *Versnippering*:
  Bedenk hoe de diverse tools en opslaglocaties samenhangen en biedt de medewerkers duidelijke instructie hoe hiermee om te gaan.
- *Beveiliging en autorisaties:*
  De al in gang gezette verbeteringen door laten lopen. Borgen dat er voldoende bemensing op blijft en dat er voortgang in zit.
- *Houding en gedrag*:
  Is deels een doe-onderwerp in de zin dat er verbeterpotentieel zit op instructie, cursus, ondersteuning én aanspreken op ongewenst gedrag.
  Is ook een regie onderwerp: de behandelend ambtenaar heeft in de afgelopen jaren veel meer veratnwoordelijkheden gekregen voor het op correcte wijze aanleggen van dossiers. Niet alle gebruikers zijn echter gekwalificeerd om die verantwoordelijkheden te dragen. Gezocht moet worden hoe de behandelend ambtenaar hierin beter gefaciliteerd kan worden met moderne techniek en functionaleit.

Aanbevelingen

1. Laat een plannetje maken om de korte termijn verbeteringen uit te voeren en door te zetten.

provincie ZUID HOLLAND

Datum
26 september 2019
Ons kenmerk

2. Stel een informatie-regieteam samen (of bedenk een andere pakkende naam) dat op korte termijn met een strategisch actieplan komt. Het gevaar van stroperigheid ligt op de loer, dus zorg dat de vaart erin blijft. Operationaliseer de visie uit 2015 en actualiseer deze waar nodig.
3. Benoem een experise & vernieuwingsteam, dat op basis van energie zoekt naar vernieuwing, aansluit bij wat al loopt en verbinding maakt met marktpartijen, startups, andere provincies, VNG, Rijk.

   Het regieteam en experitise & vernieuwingsteam versterken elkaar en moeten goed voeling met elkaar houden.

Deze actie(s) en aanbevelingen verdienen een follow – up. Voorgesteld wordt onder verantwoordelijkheid van Bureau Documentaire Informatie, eigenaar van iDMS, een informatie-regieteam in te stellen die uiterlijk eind oktober 2019 aan het MT heeft voorgelegd:
1. een plan van aanpak om op korte termijn verbeteringen uit te voeren en door te zetten.
2. een strategisch actieplan (incl. benoeming team dat op zoek gaat naar vernieuwing en verbinding maakt).

provincie ZUID HOLLAND

Memo

Afdeling Informatisering en Automatisering
Contact
art 5 1-2e
art 5 1-2e
art 5 1-2e @pzh.nl

Datum
26 september 2019

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, André art 5 1-2e, art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e

Onderwerp
Startnotitie iDMS

Status: definitief

Aanleiding

Op verzoek van concerndirecteur art 5 1-2e is een analyse uitgevoerd naar knelpunten in het document managementsysteem iDMS. De directe aanleiding voor het verzoek ligt in het beveiligingsincident in iDMS waarbij delen van beperkt toegankelijk gemaakte dossiers toch breed toegankelijk waren. Geheime documenten waarin zich ook gevoelige persoonsgegevens bevinden waren te openen. Onderzoek heeft inmiddels uitgewezen dat dit ook in andere dossiers speelt. Aanvullend speelt mee dat er in iDMS veel persoonsgegevens te vinden zijn terwijl dat niet zou moeten.

Deze startnotitie start met een korte beschrijving van iDMS, waarna bevindingen en analyse leiden tot aanbevelingen die op korte of langere termijneffect moeten sorteren. De notitie is gebaseerd op gesprekken met collega's, documentstudie, eigen ervaring en de resultaten van de enquête die als start van de campagne Up-to-Data in april 2019 in de organisatie is gehouden. Veelvuldig is gebruik gemaakt van de visie en roadmap over de beheersing van ongestructureerde gegevens[1], die in 2015 in opdracht van I&A door Capgemini is opgesteld. In dit document worden naar aanleiding van de interviews met PZH-medewerkers, benchmarking bij andere organisaties en technische ontwikkelingen voor PZH op vier hoofdgebieden verbeteringen in het iDMS beschreven:

- Complexiteit en herkenbaarheid van de omgeving
- Gebruikersvriendelijkheid
- Aanpasbaarheid
- Toekomstbestendigheid

Veel van de hierin beschreven knelpunten en adviezen gelden vandaag de dag nog steeds. Ik heb geen onderzoek gedaan naar de reden waarom dit niet is opgepakt.

[1] Capgemini, 08-06-2015, *ECM Visie en Roadmap voor de Provincie Zuid-Holland*, vastgesteld door MT I&A op 22-06-2015

provincie ZUID HOLLAND

Datum
23 juli 2019
Ons kenmerk

Typering van iDMS: het integraal document managementsysteem

Functioneel

De door het iDMS geboden functionaliteit is gericht op de beheersing van ongestructureerde gegevens (hierna: ECM: Enterprise Content Management), die in de organisatie worden verwerkt. Denk hierbij aan bestandtypes als Word, Excel, PowerPoint, e-mail, Pdf, beeld, geluid en videobestanden. Echter, content wordt niet verwerkt zonder dat hier een proces aan ten grondslag ligt of metadata ontstaat. Metadata[2] en procesgegevens[3] spelen daarom beide een essentiële rol in het iDMS.

In de loop der jaren is PZH is een volwassen organisatie geworden waar het begrip en toepassing van de basisprincipes van ECM betreft. De toepassing van procesondersteuning, document management, archivering en integraties met systemen worden als essentieel beschouwd. Zij zijn onlosmakelijk aan de werkzaamheden van de PZH-medewerkers verbonden en PZH kan niet of nauwelijks functioneren zonder deze ondersteuning.

Technisch

Technisch gezien is de iDMS omgeving van PZH opgebouwd rondom het software platform Content Server van softwareleverancier OpenText. OpenText wordt algemeen beschouwd als een van de leidende bedrijven wereldwijd op het gebied van ECM-software.

Vanuit technisch oogpunt is het daarom begrijpelijk dat PZH voor de huidige techniek heeft gekozen. Toen PZH in 2007 met iDMS begon, was Content Server een van de weinige producten op de markt die de geëiste en gewenste functionaliteit kon bieden. Ook de inrichtingskeuzes die indertijd zijn gemaakt zijn een logisch gevolg van de situatie op dat moment. Namelijk: de transformatie van een papieren naar een digitale werkwijze. En de focus op control van de stukkenstromen die destijds in de organisatie opgang deed.
Kortom, PZH heeft het iDMS ingericht op basis van de toen door de organisatie gestelde randvoorwaarden, de aanwezige kennis en de beschikbare technieken.

[2] Metadata is gestructureerde informatie over de opgeslagen gegevens (zoals versiehistorie, auteur, typering van het soort document).
[3] Procesgegevens worden opgeslagen als bewijs over het verloop van een proces.

provincie ZUID HOLLAND

Datum
23 juli 2019
Ons kenmerk

Gebruik
In het verleden werd de behandelend ambtenaar (BA) in een aantal uitvoerende taken ondersteund door I&A specialisten, bijvoorbeeld op het gebied van dossiervorming en archivering. Sinds een aantal jaren (rond 2014) is die ondersteuning veranderd in advisering en wordt verwacht dat de BA deze werkzaamheden zelf uitvoert. De BA dient er nu zelf voor te zorgen dat dossiers worden aangemaakt, dat archiefwaardige[4] stukken in het dossier staan en dat overbodige stukken tijdig worden verwijderd.

Onderstaande kentallen geven een indruk van de omvang van het gebruik van iDMS:
- Aantal e-dossiers: 285.000, waarvan er 200.000 zijn gearchiveerd ('bevroren')
- Aantal andere mappen: > 2.500.000
- Aantal documenten: > 11.000.000
- Groeicijfers jaarlijks:
    - Nieuwe e-dossiers: > 9.500
    - Nieuwe workflows: > 120.000 (waarvan ca. 18.000 besluiten)
    - Groei opslag: ca. 1,5 Tb

Bevindingen
De onderstaande bevindingen zijn zo veel mogelijk als feitelijkheden beschreven. De volgorde zegt niets over de zwaarte ervan.

Vervuiling
Met de groei van het aantal documenten, staat er ook steeds meer vervuilende content in iDMS. Er is een wildgroei aan documenten die om opschoning vraagt. De vervuiling zorgt door de vele documenten en de vele, naast elkaar staande, versies van documenten voor een onoverzichtelijk beeld bij de gebruiker. Daarnaast kan de content vervuiling de performance van iDMS negatief beïnvloeden. Onderwerp van gesprek is vooral het organieke deel van iDMS waarin zich voor een deel nog archiefwaardige informatie bevindt, maar speelt ook in de e-dossiers.

Versnippering
Naast een teveel aan (verouderde) documenten in iDMS, speelt de situatie dat medewerkers documenten op veel andere opslaglocaties (kunnen) plaatsen. De richtlijnen welke documenten waar opgeslagen dienen te worden, zijn ingewikkeld en worden niet gehandhaafd. Dit is uiteraard niet een specifiek door iDMS veroorzaakt probleem.
Het aantal locaties en tools waarmee dat kan neemt alleen maar toe. In iDMS bestaan de folderstructuren voor de primaire en ondersteunende processen. Er is ook een nog veel grotere organieke tak (zeg maar de mappen voor afdelingen en bureaus). Iedere medewerker heeft nu nog een persoonlijke werkomgeving in iDMS, een persoonlijke P-schijf op het netwerk en opslagmogelijkheden op de laptop. Er is een interne SharePoint omgeving met AGA-koppeling naar iDMS ter ondersteuning van extern samenwerken.

[4] Archiefwaardige stukken: content waarover de provincie zich in het kader van besluitvorming, geschiedschrijving, transparantie en wet- en regelgeving moet kunnen verantwoorden.

provincie ZUID HOLLAND

Datum
23 juli 2019
Ons kenmerk

Er is cloud opslag in OneDrive for business en Microsoft Teams. En waarschijnlijk nog meer.

Beveiliging en autorisaties
Voor ons iDMS geldt dat we het “Beleid vertrouwelijke informatie” hanteren. Alle documenten zijn intern openbaar, tenzij. Aan de hand van autorisaties zorgen we ervoor dat vertrouwelijke documenten en mappen slechts toegankelijk zijn voor specifieke collega’s. Denk hierbij bijvoorbeeld aan personeelsdossiers of stukken van de Eenheid Audit en Advies, de ondernemingsraad of het proces handhaving en vergunningverlening waarbij veelal sprake is van persoonsgebonden, privacygevoelige en/of bedrijfsgevoelige informatie.
In de praktijk wordt een toenemende vraag naar beperkt toegankelijke mappen gesignaleerd. De beveiliging van en autorisatie tot content en workflows wordt handmatig ingesteld. De beheerlast op dit gebied wordt als hoog ervaren. Dit komt doordat de verantwoordelijke proceseigenaar vaak niet is aan te wijzen, het niet duidelijk is wie er bij de stukken mogen en wie niet (en waarom) en doordat uitzonderingen worden toegestaan.

Deze werkwijze is bovendien niet waterdicht. Recent zijn er beveiligingsincidenten in iDMS geconstateerd, waarbij ogenschijnlijk beperkt toegankelijk gemaakte dossiers toch breed toegankelijk bleken te zijn. Met als gevolg datalekken en inbreuken op de geheimhouding van stukken, doordat ongeautoriseerde medewerkers toegang tot de documenten hadden.
Het zoeken naar e-dossiers waar dit probleem zich in iDMS nog meer voordoet, is ingewikkeld gebleken en heeft veel tijd gekost. De technische mogelijkheden om de situatie te onderzoeken, te corrigeren en te monitoren zijn in de huidige versie van de iDMS software slechts beperkt beschikbaar.

Documentclassificatie
Aanvullend op het hierboven beschreven autorisatieprobleem is dat geheimhouding of beperking van rechten in iDMS wordt geregistreerd op de map waarin documenten worden geplaatst. De documenten binnen de map krijgen via overerving dezelfde rechten als de bovenliggende map. Dit gaat niet altijd goed, waardoor documenten in vertrouwelijke mappen via de zoekfunctie gevonden en geopend konden worden door ongeautoriseerde gebruikers. Dat kan per ongeluk zijn, omdat het niet altijd voor de gebruiker klip en klaar zijn dat het een geheim stuk betreft.
Het opleggen van toegangsbeperking op het niveau van mappen is een grofmazige wijze van autoriseren, omdat niet altijd alle documenten in de map dezelfde vertrouwelijkheid nodig hebben. Ook is het zo dat de toegangsbeperking zich binnen de registratie van iDMS bevindt; daarbuiten bestaat deze niet. Een negatief gevolg hiervan is dat van een document buiten de context van de map niet duidelijk is wat de classificatie is en wie het document mag inzien. Dit zien we ook in de praktijk; gebru kers delen geheime documenten per e-mail bijvoorbeeld om collega’s om commentaar te vragen. Kopieën van geheime stukken worden elders opgeslagen zonder dat duidelijk is dat het een geheim stuk betreft. Het ontbreken van document classificatie bemoeilijkt het geautomatiseerde treffen van beveiligingsmaatregelen.

provincie ZUID HOLLAND

Datum
23 juli 2019
Ons kenmerk

Persoonsgegevens (AVG)
De AVG stelt eisen aan de afscherming van persoonsgegevens, ook in iDMS. Het moet duidelijk zijn welke persoonsgegevens in iDMS zijn opgeslagen en wat daarvoor de wettelijke grondslag is. Ook mag niet iedereen documenten met persoonsgegevens inzien en moet aantoonbaar zijn wie dat kunnen en wie niet.
Gebleken is dat er in iDMS veel breed toegankelijke persoonsgegevens zijn opgeslagen, variërend van kopie identiteitsbewijzen tot verslagen van voortgangsgesprekken en zienswijzen. Dit is niet vreemd, omdat we uit een langdurige periode komen waarin er geen aandacht was voor de bescherming van persoonsgegevens. Maar desalniettemin voldoet deze situatie niet aan de regelgeving van de Algemene Verordening Gegevensbescherming (AVG).

Wet openbaarheid van bestuur (Wob) en Wet open overheid (Woo)
De samenleving wordt mondiger, eist openheid van zaken en stapt sneller naar toezichtorganen en/of rechters. PZH wenst een open organisatie te zijn en op efficiënte wijze rekenschap te kunnen geven. Ook wenst PZH snel en efficiënt te kunnen voldoen aan juridisch getinte verzoeken als Wob-verzoeken en de aankomende verplichte informatieverstrekking in het kader van de Wet open overheid (Woo).
De Woo moet ervoor zorgen dat overheidsinformatie beter vindbaar, uitwisselbaar, eenvoudig te ontsluiten en goed te archiveren is. In de gewijzigde Woo worden specifieke informatiecategorieën benoemd, zoals besluitvorming, subsidies en informatieverzoeken, die elke overheid actief openbaar moet maken. Dit geeft overheden duidelijkheid over wat ze dienen te publiceren. Het is daarbij van belang dat de informatie op een bruikbare wijze wordt gepubliceerd en niet door elke overheid op een andere wijze. Garanties voor machine-leesbare, gestandaardiseerde en gebruikersvriendelijke ontsluiting zijn daarbij essentieel.
Om uitvoering te kunnen geven aan de Woo zijn aanpassingen in iDMS nodig. In de paragraaf Analyse wordt dit nader toegelicht.

Houding en gedrag
Ondanks (of misschien juist wel: *door*) de afhankelijkheid van iDMS, zijn de iDMS gebruikers over het algemeen sceptisch over de technieken die worden toegepast en de wijze waarop de iDMS omgeving momenteel is ingericht. Dit bleek in 2015 uit het Capgemini onderzoek en daarna ook in de rapportages die de provinciearchivaris tweejaarlijkse uitbrengt. Ondanks regelmatige communicatie, actieweken (zoals de ‘Week van het archief’) en het in 2016 uitgevoerde verbeterprogramma Archief op Koers, is dit recent ook weer bevestigd in de resultaten van de Up-to-Data enquête van april 2019.

Behandelend ambtenaren vinden dossiervorming en archivering tijdrovend en complex, het niet tot hun taak behoren, vinden het iDMS en dan met name de folderstructuur en dossierkenniskaart te ingewikkeld en ook dat de performance te wensen overlaat. Tegelijkertijd klaagt men dat zoeken niet het juiste resultaat levert omdat veel informatie dubbel in iDMS staat. En bij een Wob-verzoek zoekt iedereen zich drie slagen in de

provincie ZUID HOLLAND

Datum
23 juli 2019
Ons kenmerk

rondte om de juiste informatie boven water te krijgen. Kort samengevat: een vicieuze cirkel.

Analyse van de bevindingen
Zoals genoemd is PZH een koploper geweest waar het begrip en toepassing van de basisprincipes van ECM betreft. Of dat nog zo is weet ik niet, maar we sjokken zeker niet achteraan. Het is makkelijk om te klagen, maar de organisatie zou niet meer zonder iDMS kunnen en willen.

… en toch moet het beter!
De digitale ambitie van onze organisatie is hoog. We willen innoveren en digitaal voorooplopen. Een data-gedreven organisatie zijn en een verbindende rol spelen in de provincie. Dat vraagt om herbezinning op wat ECM hierin betekent.
De iDMS omgeving zoals wij die hebben begint wat roestig te worden qua functionele en technische mogelijkheden van de software als ook de inrichtingsconcepten die in feite dateren uit 2007. In 2015 hadden we plannen (“de ECM visie”) om de omgeving te moderniseren, maar die hebben we maar beperkt uitgevoerd. Om (minimaal) de volgende redenen is daarom nu gecoördineerde actie nodig:

- Actualiteit van de software: onze versie van een deel van de iDMS software wordt niet meer door de leverancier ondersteund, waardoor we noodgedwongen moeten upgraden. De upgrade die een deel van de OpenText software suite betreft gaat ons nieuwe mogelijkheden bieden, maar dit is toch iets anders dan een strategische transformatie naar een gewenste situatie die om andere functionaliteit vraagt dan voorheen.
- Verkenning is nodig of functionaliteit die PZH als maatwerk heeft ingebouwd, inmiddels niet standaard in de markt aanwezig is. Sturing is nodig om ervoor te zorgen dat standaard goed genoeg is en te voorkomen dat aanvullende wensen uit de organisatie alsnog tot maatwerk leiden.
- Daarbij komt dat de ontwikkelingen op andere gebieden (zoals business intelligence, artificial intelligence, datawarehousing, geografische informatietechnologie) hard gaan. Overlappingen in deze gebieden vragen om herbezinning van de rol van ECM in dit speelveld. Toepassing van artificial intelligence en business intelligence (BI) op content kan helpen bij vraagstukken die ons nu veel moeite kosten. Gedacht kan worden aan text analytics, maar ook aan creëren van overzichten ten behoeve van audit vraagstukken. Daarnaast wordt steeds vaker gevraagd om data en content in relatie tot elkaar te analyseren. Dit omdat data de harde cijfers ondersteunt, maar content analyse juist op het sentiment kan inzoomen. Zie ook de bijlage: *Content en data komen samen*
- Het belang van goed archiefbeheer binnen andere informatiesystemen is onderkend en moet worden uitgewerkt. Archief en vernietigingsregime dient ook te worden toegepast op data lakes, data warehouses en andere omgevingen.
- De impact van de Woo zit hem vooral in het herinrichten en automatiseren van processen rond opstellen, vaststellen en publiceren van documenten. Verder zullen we veel beter dan nu moeten weten welke documenten, informatie en data we hebben, wat van onszelf is en wat van derden en wat relevant is voor be-

provincie ZUID HOLLAND

Datum
23 juli 2019
Ons kenmerk

sluitvorming. Ook appjes en e-mails die relevant zijn moeten we opslaan en publiceren, net als externe adviezen die in onze opdracht zijn gemaakt.
Een ECM-omgeving dient ook met deze aspecten rekening te houden. Zekerheid van het aanbieden van de juiste content op het juiste moment voor het juiste verzoek moet kunnen worden gegeven. Snelle afhandeling van verzoeken omtrent openheid, en in het geval van een juridische zaak, moet worden gefaciliteerd. Dit betreft niet alleen archiefwaardig materiaal, maar kan ook betrekking hebben op alle content die binnen PZH aanwezig is.

Regie

Dit zijn best grote vraagstukken, wat waarschijnlijk de reden is dat de ECM-visie slechts beperkt is uitgevoerd. We moeten ze echter wel onder ogen zien en ermee aan de slag gaan. We kunnen het regie op data- en informatiebeheer noemen. Of data governance. In ieder geval is het nodig om niet meer in silo's te denken, met elkaar in gesprek te gaan, zaken in samenhang te plaatsen en strategisch richting te kiezen op een manier die past bij de dynamiek van de organisatie en de vaart van de technologische ontwikkelingen. Dat betekent dat we durven om – met begrip voor architectuur, informatieveiligheid, privacy en beheer - te zoeken naar vernieuwing en verbetering, voort te zetten wat goed werkt en afscheid durven nemen van wat tegenvalt.

Actie

Voor een ander deel van de bevindingen kunnen we direct in de doe-modus schieten. Sterker, daar lopen al activiteiten. Met een combinatie van scherpere beheerafspraken, betere monitoring en instructie van gebruikers komen we een heel eind:

- *Vervuiling:*
  Zet slimme ai-zoekmogelijkheden om te zoeken naar duplicaten, hernoemde kopieën, eerdere werkversies van documenten. Benader eigenaren en ruim op. Instrueer en communiceer.
- *Persoonsgegevens (AVG)*: idem.
- *Versnippering*:
  Bedenk hoe de diverse tools en opslaglocaties samenhangen en biedt de medewerkers duidelijke instructie hoe hiermee om te gaan.
- *Beveiliging en autorisaties*:
  De al in gang gezette verbeteringen door laten lopen. Borgen dat er voldoende bemensing op blijft en dat er voortgang in zit.
- *Houding en gedrag*:
  Is deels een doe-onderwerp in de zin dat er verbeterpotentieel zit op instructie, cursus, ondersteuning én aanspreken op ongewenst gedrag.
  Is ook een regie onderwerp: de behandelend ambtenaar heeft in de afgelopen jaren veel meer verantwoordelijkheden gekregen voor het op correcte wijze aanleggen van dossiers. Niet alle gebruikers zijn echter gekwalificeerd om die verantwoordelijkheden te dragen. Gezocht moet worden hoe de behandelend ambtenaar hierin beter gefaciliteerd kan worden met moderne techniek en functionaliteit.

Documentclassificatie en *Wet open overheid (Woo)* zijn meer regie onderwerpen.

provincie ZUID HOLLAND

Datum
23 juli 2019
Ons kenmerk

Aanbevelingen

1. Laat een plan maken om de korte termijn verbeteringen uit te voeren en door te zetten.
2. Stel een informatie-regieteam samen (of bedenk een andere pakkende naam) dat op korte termijn met een strategisch actieplan komt. Operationaliseer de visie uit 2015 en actualiseer deze waar nodig. Hak de grote vraagstukken op in kleine, benoem de afhankelijkheden en bepaal de actievolgorde. Het gevaar van stroperigheid ligt op de loer, dus zorg dat de vaart erin blijft.
3. Benoem een expertise & vernieuwingsteam, dat op basis van energie zoekt naar vernieuwing, aansluit bij wat al loopt en verbinding maakt met marktpartijen, startups, andere provincies, VNG, Rijk.

Het regieteam en het expertise & vernieuwingsteam versterken elkaar en moeten goed voeling met elkaar houden.

provincie ZUID HOLLAND

Datum
23 juli 2019
Ons kenmerk

BIJLAGE

EAA-enquête april 2019
Als opmaat naar de campagne Up-to-Data heeft EAA in april 2019 een enquête in de organisatie uitgezet met – naast de onderwerpen informatieveiligheid en AVG - vragen over dossiervorming en archivering. Deze vragen zijn direct te relateren aan kennis over en gebruik van iDMS. De enquête is ingevuld door 543 collega's (35% respons).

Van de respondenten die zich positief of negatief[5] hebben uitgesproken over vragen ten aanzien van dossiervorming en archivering, geeft 70% van de respondenten aan te weten wat er van ze wordt verwacht wanneer het gaat om het opslaan van documenten in een e-dossier in iDMS. De helft (48%) geeft aan dat er ook binnen de eigen afdeling duidelijke afspraken zijn over hoe om te gaan met het opslaan van documenten en 54% weet waar ze met vragen over iDMS terecht kunnen. De regels, afspraken en hulplijnen lijken bij de ambtenaren dus bekend te zijn.

Toch is meer dan de helft (52-67%) van de respondenten zich onvoldoende bewust van het belang van een compleet e-dossier, weet men niet welke documenten in het e-dossier horen, ziet men het niet als de eigen verantwoordelijkheid om een e-dossier compleet te maken of heeft men er geen tijd voor. En maar 35% antwoordt dat de e-dossiers op de eigen afdeling op orde zijn. Als oorzaak dat dossiers niet op orde zijn wordt vaak de gebruikersonvriendelijkheid van IDMS genoemd, of dat de naamgeving niet logisch is. Ook wijt men het niet op orde zijn van e-dossiers aan niet duidelijke regels en dat men niet wordt aangesproken op de wijze van archiveren.

Content en data komen samen
De ontwikkeling die zich na het beschikbaar maken van de content in de bedrijfsprocessen aandient is het samenvoegen van content en data. Momenteel wordt er vaak nog onderscheid gemaakt tussen content en data. Data betreft de gestructureerde informatie die is opgeslagen in databases van ERP, CRM en HR-systemen. Content betreft de ongestructureerde informatie die in document managementsystemen worden opgeslagen. Een logische keuze omdat de technische mogelijkheden om te werken met de beide informatievormen veel van elkaar verschillen. Data kan geanalyseerd, vergeleken, berekend en geëxtrapoleerd worden. Terwijl dat met platte content met weinig of zelfs geen context alweer veel moeilijker is. Om meer met content te kunnen doen is het principe van metadatering en indexering bedacht. Content kan hierdoor doorzocht, verzameld en in context van iets gebracht worden. Echter het stuk content zelf is nog steeds een specifiek object dat zijn eigen formaat (PDF, Excel, Word, Mail) en kenmerken heeft.
Nieuwe technieken zorgen er voor dat ook content als informatie type gaat veranderen en uiteindelijk ook als data beschouwd gaat worden. Het belangrijkste voorbeeld hiervan is Content analytics. Deze techniek richt zich op de analyse van geschreven tekst, zoals in documenten, e-mails en Twitter berichten. De software kan informatie uit tekst omzet-

[5] Per vraag antwoord circa 22% 'neutraal'.

provincie ZUID HOLLAND

Datum
23 juli 2019
Ons kenmerk

ten in meer gestructureerde data die vervolgens door middel van Business Intelligence (BI) worden geanalyseerd en ondersteunend zijn aan besluiten en visies.


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-10-01 09:25:16.421000+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: RE: DATALEK: Risico's in TOPdesk
"
Hallo art 5 1-2e

Dankjewel dat je zo oplettend bent.

We hebben om 10:00 privacyteam overleg.

Ik zal het daar op de agenda plaatsen.

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 < art 5 1-2e pzh.nl>
Verzonden: maandag 30 september 2019 16:54
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> ; art 5 1-2e pzh.nl> ; art 5 1-2e
art 5 1-2e pzh.nl> ; art 5 1-2e pzh.nl>
Onderwerp: DATALEK: Risico's in TOPdesk
Urgentie: Hoog

Op art 5 1-2e na heb ik nog geen reactie ontvangen.

Moet ik dit dan melden als een datalek, want volgens mij kan dit niet.

art 5 1-2e dit zijn de potentiele P&O processen en mailimports waar de risico’s zitten.

Alle P&O medewerkers kunnen dit zien en hier en daar ook mensen van daarbuiten.

En daaronder enkele voorbeelden uit zomaar een steekproef van gegevens die gewoon door iedereen te zien zijn.

Het lek zit dus echt nog niet dicht .

met vriendelijke groet,

art 5 1-2e

Senior Functioneel Specialist

Procesmanager CHM

Plv. teamcoördinator

Afdeling I&A | Bureau Bedrijfsinformatie

T 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/>

"


provincie
ZUID HOLLAND

P&O - Aanmelden externe medewerker

P&O - Aanvraag dashboard arbeidscapaciteit

P&O - Aanvraagformulier in- en externe cursussen (geen POB)

P&O - Aanvraagformulier Persoonlijk ontwikkel budget (POB)

P&O - Aanvraagformulier PZH akademie

P&O - Eigen bijdrage NS-abonnement

P&O - Formatie mutaties Beaufort Lias

P&O - HP Status

P&O - indiensttreding INTERNE medewerker (3=1)

P&O - Indiensttreding OVERIGE medewerker

P&O - Parkeerkaart carpool & creche

P&O - Parkeerkaart dienstgebruik eigen auto

P&O - Verloren toegangspas melden

provincie ZUID HOLLAND

INLICHTINGENFORMULIER

art 5 1-2e

provincie ZUID HOLLAND

GEGEVENSFORMULIER STAGIAIRES

art 5 1-2e


provincie
ZUID HOLLAND

provincie ZUID HOLLAND

GEGEVENSFORMULIER STAGIAIRES

art 5 1-2e

art 5 1-2e

"Van: art 5 1-2e
Verzonden: 2019-10-01 14:15:36.518000+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019
"
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 < art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 13:55
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: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Tk

Voortouw ligt bij art 5 1-2e we hadden afgesproken dat zij coördineert.

En wat de routing betreft: is aan art 5 1-2e ij is verantwoordelijk voor de datalekken. art 5 1-2e een puntje om te bespreken met hem.

Groet,

art 5 1-2e

Verzonden vanuit Mail <https://go.microsoft.com/fwlink/?LinkId=550986> voor Windows 10

Van: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 13:51
Aan: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Dag art 5 1-2e

Hier hadden we het over. Coördineer jij, zoals afgesproken?

Groet,

art 5 1-2e

Verzonden vanuit Mail <https://go.microsoft.com/fwlink/?LinkId=550986> voor Windows 10

Van: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 13:20
Aan: art 5 1-2e <mailto : art 5 1-2e pzh.nl> ; art 5 1-2e <mailto: art 5 1-2e pzh.nl>
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Hallo art 5 1-2e en art 5 1-2e

SGP/CU heeft statenvragen gesteld over het datalek.

De vragen zijn via de afd. Bestuur gerouteerd naar art 5 1-2e (FG).

Wij (art 5 1-2en het privacyteam) zijn echter van mening dat de beantwoording uit de ambtelijke lijn moet komen en niet van de FG, die adviseur en toezichthouder is.

Ik ga er dus mee aan de slag.

* Willen jullie dit a.s. maandag in het MT melden?
* art 5 1-2e misschien is de routering van dit soort vragen een onderwerp om kort met Willy de Zoete te bespreken ?

Ik stem de beantwoording af met het privacyteam en houd jullie in de loop.

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 < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 1 oktober 2019 10:20
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> >
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

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
Verzonden: dinsdag 1 oktober 2019 09:23
Aan: art 5 1-2e
Onderwerp: Fwd: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Hi art 5 1-2e hierbij ontvang je statenvragen over data lek. Wil je voor de beantwoording zorgdragen?

Groet, art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

---------- Forwarded message ----------
From: " art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Date: Fri, Sep 27, 2019 at 4:52 PM +0200
Subject: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019
To: "" art 5 1-2e " < art 5 1-2e pzh.nl <mailt o art 5 1-2e zh.nl> >

Beste art 5 1-2e

Hierbij nieuwe schriftelijke vragen, iets voor art 5 1-2e

Met vriendelijke groet,

art 5 1-2e

Administratief ondersteuner A

Afdeling Bestuur | Bureau Beleidscoördinatie en Advies | GS-ondersteuning

T art 5 1-2e

art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl>

gsondersteuning@pzh.nl <mailto:gsondersteuning@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>
"

ChristenUnie & SGP
Zuid-Holland

Melding datalek 24 september 2019
Schriftelijke vraag conform artikel 49 Reglement van Orde nr 3556

Aan de voorzitter van het college van Gedeputeerde Staten, 27 september 2019

Toelichting
Op 24 september hebben een aantal leden van Provinciale Staten een brief ontvangen over een datalek in één van de provinciale systemen. Een alerte medewerker heeft op 11 september 2019 het datalek gemeld. Deze medewerker kon meer gegevens inzien dan voor de functie noodzakelijk. Na onderzoek bleek dat een andere groep van 406 behandelaren ook "zij het met wat meer moeite" meer gegevens kon inzien dan noodzakelijk. De provincie heeft zowel een melding gedaan bij de Autoriteit Persoonsgegevens als de betrokkenen middels een brief van 24 september op de hoogte gebracht. De provincie heeft dit datalek inmiddels 'gedicht'.

Volgens de Autoriteit Personeelsgegevens (website; geraadpleegd 27 september 2019) is de meldplicht afhankelijk van de (potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van betrokkenen. "U hoeft een datalek niet te melden als het niet waarschijnlijk is dat het datalek leidt tot een risico voor de rechten en vrijheden van betrokkenen." De website van de Autoriteit Persoonsgegevens vermeld verder dat de betrokkenen (de personen van wie u gegevens verwerkt) alleen geïnformeerd hoeven te worden als "een datalek waarschijnlijk een hoog risico voor hun rechten en vrijheden oplevert."

<u>Vragen</u>

1. Aan hoeveel betrokken personen is de brief van 24 september verstuurd? Op hoeveel personen heeft dit datalek in totaal betrekking? Om welke groep(en) van personen gaat het?
2. Welke gegevens van deze personen konden door daartoe onbevoegde medewerkers van de ambtelijke organisatie worden ingezien? Hoe lang heeft dit datalek bestaan?
3. GS geeft aan dat het niet bekend is hoeveel medewerkers onbevoegd informatie heeft ingezien. Logt het systeem niet wie welke gegevens inziet? Zo nee, waarom niet?
4. Hoe en op welke termijn, na hoeveel tijd, zijn door de medewerker, zijn afdelingshoofd, de functionaris gegevens bescherming, de concerndirectie, gedeputeerde staten, de Autoriteit Persoonsgegevens en uiteindelijk de betrokkenen op de hoogte gesteld? Wat is de tijdlijn? Kunt u in deze tijdlijn ook de maatregelen meenemen en om het lek te stoppen en de genomen maatregelen om de schade te beperken.
5. Is er bij dit datalek binnen de wettelijke termijnen gehandeld? Zo nee, waarom niet?
6. Hoe is de ernst van dit datalek gekwalificeerd? Welke 'rechten en vrijheden' van personen zijn bij dit datalek in het geding?
7. Hoe is GS op grond van de inschatting van de 'ernst' van het datalek en de hoogte van het risico (zie vraag 6) tot de conclusie gekozen om: 1] een officiële melding bij de Autoriteit Persoonsgegevens te doen en 2] de betrokkenen over het datalek te informeren? Graag op beide onderdelen van deze vraag een apart gemotiveerd antwoord.
8. Welke leerpunten trekt GS uit dit datalek over de beveiliging van persoonsgegevens in de andere provinciale systemen?

Namens de fractie ChristenUnie en SGP,

art 5 1-2e


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-10-02 09:29:39.391000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019
"
Hoi art 5 1-2e

Hierbij vast de procedurebeschrijving.

Een concept voor de inhoudelijke beantwoording volgt later.

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 < art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 17:12
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: RE: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

In dit geval blijf ik nog coördineren.

Fijn art 5 1-2e art 5 1-2e dat jij de inhoudelijke beantwoording oppakt. Zou je mij ook de procesbeschrijving van melding datalekken, met rollen en verantwoordelijkheden willen toesturen?

Hartelijke groet,

art 5 1-2e

M art 5 1-2e

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

Provincie Zuid-Holland

Van: art 5 1-2e
Verzonden: dinsdag 1 oktober 2019 13:55
Aan: art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24

september 2019

Tk

Voortouw ligt bij art 5 1-2e we hadden afgesproken dat zij coördineert.

En wat de routing betreft: is aan art 5 1-2e hij is verantwoordelijk voor de datalekken. art 5 1-2e een puntje om te bespreken met hem.

Groet,

art 5 1-2e

Verzonden vanuit Mail <https://go.microsoft.com/fwlink/?LinkId=550986> voor Windows 10

Van: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 13:51
Aan: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Dag art 5 1-2e

Hier hadden we het over. Coördineer jij, zoals afgesproken?

Groet,

art 5 1-2e

Verzonden vanuit Mail <https://go.microsoft.com/fwlink/?LinkId=550986> voor Windows 10

Van: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 13:20
Aan: art 5 1-2e <mailto : art 5 1-2e pzh.nl> ; art 5 1-2e <mailto: art 5 1-2e pzh.nl>
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Hallo art 5 1-2e en art 5 1-2e

SGP/CU heeft statenvragen gesteld over het datalek.

De vragen zijn via de afd. Bestuur gerouteerd naar art 5 1-2e (FG).

Wij (art 5 1-2e en het privacyteam) zijn echter van mening dat de beantwoording uit de ambtelijke lijn moet komen en niet van de FG, die adviseur en toezichthouder is.

Ik ga er dus mee aan de slag.

* Willen jullie dit a.s. maandag in het MT melden?
* art 5 1-2e misschien is de routering van dit soort vragen een onderwerp om kort met Willy de Zoete te bespreken ?

Ik stem de beantwoording af met het privacyteam en houd jullie in de loop.

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 < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 1 oktober 2019 10:20
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> >
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

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
Verzonden: dinsdag 1 oktober 2019 09:23
Aan: art 5 1-2e
Onderwerp: Fwd: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Hi art 5 1-2e hierbij ontvang je statenvragen over data lek. Wil je voor de beantwoording zorgdragen?

Groet, art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

---------- Forwarded message ----------
From: " art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >
Date: Fri, Sep 27, 2019 at 4:52 PM +0200
Subject: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019
To: "" art 5 1-2e " < art 5 1-2e ozh.nl <mailto : art 5 1-2e ozh.nl> >

Beste art 5 1-2e

Hierbij nieuwe schriftelijke vragen, iets voor art 5 1-2e

Met vriendelijke groet,

art 5 1-2e

Administratief ondersteuner A

Afdeling Bestuur | Bureau Beleidscoördinatie en Advies | GS-ondersteuning

T art 5 1-2e

art 5 1-2e pzh.nl <mailt o art 5 1-2e ozh.nl>

gsondersteuning@pzh.nl <mailto:gsondersteuning@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>
"


provincie
ZUID HOLLAND

provincie ZUID HOLLAND

Procedure voor het afhandelen van datalekken

Provincie Zuid-Holland

Mei 2018
Provincie Zuid-Holland
Versie: 1.1

overzicht besluitvorming / bespreking

Documenthistorie

Versie	Datum	Wie	Wijziging
1.0	7 februari 2016	art 5 1-2e	Eerste procedure
1.1	9 mei 2018	art 5 1-2e	Geactualiseerd n.a.v. de AVG

Vastgesteld door concerndirecteur art 5 1-2e op 11 mei 2018.

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Vanaf 1 januari 2016 is de meldplicht Datalekken van kracht. Dit houdt in dat de provincie verplicht is om (potentiële) datalekken te melden aan de landelijke toezichthouder, de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene van wie de gegevens zijn gelekt. Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) formeel van kracht die de huidige Wet bescherming persoonsgegevens (Wbp) vervangt. Ook onder de AVG geldt de meldplicht datalekken.

Er is echter wel een aantal veranderingen ten opzichte van de Wbp, die tot een lichte wijziging in de huidige procedure leidt. Zoals de aanwezigheid in de provincie van een functionaris voor de gegevensbescherming en licht aangepaste terminologie.

1.2 Persoonsgegevens

Een persoonsgegeven is volgens de AVG alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”). Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Er kan een onderscheid worden gemaakt in direct en indirect identificerende gegevens.

Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum.
Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.

Voorbeelden:

- Wanneer bijvoorbeeld een telefoonnummer (indirect identificerend) via een telefoonboek gekoppeld kan worden aan een naam (direct identificerend), dan is het telefoonnummer een persoonsgegeven. Bij de beoordeling of gegevens gekoppeld kunnen worden gaat het niet alleen om de gegevens die de verwerkingsverantwoordelijke in zijn bezit heeft. Ook gegevens die bijvoorbeeld via internet openbaar toegankelijk zijn kunnen worden meegewogen in de beslissing of iemand identificeerbaar is.
- Als door een combinatie van gegevens een dusdanig uniek beeld ontstaat dat de gegevens maar op één persoon betrekking kunnen hebben. Een voorbeeld van een dergelijke spontane identificatie is: ‘een 39-jarige mannelijke jurist woonachtig aan de Oxfordlaan te Leiden’. Het is zeer onwaarschijnlijk dat deze combinatie op meer dan één geïdentificeerde persoon betrekking heeft.

1.3 Datalek

In tegenstelling tot de Wbp, komt in de AVG het letterlijke woord datalek niet voor, maar wordt gesproken over “inbreuk in verband met persoonsgegevens”. Omdat de term datalek echter inmiddels ingeburgerd is, blijven wij (net als de Autoriteit Persoonsgegevens) deze term hanteren.

Bij een datalek is sprake van een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die eventueel zijn getroffen waren niet toereikend om dit te voorkomen.

Voorbeelden van een datalek zijn het verlies van een papieren document of mobiel apparaat waarop gevoelige persoonsgegevens staan. Maar ook computer hacking, besmetting met ransomware, of het technische falen van apparatuur, stroomuitval, wateroverlast kunnen leiden tot een datalek.

1.4 Inhoud meldplicht

De melding moet zo mogelijk gebeuren binnen 72 uur, zonder onderscheid tussen werkdagen, weekenden of feestdagen. Als het incident later dan 72 uur na ontdekking aan de Autoriteit Persoonsgegevens wordt gemeld, dan moet dit worden gemotiveerd. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. De Autoriteit Persoonsgegevens slaat de melding op in een register met alle ontvangen meldingen over datalekken. Dit register is niet openbaar.

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.

1.5 Doel en reikwijdte van deze procedure

Deze procedure beschrijft de wijze waarop binnen de provincie Zuid-Holland wordt omgegaan met de meldplicht datalekken in de zin van de Algemene Verordening Gegevensbescherming (AVG). De procedure is gericht op het beperken van de schade, analyseren van de (ernst van) de situatie en het opstellen van een onderbouwd advies aan de eindverantwoordelijke functionaris binnen de provincie. Dit is de concerndirecteur die gemandateerd is te besluiten om al dan niet melding te doen bij de Autoriteit Persoonsgegevens en betrokkenen (wiens persoonsgegevens het betreft).

De procedure wordt onder coördinatie van de afdeling I&A uitgevoerd, in nauwe samenwerking met de informatiebeheerder van P&O, de privacy jurist van FJZ, de I&A incident manager, een medewerker documentaire informatie van I&A, de functioneel/technisch beheerder van het systeem, betrokken medewerker(s) en diens leidinggevende. Per potentieel datalek wordt op die manier een datalekteam geformeerd.

De functionaris gegevensbescherming (FG) wordt geïnformeerd over het optreden van het potentiële datalek en de afhandeling ervan. De FG kan tijdens de afhandeling gevraagd en ongevraagd adviseren en beoordeelt de correcte uitvoering van de procedure. De FG kan hiertoe per afzonderlijk geval besluiten deel te nemen aan het datalekteam.

Hieronder volgt een nadere uitwerking van deze procedure.

2 Procedurebeschrijving

2.1 Melden incident

2.1.1 Interne medewerkers

De meldplicht datalekken geldt voor de gehele organisatie en iedere medewerker. Iedere medewerker die te maken heeft met vermissing/diefstal van zaken die van de provincie zijn, of met een informatiebeveiligingsincident, dient dit te melden bij het ICT-plein. Dit kan telefonisch via toestelnummer (070) 441 77 77 of via het meldingsformulier in het Loket op Topdesk.
Naam en contactgegevens van de melder worden automatisch in het formulier geregistreerd met de informatie over het incident. De melder kan namelijk gevraagd worden om aanvullende informatie te geven over het incident. Dit is belangrijk voor de goede en snelle afhandeling van het incident en de volledigheid voor een eventuele melding aan de AP.

2.1.2 Verwerkers van persoonsgegevens namens de provincie

Als er externe partijen zijn die in opdracht van de provincie persoonsgegevens verwerken, dan is met deze partijen een verwerkersovereenkomst gesloten, waarin is opgenomen hoe het onderlinge contact verloopt bij mogelijke datalekken. Het betreft dan vaak beveiligingsincidenten met applicaties die in het datacenter van de leverancier draaien.

2.1.3 Derden

Ook burgers of bedrijven kunnen melding doen van een mogelijk datalek bij de provincie. Op verschillende manieren kan zo'n melding de provincie bereiken. Men kan zich via de contactgegevens op de provinciale website wenden tot het Klantcontactcentrum of de provinciale functionaris gegevensbescherming. Ook is het mogelijk dat een burger of bedrijf zich eerst wendt tot de Autoriteit Persoonsgegevens. In dat geval zal de autoriteit contact opnemen met de provinciale functionaris gegevensbescherming.

De FG zal de melding registreren via het meldingsformulier in het Loket op Topdesk.

2.2 Beoordeling of er sprake is van een datalek

2.2.1 Eerste beoordeling

Zo snel mogelijk na de melding van een incident doet de adviseur informatieveiligheid (I&A) een eerste beoordeling of er sprake kan zijn van een datalek dat valt onder de meldplicht van de AVG. Als dit niet kan worden uitgesloten, formeert de adviseur informatieveiligheid het Datalekteam.

2.2.2 Formeren Datalek team

Het Datalekteam bestaat naast de adviseur informatieveiligheid, en afhankelijk van de situatie, uit: de informatiebeheerder van P&O, de privacy jurist van FJZ, de I&A incident manager, een medewerker documentaire informatie van I&A, de functioneel/technisch beheerder van het systeem, betrokken medewerker(s) en diens leidinggevende. Afhankelijk

van de beoordeling van situatie wordt de afdeling Communicatie betrokken in verband met persvoorlichting, interne en/of externe communicatie.

De adviseur informatieveiligheid informeert zo snel mogelijk telefonisch de FG.

2.2.3 Doelen en taken datalekteam

Het Datalekteam heeft als doelstelling:

- Maatregelen (laten) treffen ter beperken van verdere schade;
- Onderzoek te (laten) doen naar de oorzaak van het datalek;
- Gevolgen daarvan voor zowel de provincie Zuid-Holland als de bij het datalek betrokken personen vast te (laten) stellen;
- Acties vast te (laten) stellen voor afhandeling van het datalek en
- Uitgevoerde acties te (laten) controleren

De taken van het Datalekteam zijn:

- Vaststellen van noodzakelijke (directe) acties om de gevolgen van het datalek te beperken en in de toekomst vergelijkbare datalekken te voorkomen;
- Medewerkers van de provincie Zuid-Holland aan te sturen in de uitvoering van de noodzakelijke acties;
- Informeren van directie en bestuur;
- Zorg dragen voor besluitvorming ten aanzien van het datalek;
- (Indien noodzakelijk) interne communicatie rondom het datalek te (laten) verzorgen;
- Vaststellen van de wijze van informeren van betrokkenen (personen waarvan de gegevens bij het incident ‘gelekt’ zijn).

2.2.4 Beoordelen

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.

2.2.5 Advies

De FG gehoord hebbende stelt het datalekteam een advies op voor de concerndirecteur, belast met de bedrijfsvoering.
De concerndirecteur beoordeelt het incident en het bijgevoegde advies en besluit of er sprake is van een datalek dat gemeld moet worden aan de toezichthouder en eventueel de betrokkene(n).
Een afschrift van het advies wordt aan de FG toegezonden.
De gedeputeerde Middelen wordt geïnformeerd.

2.2.6 Melden

De adviseur informatieveiligheid is er verantwoordelijk voor dat het meldingsformulier van de toezichthouder wordt ingevuld en vervolgens wordt toegestuurd naar de toezichthouder.

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.

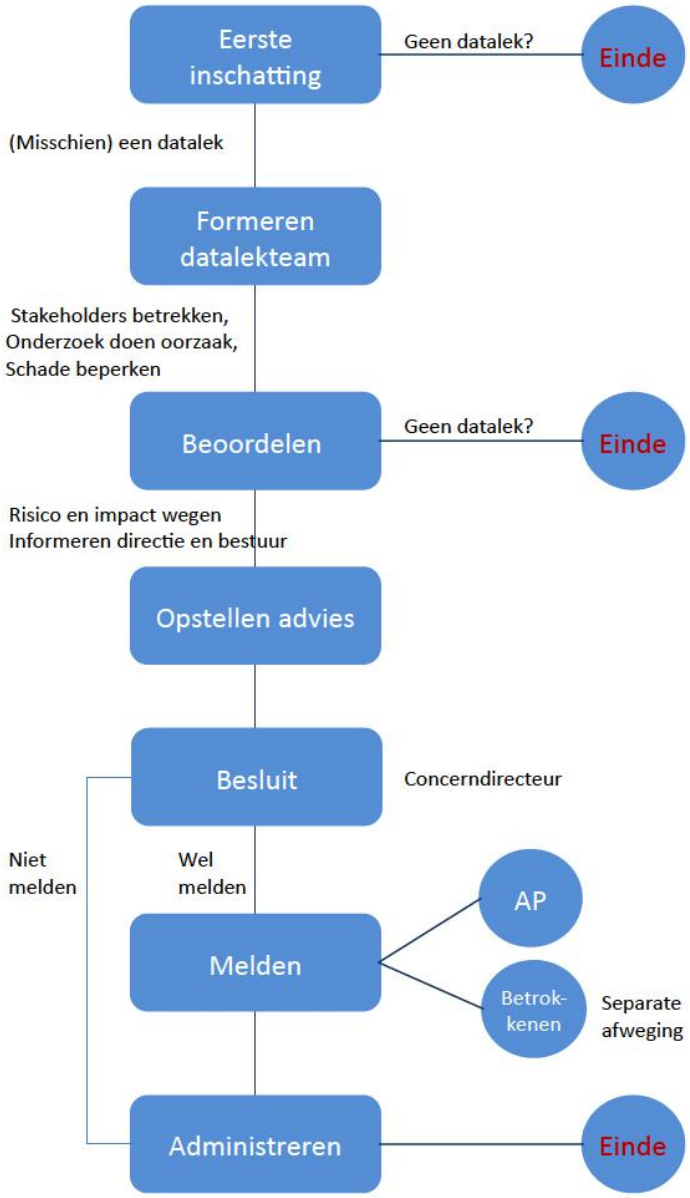
2.2.7 Administreren

De adviseur informatieveiligheid houdt een administratie bij waarin alle datalekken die zich voordoen in de organisatie geregistreerd worden. Dit betekent dat ook wanneer een lek niet gemeld hoeft te worden, er een documentatieplicht geldt.
De administratie bevat de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.

In het logboek worden in ieder geval de volgende gegevens vermeld:

a) het onderwerp van het datalek.
b) de datum van het datalek;
c) de duur van het datalek;
d) de aard van de inbreuk;
e) de instanties waar meer informatie over de inbreuk kan worden verkregen;
f) de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk gevolgen te beperken.
g) een beschrijving van de gevolgen voor de verwerkte persoonsgegevens;
h) de maatregelen die de provincie heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen;
i) de kennisgeving aan betrokkenen.

Beoordelen datalekken



In beginsel moet ieder datalek aan de **Autoriteit Persoonsgegevens (AP)** 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.

"Van: art 5 1-2e
Verzonden: 2019-10-02 16:14:51.499000+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: Memo opschonen Topdesk_
"
Hallo art 5 1-2e art 5 1-2e en art 5 1-2e

Bijgaand de concept memo over de opschoning van persoonsgegevens in Topdesk.

Graag jullie op/aanmerkingen.

Mvg, art 5 1-2e
"

provincie ZUID HOLLAND

Memo

Contact
art 5 1-2e
T 070 - 441 63 34
art 5 1-2e)pzh.nl

Datum
2 oktober 2019

Aan
MT I&A

Kopie aan
Team informatieveiligheid, art 5 1-2e

Onderwerp
Opschonen persoonsgegevens Topdesk

A
anleiding
Op 11 september is door een alerte I&A collega een (intern) datalek in Topdesk geconstateerd. Het betrof de in Topdesk ingerichte workflow indiensttreding (P&O) voor het aanmelden van nieuwe statenleden en fractiemedewerkers. Hierin worden de persoonsgegevens geregistreerd die u de provincie heeft verstrekt met oog op de salarisverwerking en het verstrekken van toegangspassen en IT-middelen.

Probleem
Voor de collega's die Topdesk behandelaar in dit proces zijn en hierbinnen een taak uit te voeren hebben, waren te veel persoonsgegevens te zien, die niet nodig zijn voor de uitvoering van de taak. Bovendien waren de persoonsgegevens ook via Topdesk inzichtelijk voor een te ruime groep Topdesk behandelaren. Deze situatie is in strijd met het op grond van de Algemene Verordening Gegevensbescherming vereiste beginselen van minimale gegevensverwerking, opslagbeperking en vertrouwelijkheid.

Na constatering zijn de persoonsgegevens uit het bewuste systeem verwijderd en 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

Gevolg
Conform de procedure voor afhandeling van datalekken is een risicoanalyse uitgevoerd. De functionaris voor gegevensbescherming, de concerndirectie, Gedeputeerde Staten en Provinciale Staten zijn geïnformeerd. Er is een officiële melding gedaan bij de Autoriteit Persoonsgegevens en de betrokken (voormalig) statenleden en fractiemedewerkers zijn per brief op de hoogte gesteld. Ook heeft dit datalek de pers gehaald en zijn er in PS statenvragen over het datalek gesteld.

Benodigde vervolgacties
In de huidige situatie is in Topdesk is de functionaliteit voor de aanmelding van statenleden en fractiemedewerkers uitgezet. Hier moet een oplossing voor gezocht worden, die wel voldoet aan de vereisten van de AVG.

provincie ZUID HOLLAND

Datum
2 oktober 2019
Ons kenmerk

Ook is op zeer korte termijn een controle nodig of de andere processen die via Topdesk worden ondersteund aan de AVG voldoen. Daar waar tekortkomingen geconstateerd worden, is direct ingrijpen nodig en dient vervolgens met de stakeholders (waaronder de proceseigenaar, Topdesk beheer, documentaire informatie, informatieveiligheid, architectuur) een alternatieve oplossing gevonden te worden.
Aandachtspunten daarbij zijn: aanpassing van het proces, aanscherping van toegangsrechten, inzet van andere systemen, borgen dat persoonsgegevens eenmalig worden opgeslagen in het juiste dossier, zorgen voor tijdige vernietiging van persoonsgegevens in Topdesk, en/of acceptatie van risico's door de proceseigenaar.

Besluitpunten
Gevraagd besluit van het MT I&A:

- Opdracht gegeven voor het per direct starten van een informatie- en procesanalyse om te borgen dat de verwerking van persoonsgegevens aan de AVG voldoet.
- Een opdrachtgever voor deze analyse aangesteld binnen het MT I&A.

"Van: art 5 1-2e
Verzonden: 2019-10-02 16:22:35.154000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019
"
Ja dat gaat lukken.

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 < art 5 1-2e pzh.nl>
Verzonden: woensdag 2 oktober 2019 16:08
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: RE: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Dank! Lukt het om deze week een eerste versie te hebben? Dan kan ik alvast gaan kijken wanneer we het Willy kunnen voorleggen.

Hartelijke groet,

art 5 1-2e

M art 5 1-2e

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

Provincie Zuid-Holland

Van: art 5 1-2e
Verzonden: woensdag 2 oktober 2019 09:30
Aan: art 5 1-2e
Onderwerp: RE: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Hoi art 5 1-2e

Hierbij vast de procedurebeschrijving.

Een concept voor de inhoudelijke beantwoording volgt later.

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 < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 1 oktober 2019 17:12
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: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

In dit geval blijf ik nog coördineren.

Fijn art 5 1-2e dat jij de inhoudelijke beantwoording oppakt. Zou je mij ook de procesbeschrijving van melding datalekken, met rollen en verantwoordelijkheden willen toesturen?

Hartelijke groet,

art 5 1-2e

M art 5 1-2e

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

Provincie Zuid-Holland

Van: art 5 1-2e
Verzonden: dinsdag 1 oktober 2019 13:55
Aan: art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Tk

Voortouw ligt bij art 5 1-2e we hadden afgesproken dat zij coördineert.

En wat de routing betreft: is aan art 5 1-2e hij is verantwoordelijk voor de datalekken. art 5 1-2e een puntje om te bespreken met hem.

Groet,

art 5 1-2e

Verzonden vanuit Mail <https://go.microsoft.com/fwlink/?LinkId=550986> voor Windows 10

Van: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 13:51
Aan: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Dag art 5 1-2e

Hier hadden we het over. Coördineer jij, zoals afgesproken?

Groet,

art 5 1-2e

Verzonden vanuit Mail <https://go.microsoft.com/fwlink/?LinkId=550986> voor Windows 10

Van: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 13:20
Aan: art 5 1-2e <mailto : art 5 1-2e pzh.nl> ; art 5 1-2e <mailto: art 5 1-2e pzh.nl>
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Hallo art 5 1-2e en art 5 1-2e

SGP/CU heeft statenvragen gesteld over het datalek.

De vragen zijn via de afd. Bestuur gerouteerd naar art 5 1-2e (FG).

Wij (art 5 1-2en het privacyteam) zijn echter van mening dat de beantwoording uit de ambtelijke lijn moet komen en niet van de FG, die adviseur en toezichthouder is.

Ik ga er dus mee aan de slag.

* Willen jullie dit a.s. maandag in het MT melden?
* art 5 1-2e misschien is de routering van dit soort vragen een onderwerp om kort met Willy de Zoete te bespreken ?

Ik stem de beantwoording af met het privacyteam en houd jullie in de loop.

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 <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 1 oktober 2019 10:20
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: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

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
Verzonden: dinsdag 1 oktober 2019 09:23
Aan: art 5 1-2e
Onderwerp: Fwd: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Hi art 5 1-2e hierbij ontvang je statenvragen over data lek. Wil je voor de beantwoording zorgdragen?

Groet, art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

---------- Forwarded message ----------
From: "" art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >
Date: Fri, Sep 27, 2019 at 4:52 PM +0200
Subject: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019
To: "" art 5 1-2e " <art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >

Beste art 5 1-2e

Hierbij nieuwe schriftelijke vragen, iets voor art 5 1-2e

Met vriendelijke groet,

art 5 1-2e

Administratief ondersteuner A

Afdeling Bestuur | Bureau Beleidscoördinatie en Advies | GS-ondersteuning

T art 5 1-2e

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

gsondersteuning@pzh.nl <mailto:gsondersteuning@pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

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


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-10-02 16:26:38.227000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019
"
Komt goed. Ik heb contact met art 5 1-2e Deze week eerste versie.

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 < art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 14:57
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: RE: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Hoi art 5 1-2e

Ik voel vertraging opkomen als ik de reactie van art 5 1-2e lees En volgens mij hebben we die tijd niet.

Ik schat dat het uiteindelijk toch op het bordje van een van ons tweeën wordt gelegd, dus hoe vliegen wij dit aan?

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
Verzonden: dinsdag 1 oktober 2019 14:16
Aan: art 5 1-2e art 5 1-2e art 5 1-2e
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

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 < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 1 oktober 2019 13:55
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: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Tk

Voortouw ligt bij art 5 1-2e we hadden afgesproken dat zij coördineert.

En wat de routing betreft: is aan art 5 1-2e Hij is verantwoordelijk voor de datalekken. art 5 1-2e een puntje om te bespreken met hem.

Groet,

art 5 1-2e

Verzonden vanuit Mail <https://go.microsoft.com/fwlink/?LinkId=550986> voor Windows 10

Van: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 13:51

Aan: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Dag art 5 1-2e

Hier hadden we het over. Coördineer jij, zoals afgesproken?

Groet,

art 5 1-2e

Verzonden vanuit Mail <https://go.microsoft.com/fwlink/?LinkId=550986> voor Windows 10

Van: art 5 1-2e <mailto : art 5 1-2e pzh.nl>
Verzonden: dinsdag 1 oktober 2019 13:20
Aan: art 5 1-2e <mailto : art 5 1-2e pzh.nl> ; art 5 1-2e <mailto: art 5 1-2e pzh.nl>
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Hallo art 5 1-2e en art 5 1-2e

SGP/CU heeft statenvragen gesteld over het datalek.

De vragen zijn via de afd. Bestuur gerouteerd naar art 5 1-2e (FG).

Wij (art 5 1-2en het privacyteam) zijn echter van mening dat de beantwoording uit de ambtelijke lijn moet komen en niet van de FG, die adviseur en toezichthouder is.

Ik ga er dus mee aan de slag.

* Willen jullie dit a.s. maandag in het MT melden?
* art 5 1-2e misschien is de routering van dit soort vragen een onderwerp om kort met Willy de Zoete te bespreken ?

Ik stem de beantwoording af met het privacyteam en houd jullie in de loop.

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 <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 1 oktober 2019 10:20
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> >
Onderwerp: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

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
Verzonden: dinsdag 1 oktober 2019 09:23
Aan: art 5 1-2e
Onderwerp: Fwd: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019

Hi art 5 1-2e hierbij ontvang je statenvragen over data lek. Wil je voor de beantwoording zorgdragen?

Groet, art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

---------- Forwarded message ----------
From: "" art 5 1-2e pzh.nl <mailto : art 5 1-2e zh.nl> >
Date: Fri, Sep 27, 2019 at 4:52 PM +0200
Subject: FW: nieuwe Schriftelijke vragen 3556 SGP CU Melding datalek 24 september 2019
To: "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >

Beste art 5 1-2e

Hierbij nieuwe schriftelijke vragen, iets voor art 5 1-2e

Met vriendelijke groet,

art 5 1-2e

Administratief ondersteuner A

Afdeling Bestuur | Bureau Beleidscoördinatie en Advies | GS-ondersteuning

T art 5 1-2e

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

gsondersteuning@pzh.nl <mailto:gsondersteuning@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>
"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-10-03 11:24:56.873000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: FW: Memo opschonen Topdesk_
"
Hoi art 5 1-2e

Heb jij hier nog op/aanmerkingen bij?

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: woensdag 2 oktober 2019 16:15
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: Memo opschonen Topdesk_

Hallo art 5 1-2e art 5 1-2e en art 5 1-2e

Bijgaand de concept memo over de opschoning van persoonsgegevens in Topdesk.

Graag jullie op/aanmerkingen.

Mvg, art 5 1-2e
"

provincie ZUID HOLLAND

Memo

Contact
art 5 1-2e
T art 5 1-2e
art 5 1-2e pzh.nl

Datum
2 oktober 2019

Aan
MT I&A

Kopie aan
Team informatieveiligheid, art 5 1-2e

Onderwerp
Opschonen persoonsgegevens Topdesk

A
anleiding
Op 11 september is door een alerte I&A collega een (intern) datalek in Topdesk geconstateerd. Het betrof de in Topdesk ingerichte workflow indiensttreding (P&O) voor het aanmelden van nieuwe statenleden en fractiemedewerkers. Hierin worden de persoonsgegevens geregistreerd die u de provincie heeft verstrekt met oog op de salarisverwerking en het verstrekken van toegangspassen en IT-middelen.

Probleem
Voor de collega's die Topdesk behandelaar in dit proces zijn en hierbinnen een taak uit te voeren hebben, waren te veel persoonsgegevens te zien, die niet nodig zijn voor de uitvoering van de taak. Bovendien waren de persoonsgegevens ook via Topdesk inzichtelijk voor een te ruime groep Topdesk behandelaren. Deze situatie is in strijd met het op grond van de Algemene Verordening Gegevensbescherming vereiste beginselen van minimale gegevensverwerking, opslagbeperking en vertrouwelijkheid.

Na constatering zijn de persoonsgegevens uit het bewuste systeem verwijderd en 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

Gevolg
Conform de procedure voor afhandeling van datalekken is een risicoanalyse uitgevoerd. De functionaris voor gegevensbescherming, de concerndirectie, Gedeputeerde Staten en Provinciale Staten zijn geïnformeerd. Er is een officiële melding gedaan bij de Autoriteit Persoonsgegevens en de betrokken (voormalig) statenleden en fractiemedewerkers zijn per brief op de hoogte gesteld. Ook heeft dit datalek de pers gehaald en zijn er in PS statenvragen over het datalek gesteld.

Benodigde vervolgacties
In de huidige situatie is in Topdesk is de functionaliteit voor de aanmelding van statenleden en fractiemedewerkers uitgezet. Hier moet een oplossing voor gezocht worden, die wel voldoet aan de vereisten van de AVG.

provincie ZUID HOLLAND

Datum
2 oktober 2019
Ons kenmerk

Ook is op zeer korte termijn een controle nodig of de andere processen die via Topdesk worden ondersteund aan de AVG voldoen. Daar waar tekortkomingen geconstateerd worden, is direct ingrijpen nodig en dient vervolgens met de stakeholders (waaronder de proceseigenaar, Topdesk beheer, documentaire informatie, informatieveiligheid, architectuur) een alternatieve oplossing gevonden te worden.
Aandachtspunten daarbij zijn: aanpassing van het proces, aanscherping van toegangsrechten, inzet van andere systemen, borgen dat persoonsgegevens eenmalig worden opgeslagen in het juiste dossier, zorgen voor tijdige vernietiging van persoonsgegevens in Topdesk, en/of acceptatie van risico's door de proceseigenaar.

Besluitpunten
Gevraagd besluit van het MT I&A:

- Opdracht gegeven voor het per direct starten van een informatie- en procesanalyse om te borgen dat de verwerking van persoonsgegevens aan de AVG voldoet.
- Een opdrachtgever voor deze analyse aangesteld binnen het MT I&A.


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-10-03 11:34:55.524000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: memo over opschonen persoonsgegevens in idms
"
Hallo art 5 1-2e

Bij nader inzien wil ik de (derde) memo over opschonen persoonsgegevens in idms voor het MT laten vervallen.

In de startnotitie iDMS is dat onderwerp al voldoende beschreven (zie onder).

De enige toevoeging zou zijn dat dit urgent is, maar dat kan ik ook met art 5 1-2e bespreken en zien hoe we dit in gang kunnen zetten. Ik heb morgen een afspraak met haar.

Mocht het dan in de knel komen ten opzichte van andere onderwerpen, dan kunnen we dat alsnog aan het MT voorleggen.

Mvg, art 5 1-2e

Uit de startnotitie:

Persoonsgegevens (AVG)

De AVG stelt eisen aan de afscherming van persoonsgegevens, ook in iDMS. Het moet duidelijk zijn welke persoonsgegevens in iDMS zijn opgeslagen en wat daarvoor de wettelijke grondslag is. Ook mag niet iedereen documenten met persoonsgegevens inzien en moet aantoonbaar zijn wie dat kunnen en wie niet.

Gebleken is dat er in iDMS veel breed toegankelijke persoonsgegevens zijn opgeslagen, variërend van kopie identiteitsbewijzen tot verslagen van voortgangsgesprekken en zienswijzen. Dit is niet vreemd, omdat we uit een langdurige periode komen waarin er geen aandacht was voor de bescherming van persoonsgegevens. Maar desalniettemin voldoet deze situatie niet aan de regelgeving van de Algemene Verordening Gegevensbescherming (AVG).

Voor een ander deel van de bevindingen kunnen we direct in de doe-modus schieten. Sterker, daar lopen al activiteiten. Met een combinatie van scherpere beheerafspraken, betere monitoring en instructie van gebruikers komen we een heel eind:

* Vervuiling:
  Zet slimme ai-zoekmogelijkheden om te zoeken naar duplicaten, hernoemde kopieën, eerdere werkversies van documenten. Benader eigenaren en ruim op. Instrueer en communiceer.
* Persoonsgegevens (AVG): idem.

Aanbevelingen

1. Laat een plan maken om de korte termijn verbeteringen uit te voeren en door te zetten.

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

"Van: art 5 1-2e
Verzonden: 2019-10-03 16:28:51.430000+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e
Onderwerp: RE: Stukken voor MT 7 oktober
"
Dit zijn de goede versies

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: donderdag 3 oktober 2019 16:00
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: Stukken voor MT 7 oktober

Hallo art 5 1-2e

Hierbij de stukken voor a.s. maandag.

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

provincie ZUID HOLLAND

Memo

Contact
art 5 1-2e
T art 5 1-2e
art 5 1-2e pzh.nl

Datum
2 oktober 2019

Aan
MT I&A

Kopie aan en afgestemd met:
Team informatieveiligheid, art 5 1-2e, art 5 1-2e
art 5 1-2e art 5 1-2e (FG), art 5 1-2e (P&O)

Onderwerp
AVG-proof maken Topdesk

A
anleiding

Op 11 september is door een alerte I&A collega een datalek in Topdesk geconstateerd.
Het betrof de in Topdesk ingerichte workflow indiensttreding (P&O) voor het aanmelden van nieuwe statenleden en fractiemedewerkers. Hierin worden de persoonsgegevens geregistreerd die zij de provincie hebben verstrekt met oog op de salarisverwerking en het verstrekken van toegangspassen en IT-middelen.

Probleem

Voor de collega's die Topdesk behandelaar in dit proces zijn en hierbinnen een taak uit te voeren hebben, waren te veel persoonsgegevens te zien, die niet nodig zijn voor de uitvoering van de taak. Bovendien waren de persoonsgegevens via Topdesk ook inzichtelijk voor een te ruime groep Topdesk behandelaren. Deze situatie is in strijd met de op grond van de Algemene Verordening Gegevensbescherming vereiste beginselen van minimale gegevensverwerking, opslagbeperking en vertrouwelijkheid.

Na constatering zijn de persoonsgegevens uit het bewuste systeem verwijderd en 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

Gevolg

Conform de procedure voor afhandeling van datalekken is een risicoanalyse uitgevoerd. De functionaris voor gegevensbescherming, de concerndirectie, Gedeputeerde Staten en Provinciale Staten zijn geïnformeerd. Er is een officiële melding gedaan bij de Autoriteit Persoonsgegevens en de betrokken (voormalig) statenleden en fractiemedewerkers zijn per brief op de hoogte gesteld. Dit datalek heeft de pers gehaald en er zijn in PS statenvragen over het datalek gesteld.

Benodigde vervolgacties

In de huidige situatie is in Topdesk de functionaliteit voor de aanmelding van statenleden en fractiemedewerkers uitgezet. Hier moet een oplossing voor gezocht worden, die wel voldoet aan de vereisten van de AVG.

provincie ZUID HOLLAND

Datum
2 oktober 2019
Ons kenmerk

Ook is op zeer korte termijn een controle nodig of de andere processen die via Topdesk worden ondersteund aan de AVG voldoen. Daar waar tekortkomingen geconstateerd worden, is direct ingrijpen nodig en dient vervolgens met de stakeholders binnen P&O, FZ en I&A (waaronder de proceseigenaar, Topdesk beheer, documentaire informatie, informatieveiligheid, architectuur) een alternatieve oplossing gevonden te worden.
Aandachtspunten daarbij zijn: aanpassing van het proces, aanscherping van toegangsrechten, inzet van andere systemen, borgen dat persoonsgegevens eenmalig worden opgeslagen in het juiste dossier, zorgen voor tijdige vernietiging van persoonsgegevens in Topdesk, en/of acceptatie van risico's door de proceseigenaar.

Besluitpunten
Gevraagd besluit van het MT I&A:

- Opdracht gegeven voor het per direct starten van bovengenoemde activiteiten via het informatiemanagement proces via de Verkenningstafel.
- Een opdrachtgever voor deze analyse aangesteld binnen het MT I&A.

provincie ZUID HOLLAND

Memo

Contact
art 5 1-2e
T art 5 1-2e
art 5 1-2e pzh.nl

Datum
2 oktober 2019

Bijlage: Beantwoording statenvragen 3543 PVV

Aanleiding

Het SIDN fonds[1] heeft de totstandkoming van de Faalkaart gesteund. De Faalkaart is een website[2] met een geografische kaart die met stoplichtkleuren aangeeft of de websites en externe netwerkdiensten van lokale overheden en provincies qua online veiligheid op orde zijn. De insteek is dat het falen wordt verholpen, zodra dit inzichtelijk wordt gemaakt. Op de Faalkaart is te zien dat Zuid-Holland ten opzichte van andere provincies slecht scoort.
Naar aanleiding van een artikel over de Faalkaart in Binnenlands Bestuur heeft de PVV statenvragen gesteld, waarin ernstige zorgen zijn geuit over "de veiligheid van de ICT-systemen van de provincie". De beantwoording van de statenvragen is als bijlage bij deze memo gevoegd.

In de beantwoording van de statenvragen wordt duiding gegeven aan de resultaten van de Faalkaart. Kort gezegd kloppen niet alle vermeldingen, wat echter niet wegneemt dat er nog steeds veel websites wél terecht worden vermeld. Ook wordt in de beantwoording onderscheid gemaakt tussen de corporate website van de provincie (www.zuid-holland.nl) en het veelvoud aan andere websites die divers van aard zijn. Op deze websites wordt bijvoorbeeld informatie verstrekt over specifieke onderwerpen (zoals het coalitieakkoord, de begroting en archeologie) en er worden bijvoorbeeld filmpjes, foto's of kaarten getoond.

Probleemstelling

De corporate website is in beheer bij I&A. De beveiliging van de website wordt jaarlijks gecontroleerd en is in orde. Het probleem ligt bij de categorie andere websites, die in veel gevallen zonder betrokkenheid van I&A vanuit de vakafdelingen of vanuit opgaven tot stand zijn gekomen. Het zijn deze websites die (deels) niet voldoen aan verplichte beveiligingsstandaarden en die er in de Faalkaart voor zorgen dat Zuid-Holland slecht scoort. I&A heeft geen volledige registratie van welke websites er op deze manier tot stand zijn gekomen. De Faalkaart noemt er een aantal, maar er bestaan bijvoorbeeld binnen I&A en de afdeling Communicatie deels aanvullende en deels overlappende overzichten. Het volledige beeld van websites waar onze organisatie haar naam aan heeft verbonden ontbreekt.

Kortom: op dit moment heeft de provincie dus veel verschillende websites die niet voldoen aan de verplichte beveiligingsstandaarden. Er zijn vanuit de provincie verschillende opdrachtgevers en deze websites worden door verschillende externe partijen gehost. Er is binnen de provincie geen volledig overzicht welke websites het betreft. Wel is het nodig dat al deze websites veilig gemaakt worden of – met onderbouwing – door de opdrachtgever als risico wordt geaccepteerd.

Benodigde vervolgacties

De maatschappelijke en politieke aandacht op dit onderwerp geeft voldoende urgentie om dit op zeer korte termijn voor elkaar te brengen.
De volgende activiteiten worden voorgesteld:

- Uitvoeren van een organisatiebrede inventarisatie van provinciale websites (en opdrachtgevers) waarvoor de provincie opdrachtgever is.

1 Het SIDN fonds is opgericht door de Stichting Internet Domeinregistratie Nederland (SIDN)
2 https://basisbeveiliging.nl/#info

provincie ZUID HOLLAND

Datum
2 oktober 2019
Ons kenmerk

- In afstemming met de de provinciale opdrachtgevers er voor zorgen dat deze websites voldoen aan de verplichte beveiligingsstandaarden, als eerste te beginnen met de in de Faalkaart genoemde websites.
- Afstemmen met de afdeling Communicatie over een gezamenlijke aanpak (zie opmerking hieronder)

NB: Binnen de afdeling Communicatie is de ambitie ‘corporate website, tenzij’ geformuleerd en loopt een project voor de vernieuwing van het digitaal platform Zuid-Holland onder het adagium: Corporate website, tenzij. De bedoeling is om consistentie te krijgen in de digitale uitingen van de provincie en ook om alle websites op hetzelfde kwaliteitsniveau (waaronder informatiebeveiliging) te brengen. I&A is hier al betrokken en het ligt voor de hand om de verbinding te versterken en met elkaar vast te stellen wat het gemeenschappelijke scope, doel en tijdpad is.

Besluitpunten
Gevraagd besluit van het MT I&A:

- Opdracht gegeven voor het per direct starten van bovengenoemde activiteiten via het informatiemanagement proces via de Verkenningstafel.
- Een opdrachtgever voor deze analyse aangesteld binnen het MT I&A.

Antwoord

van Gedeputeerde Staten
op vragen van
J. Mooiman (PVV)
(d.d. 23 augustus 2019)

Nummer
3543

Onderwerp
Grote zorgen veiligheid ICT systemen Provincie Zuid-Holland

Aan de leden van Provinciale Staten

Toelichting vragensteller
Uit een bericht van Binnenlands Bestuur (*) komt naar voren dat uit de op basisbeveiliging.nl staande Faalkaart blijkt dat het over het algemeen slecht is gesteld met de veiligheid van ICT van Nederlandse gemeenten en provincies.

Tot schrik van de PVV zijn de resultaten voor de Provincie Zuid-Holland zwaar onvoldoende. 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. (**)

Het doel van de genoemde website is om de beveiliging en privacy voor o.a. provincies te verbeteren, en hoogleraar art 5 1-2e *Universiteit Twente) is van mening dat de Faalkaart een goed instrument ka de overheids -ICT te verbeteren. De waarde van de Faalkaart wordt ook door het SIDN fonds onderschreven, opgericht door de Stichting Internet Domeinregistratie Nederland, de autoriteit die het .nl domein beheert.*

Hoogleraar art 5 1-2e *oonde onlangs ook al aan dat de cruciale digitale infrastructuur van Nederland kwetsbaar is en dat o.a. het kennisniveau van Nederlandse politici over ICT tekort schiet. (***)*

De PVV Zuid-Holland maakt zich grote zorgen over de staat waarin de veiligheid van de Zuid-Hollandse ICT zich bevindt met alle gevolgen van dien voor onze burgers, ondernemers en provinciale overheid en stellen daarom de volgende vragen aan Gedeputeerde Staten:

1. *Bent u bekend met de zogenoemde Faalkaart en deelt u de mening dat de resultaten voor de Provincie Zuid-Holland zéér zorgwekkend zijn? Zo nee, waarom niet?*

Antwoord
GS hebben kennisgenomen van de Faalkaart, vinden het belangrijk dat tekortkomingen waar nodig worden gerepareerd, maar zijn niet van mening dat de

resultaten zéér zorgwekkend zijn voor de veiligheid van de IT systemen van de provincie.

De provinciale ‘corporate’ website

De Faalkaart heeft betrekking op provinciale websites. De primaire ‘corporate’ website van de provincie Zuid-Holland is www.zuid-holland.nl. Via deze website wordt belangrijke informatie over de provincie verstrekt. Ook de besluiten van PS en GS zijn hierop te vinden. Deze website is een zogenaamde *transactiewebsite*. Als enige provinciale website vindt hier interactie met burgers en bedrijven plaats in de vorm van digitale contact- en aanvraagformulieren. Deze formulieren worden vanaf de website geautomatiseerd verwerkt naar de interne ICT-systemen van de provincie. Mede door deze koppeling is het risicoprofiel voor deze website hoger dan voor andere provinciale websites

De veiligheid van de corporate website wordt jaarlijks op een aantal manieren getoetst. Ten eerste laat de afdeling Informatisering en Automatisering van de provincie jaarlijks beveiligingsonderzoeken op deze website uitvoeren. Daarnaast toetst het Forum Standaardisatie jaarlijks of deze website aan verplichte beveiligingsstandaarden voor de publieke sector voldoet. Het Forum Standaardisatie is opgericht door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en onderhoudt de lijst met verplichte open standaarden voor de publieke sector en toetst de toepassing ervan. In de meest recente meting van maart 2019 is geconstateerd dat www.zuid-holland.nl aan alle verplichte internetstandaarden voldoet.
NB: In onderstaande tabel wordt ook het www.pzh.nl vermeld. Dit is echter geen publiek toegankelijke webadres. De bezoeker die dit webadres intypt, wordt naar de veilige zuid-holland.nl website geleid. In de volgende paragraaf wordt uitgelegd waarom dit bij een geautomatiseerde test tot verkeerde constateringen kan leiden.

Resultaten web provincies

Domeinnaam	DNSSEC	HSTS	HTTPS Afgedwongen	TLS	TLS NCSC
provincie.drenthe.nl	WAAR	WAAR	ONWAAR	WAAR	WAAR
www.bij12.nl	WAAR	ONWAAR	WAAR	WAAR	WAAR
www.brabant.nl	WAAR	ONWAAR	WAAR	WAAR	ONWAAR
www.drenthe.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.flevoland.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.fryslan.frl	WAAR	WAAR	WAAR	WAAR	WAAR
www.fryslan.nl	WAAR	ONWAAR	ONWAAR	ONWAAR	ONWAAR
www.gelderland.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.ipo.nl	ONWAAR	ONWAAR	WAAR	WAAR	WAAR
www.limburg.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.noord-holland.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.overijssel.nl	WAAR	WAAR	ONWAAR	WAAR	WAAR
www.provincie-utrecht.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.provinciegroningen.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.prvlimburg.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.pzh.nl	WAAR	ONWAAR	ONWAAR	ONWAAR	ONWAAR
www.zeeland.nl	WAAR	WAAR	WAAR	WAAR	WAAR
www.zuid-holland.nl	WAAR	WAAR	WAAR	WAAR	WAAR

Meting informatieveiligheidstandaarden maart 2019

Tot slot zijn alle organisaties die DigiD op hun website gebruiken – waaronder de provincie – verplicht te voldoen aan een zware beveiligingsnorm. Via een jaarlijks

provincie ZUID HOLLAND

ICT-beveiligingsassessment ziet Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, hierop toe. Ook in 2019 heeft Logius aan onze provincie goedkeuring verleend.

Overige provinciale websites
Naast de corporate website beschikt de provincie over een veelvoud van andere websites die divers van aard zijn. Hierop wordt informatie verstrekt over specifieke onderwerpen (zoals het coalitieakkoord, de begroting en archeologie) en er worden bijvoorbeeld filmpjes, foto's of kaarten getoond. Kenmerkend is dat er geen transacties plaatsvinden, er wordt geen DigiD gebruikt en er bestaat geen verbinding tussen de website en de interne ICT-systemen in de provinciale datacenters. Het risicoprofiel van dit soort websites is lager.

Om die reden zijn binnen de overheid de streefbeeldafspraken over de toepassing van de informatieveiligheidsstandaarden voor websites de afgelopen jaren juist gericht geweest op de transactiewebsites van de overheid (zoals www.zuid-holland.nl). Dit zijn afspraken die in het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) zijn vastgesteld en die jaarlijks worden getoetst door het Forum Standaardisatie.
Desalniettemin is de afspraak op dit moment dat (sinds einde 2018) álle overheidswebsites moeten voldoen aan een aantal beveiligingsstandaarden. De Faalkaart laat zien dat dit voor deze categorie provinciale websites nog niet in alle gevallen zo is.

Duiding
Op dit moment heeft de provincie veel verschillende websites. Dit compliceert om consistentie te krijgen in haar digitale uitingen en ook om alle websites op hetzelfde kwaliteitsniveau te brengen. De provincie heeft hier aandacht en streeft ernaar om alle websites te laten voldoen aan het hierboven genoemde afsprakenstelsel.

Er is vanuit de Faalkaart geen contact met de provincie Zuid-Holland geweest over de wijze van testen en het beoordelen van de resultaten. Dit maakt het voor de provincie lastig om de in de Faalkaart genoemde tekortkomingen exact te duiden. Dit komt omdat er meerdere redenen kunnen zijn waarom een dergelijke geautomatiseerde test bij een website een foutmelding oplevert en daardoor plaatsing op de Faalkaart. Een eerste controle (na de publicatie van de Faalkaart) van de testresultaten door de afdeling Informatisering & Automatisering van de province, laat zien dat bij circa een kwart van de websites de genoemde tekortkomingen niet (meer) worden aangetroffen of dat een andere oorzaak heeft geleid tot een vermelding op de Faalkaart.

2. *Wat is en wordt door de provincie ondernomen om de ICT-omgeving zo veilig mogelijk te maken voor onze burgers, ondernemers en provinciale overheid? Graag een gemotiveerd antwoord.*

Antwoord
Op dit moment heeft de provincie veel verschillende websites. Dit compliceert om consistentie te krijgen in haar digitale uitingen en ook om alle websites op hetzelfde kwaliteitsniveau te brengen.

provincie ZUID HOLLAND

Daarom is binnen onze provincie de ambitie ‘corporate website, tenzij’ geformuleerd, waarbij de corporate website altijd het eerste uitgangspunt is, tenzij het om een project gaat waar de provincie een van de vele deelnemers is en niet de trekker. Dit wordt verder uitgewerkt bij de vernieuwing van het digitaal platform Zuid-Holland, waarbij de provincie streeft naar kwaliteit op het gebied van informatieveiligheid, gebruiksvriendelijkheid, actualiteit, toegankelijkheid, leesbaarheid en vindbaarheid.

3. *Welke (aanvullende) maatregelen mogen wij van u verwachten n.a.v. de bijzonder zorgwekkende cijfers voor de Provincie Zuid-Holland? Graag een gemotiveerd antwoord.*

Antwoord
De provincie is voornemens om in 2023 aantoonbaar te voldoen aan de ISO27001 norm voor beheersing van informatieveiligheid met risicomanagement als vertrekpunt. In de tweede helft van 2019 worden hiervoor de eerste plannen gemaakt en concrete stappen gezet.

4. *Wat wordt door de Provincie en eventuele partners ondernomen om het kennisniveau inzake ICT veiligheid van de provinciale overheid (politici, bestuurders, ambtenaren en gezien haar rol ook de griffie) op pijl te houden en waar mogelijk verder te vergroten?*

Antwoord
Informatieveiligheid is een onderwerp dat regelmatig op de agenda staat van het portefeuilleoverleg met de gedeputeerde. Voor de provinciale organisatie is begin 2019 een bewustwordingscampagne (Up-to-data) gestart met informatie en activiteiten rond informatieveiligheid, privacy en informatiebeheer. Vorige week onder meer een bijeenkomst met een hacker. De bewustwordingscampagne heeft een continu karakter en zal de komende jaren voortduren.

Uit een bericht van Trouw (****) blijkt dat de gemeente Den Haag eind november 2018 een wedstrijd met prijzenpot organiseerde voor ethische hackers om een dag lang de Haagse systemen te hacken.

De hackers vonden maar liefst 62 zwakke plekken in de Haagse systemen, waarvan 10 vielen in de categorie “hoge impact” en 1 zelfs zo ernstig was dat een systeem direct moest worden uitgezet. De wedstrijd was daarmee erg “succesvol” en goedkoper dan het inhuren van een bedrijf om hetzelfde werk te doen.

5. *Deelt u de mening dat het regelmatig controleren van de provinciale systemen op zwakke plekken van groot belang is om de veiligheid van gevoelige informatie zo goed mogelijk op peil te houden? Zo ja, bent u bereid in navolging van de gemeente Den Haag een soortgelijke activiteit te organiseren voor ethische hackers? Zo nee, waarom niet?*

Antwoord
Ja, wij zijn van mening dat regelmatige controle belangrijk is. De in de Faalkaart genoemde websites maken echter een beperkt deel uit van de provinciale informatiesystemen en bevatten openbare informatie. Er is hier geen sprake van bedreiging van de veiligheid van gevoelige informatie.

provincie ZUID HOLLAND

De provincie neemt continu maatregelen om de veiligheid van de informatie¬voorziening te waarborgen en net als de gemeente den Haag maakt de provincie gebruik van ethische hackers. De provincie zet hen al enige jaren in op contractbasis.

Den Haag, 24 september 2019

Gedeputeerde Staten van Zuid-Holland,
secretaris, voorzitter,

drs. H.M.M. Koek drs. J. Smit

BRON

(*) https://www.binnenlandsbestuur.nl/digitaal/nieuws/faalkaart-toont-kwetsbaarheid-ict-overheden.10559222.lynkx

(**) https://basisbeveiliging.nl/#report-zuid-holland

(***) https://www.binnenlandsbestuur.nl/digitaal/nieuws/belangrijke-nederlandse-ict-infrastructuur-is.10414668.lynkx

(****) https://www.trouw.nl/nieuws/den-haag-laat-zich-bewust-hacken-een-stuk-goedkoper-dan-een-bedrijf-inhuren~bd68f62c/?referer=https%3A%2F%2Fwww.google.nl%2F

"Van: art 5 1-2e
Verzonden: 2019-10-04 16:29:12.466000+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: FW: Concept beantwoording statenvragen 3556
"
Hallo allen,

Graag jullie op- en aanmerkingen op dit concept.

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 4 oktober 2019 16:26
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: FW: Concept beantwoording statenvragen 3556

Hallo art 5 1-2e

Zoals afgesproken stuur ik je bijgaand het eerste concept van de beantwoording.

Ligt ook nog ter review bij het privacyteam.

Zorg jij voor afstemming met art 5 1-2e en Willy?

Ik hoor graag wat de verdere tijdlijn wordt en of eventueel uitstel voor beantwoording gevraagd wordt.

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 4 oktober 2019 16:22
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: Concept beantwoording statenvragen 3556

""DOS-2019-0007559 Statenvragen 3556 CU SGP - Melding datalek 24 september 2019"" kan via de volgende koppeling worden geopend:
http://idms/otcs/llisapi.dll/properties/710313250
<http://idms/otcs/llisapi.dll/properties/710313250>

Hallo art 5 1-2e

Bijgaand de concept beantwoording van de statenvragen. Ligt ook nog voor afstemming bij het privacyteam.Ik stuur deze ook vast door aan art 5 1-2e

Misschien goed om deze nog bij de stukken voor het MT a.s. maandag te doen, omdat daar de statenvragen al op de agenda staan?

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

ANTWO

VAN GEDEPUTEERDE STATEN OP VRAGEN VAN

A. Witte (CU SGP)
(D.d. 27 september 2019)

Nummer
3556

Onderwerp
Melding datalek 24 september 2019

Aan de leden van Provinciale Staten

Toelichting vragensteller
Op 24 september hebben een aantal leden van Provinciale Staten een brief ontvangen over een datalek in één van de provinciale systemen. Een alerte medewerker heeft op 11 september 2019 het datalek gemeld. Deze medewerker kon meer gegevens inzien dan voor de functie noodzakelijk. Na onderzoek bleek dat een andere groep van 406 behandelaren ook "zij het met wat meer moeite" meer gegevens kon inzien dan noodzakelijk. De provincie heeft zowel een melding gedaan bij de Autoriteit Persoonsgegevens als de betrokkenen middels een brief van 24 september op de hoogte gebracht. De provincie heeft dit datalek inmiddels 'gedicht'.

Volgens de Autoriteit Personeelsgegevens (website; geraadpleegd 27 september 2019) is de meldplicht afhankelijk van de (potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van betrokkenen. "U hoeft een datalek niet te melden als het niet waarschijnlijk is dat het datalek leidt tot een risico voor de rechten en vrijheden van betrokkenen." De website van de Autoriteit Persoonsgegevens vermeld verder dat de betrokkenen (de personen van wie u gegevens verwerkt) alleen geïnformeerd hoeven te worden als "een datalek waarschijnlijk een hoog risico voor hun rechten en vrijheden oplevert."

1. *Aan hoeveel betrokken personen is de brief van 24 september verstuurd? Op hoeveel personen heeft dit datalek in totaal betrekking? Om welke groep(en) van personen gaat het?*

Antwoord:
Er zijn brieven verstuurd aan de 42 personen wiens persoonsgegevens het betreft. Het zijn actieve en voormalige statenleden en fractiemedewerkers.

2. *Welke gegevens van deze personen konden door daartoe onbevoegde medewerkers van de ambtelijke organisatie worden ingezien? Hoe lang heeft dit datalek bestaan?*

Antwoord:
Het betreft persoonsgegevens die de betrokkenen aan de provincie hebben verstrekt met oog op de salarisverwerking en het verstrekken van toegangspassen en IT-

middelen. Deze werkwijze is gevolgd in de periode 16-02-2016 tot 27-08-2019, toen de laatste aanvraag is verwerkt.

3. *GS geeft aan dat het niet bekend is hoeveel medewerkers onbevoegd informatie heeft ingezien. Logt het systeem niet wie welke gegevens inziet? Zo nee, waarom niet?*

Antwoord:
Het betreft een door de provincie aangeschaft standaard systeem van een van de marktleiders op het gebied van digitale ondersteuning van servicemanagement processen. Het is bedoeld voor het registreren en routeren van aanvragen en ondersteunt de afhandeling ervan. Het systeem registreert welke wijzigingen er tijdens de afhandeling van een aanvraag door wie worden aangebracht. Het systeem voorziet niet in een logging van personen die gegevens inzien zonder daar wijzigingen in aan te brengen.

4. *Hoe en op welke termijn, na hoeveel tijd, zijn door de medewerker, zijn afdelingshoofd, de functionaris gegevens bescherming, de concerndirectie, gedeputeerde staten, de Autoriteit Persoonsgegevens en uiteindelijk de betrokkenen op de hoogte gesteld? Wat is de tijdlijn? Kunt u in deze tijdlijn ook de maatregelen meenemen en om het lek te stoppen en de genomen maatregelen om de schade te beperken.*

Antwoord:
De tijdlijn is als volgt geweest:

Actie	Toelichting
Melding door de medewerker	Op 11-09-2019 per e-mail aan collega's. Dit is door afwezigheid van deze collega's niet direct opgemerkt. Op 16-09-2019 heeft de medewerker via het Datalekformulier gemeld, waarna direct de procedure voor het afhandelen van datalekken is gestart.
Inlichten afdelingshoofd	16-09-2019
Inlichten functionaris voor gegevensbescherming	16-09-2019
Inlichten concerndirectie	16-09-2019
Inlichten gedeputeerde staten	16-09-2019 (gedeputeerde) 19-09-2019 (door gedeputeerde aan GS)
Maatregelen om het lek te stoppen	16-09-2019 Alle aanvragen zijn uit het systeem verwijderd en kunnen niet meer worden ingezien. De digitale aanmeldingsprocedure is gedeactiveerd. Er zijn procesafspraken gemaakt over de afhandeling van eventuele nog komende tussentijdse aanmeldingen. Tot er een oplossing is, zal dit tijdelijk niet via het systeem worden uitgevoerd.

Actie	Toelichting
Melding bij de Autoriteit Persoonsgegevens	18-09-2019
Brief aan de betrokkenen	24-09-2019
Maatregelen om de schade te beperken	Om de betrokkenen in staat te stellen de nodig voorzorgsmaatregelen te nemen, zijn zij per brief geïnformeerd. In de brief wordt geadviseerd om alert te zijn op signalen van identiteitsfraude of ander misbruik van persoonsgegevens. Ook worden in de brief contactgegevens vermeld voor het stellen van vragen.

5. *Is er bij dit datalek binnen de wettelijke termijnen gehandeld? Zo nee, waarom niet?*

Antwoord:
De Algemene Verordening Gegevensbescherming (AVG) schrijft voor dat de verwerkingsverantwoordelijke een inbreuk in verband met persoonsgegevens ('datalek') meldt zonder onredelijke vertraging en indien mogelijk uiterlijk binnen 72 uur nadat hij er kennis van heeft genomen. De datalekprocedure is gestart op 16-09-2019 en de melding aan de Autoriteit Persoonsgegevens is gedaan op 18-09-2019. Dit is binnen 72 uur nadat kennis is genomen van het datalek.

6. *Hoe is de ernst van dit datalek gekwalificeerd? Welke 'rechten en vrijheden' van personen zijn bij dit datalek in het geding?*

Antwoord:
In deze situatie is geoordeeld de persoonsgegevens gezien hun aard gebruikt zouden kunnen worden bij vormen van (identiteits)fraude.

7. *Hoe is GS op grond van de inschatting van de 'ernst' van het datalek en de hoogte van het risico (zie vraag 6) tot de conclusie gekozen om: 1] een officiële melding bij de Autoriteit Persoonsgegevens te doen en 2] de betrokkenen over het datalek te informeren? Graag op beide onderdelen van deze vraag een apart gemotiveerd antwoord.*

Antwoord:
1. Volgens het afwegingskader van de AVG is melding van een datalek aan de Autoriteit Persoonsgegevens nodig als er (a) sprake is een beveiligingsincident en (b) onrechtmatige verwerking redelijkerwijs niet is uit te sluiten.
   In dit geval is geoordeeld dat:
   (a) er sprake was van een beveiligingsincident, aangezien de vertrouwelijkheid van persoonsgegevens in dit aanmeldingsproces niet voldoende was geborgd. Namelijk, ook een aantal provinciemedewerkers die het systeem gebruiken voor andere ondersteunende taken dan de aanmelding van statenleden en fractiemedewerkers, konden potentieel kennis nemen van de betreffende persoonsgegevens.

(b) onrechtmatige verwerking redelijkerwijs niet was uit te sluiten, omdat er geen logbestanden aanwezig zijn op basis waarvan was uit te sluiten dat daadwerkelijk provinciemedewerkers onterecht kennis hebben genomen van de persoonsgegevens.

2. Op grond van de AVG dient de provincie dient de provincie aan betrokkenen mede te delen dat er sprake is geweest van een datalek, wanneer is vastgesteld dat het datalek waarschijnlijk een hoog risico voor betrokkenen inhoudt.
In dit geval is geoordeeld dat de persoonsgegevens gezien hun aard mogelijk gebruikt kunnen worden bij vormen van (identiteits)fraude én dat op grond van logging niet is uit te sluiten dat de persoonsgegevens door te veel provinciemedewerkers in zijn gezien. Ondanks ons vertrouwen in de provinciale medewerkers en de verwachting dat zij zich integer gedragen, is besloten om betrokkenen per brief te informeren.

8. *Welke leerpunten trekt GS uit dit datalek over de beveiliging van persoonsgegevens in de andere provinciale systemen?*

Antwoord:
Het optreden van dit datalek toont aan dat er continu aandacht nodig blijft voor het zorgvuldige omgaan met persoonsgegevens. Zowel in systemen die de provincie al meerdere jaren gebruikt als bij de aanschaf en inrichting van nieuwe systemen en het in gebruik nemen van nieuwe technologieën. We zetten de lijn door die we ingezet hebben. Daarbij is het bemoedigend dat onze aandacht voor bewustwording op dit onderwerp geleid heeft tot alertheid bij provinciale medewerkers, zoals in dit geval.
VERDER AANVULLEN

Den Haag, @ oktober 2019

Gedeputeerde Staten van Zuid-Holland,
secretaris, voorzitter,

drs. H.M.M. Koek drs. J. Smit

"Van: art 5 1-2e
Verzonden: 2019-10-09 13:22:04.510000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Actuele versie in IDMS
"
De lijst bevat 42 personen.

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 < art 5 1-2e pzh.nl>
Verzonden: woensdag 9 oktober 2019 13:18
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Re: Actuele versie in IDMS

Hai art 5 1-2e

Later is dit ergens 43 geworden....we moeten dit nu wel echt scherp hebben. Heb jij de lijst op basis waarvan de brieven / mails verstuurd zijn? Laten we dat aantal aanhouden.

Publiekssamenvatting eerste reactie ok, ik kom er zo nog even op terug als ik Jet heb gesproken.

Groeten,

art 5 1-2e

M art 5 1-2e

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

Provincie Zuid-Holland

On Wed, Oct 9, 2019 at 12:15 PM +0200, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Hoi art 5 1-2e

In de definitieve beantwoording zie ik dat er nu 43 personen worden genoemd ipv 42.

Het zijn er 42; dit staat ook in het adviesdocument waar art 5 1-2e op heeft besloten en is ook gemeld aan de Autoriteit Persoonsgegevens.

Ik heb dit weer aangepast.

Voorstel publiekssamenvatting:

Gedeputeerde Staten (GS) hebben de beantwoording van de statenvragen met betrekking tot “Melding datalek 24 september 2019” vastgesteld.

De statenvragen zijn gesteld naar aanleiding van een binnen de provincie opgetreden datalek dat is gemeld bij de Autoriteit Persoonsgegevens en waarover Provinciale Staten zijn geïnformeerd.

GS geven uitleg over de gevolgde procedure, de risicobeoordeling en de leerpunten die GS uit dit datalek trekken over de beveiliging van persoonsgegevens in de andere provinciale systemen.

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 < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: woensdag 9 oktober 2019 11:45
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: Actuele versie in IDMS

Ach onhandig! Gedaan!

Inderdaad GS van 15 oktober, daarna is het alweer herfstreces.

Zojuist ook art 5 1-2e even gevraagd mee te denken over de publiekssamenvatt eageert waarschijnlijk begin van de middag :) Als je een voorzet hebt kan ik die ook aan haar doorsturen.

Hartelijke groet,

art 5 1-2e

M art 5 1-2e

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

Provincie Zuid-Holland

Van: art 5 1-2e
Verzonden: woensdag 9 oktober 2019 11:42
Aan: art 5 1-2e
Onderwerp: RE: Actuele versie in IDMS

Zou je de reservering er nog even af willen art 5 1-2e

En is al duidelijk op welke op welke GS vergadering mikken we; 15 oktober?

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 <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: woensdag 9 oktober 2019 11:23
Aan: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Actuele versie in IDMS

Hai art 5 1-2e

Actuele versie staat in IDMS.

Watermerk staat er nog in en datum heb ik nog niet ingevuld, maar zal 15 oktober zijn.

Hartelijke groet,

art 5 1-2e

"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-10-15 14:50:35.139000+00:00
"Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: RE: Stukken datalek ivm Statenvergadering morgenvroeg
"
Hallo art 5 1-2e

Het informeren van PS en betrokkenen is onder coördinatie van art 5 1-2e uitgevoerd.

Ik beschik niet over de brief aan PS en ook niet over Q&A.

art 5 1-2e kun jij die stukken aa n art 5 1-2e sturen?

Ik ben morgen tussen 10-12 beschikbaar

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 < art 5 1-2e pzh.nl>
Verzonden: dinsdag 15 oktober 2019 13:41
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
CC: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Stukken datalek ivm Statenvergadering morgenvroeg
Urgentie: Hoog

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

(hopelijk spel ik je naam goed)

Zojuist ook een voicemail ingesproken. Morgen is de Statenvergadering. Er is een kleine kans dat er nog wordt gepraat over het datalek van september j.l.

Twee vragen:

1. Zou je per ommegaande de stukken willen sturen die gemaakt zijn ihkv het datalek van september j.l.? Zo heb ik bijvoorbeeld niet de definitieve brief die naar PS is gegaan (alleen de conceptbrief). En ook de Q&A.
2. Ben je telefonisch bereikbaar indien dat nodig is, tussen 10 en 12?

Groet

art 5 1-2e

art 5 1-2e

Bestuursadviseur Gedeputeerde W.H. de Zoete

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

art 5 1-2e pzh.nl <mailt o 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/>
"


provincie
ZUID HOLLAND


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-11-13 13:39:59+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: FW: GEWIJZIGDE VERSIE met de juiste Link HTM verlenging 2019-2020
"
Dag art 5 1-2e

Hierbij de betreffende mail.

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
Verzonden: dinsdag 12 november 2019 13:28
Aan: fg
Onderwerp: FW: GEWIJZIGDE VERSIE met de juiste Link HTM verlenging 2019-2020

Van: art 5 1-2e
Verzo november 2019 11:31
Aan: art 5 1-2e
Onderwerp: FW: GEWIJZIGDE VERSIE met de juiste Link HTM verlenging 2019-2020

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: GEWIJZIGDE VERSIE met de juiste Link HTM verlenging 2019-2020

Beste Collega,

Je huidige HTM-abonnement verloopt op 1 december 2019. We zijn alweer druk bezig met de voorbereidingen van de verlenging. Om dit zo goed mogelijk te laten verlopen willen we je vragen om de volgende zaken te controleren.

* Wanneer je in het afgelopen jaar een nieuwe OV-chipkaart hebt gekregen door verlies of defecte kaart, geeft het nieuwe nummer van de OV-chipkaart door aan het Loket vÃ³Ã³r 8 november 2019. Dit is nodig om het nieuwe abonnement te kunnen koppelen aan de OV-chipkaart. Lever daarom altijd een fotokopie in van je nieuwe OV-chipkaart na vervanging. Je kunt je fotokopie mailen onder vermelding van je naam naar personenvervoer@pzh.nl <mailto:personenvervoer@pzh.nl> .

* Loopt je OV-chipkaart bijna af, vraag dan een vernieuwende kaart aan via deze link https://www.ov-chipkaart.nl/vervangen-of-beeindigen/wat-te-doen-met-een-bijna-verlopen-kaart.htm <https://www.ov-chipkaart.nl/vervangen-of-beeindigen/wat-te-doen-met-een-bijna-verlopen-kaart.htm> , uiterlijk 6 weken van te voren en niet eerder.

Je abonnement wordt dan op die kaart overgezet. Lever altijd een fotokopie in van je nieuwe OV-chipkaart. Je kunt je fotokopie mailen onder vermelding van je naam naar personenvervoer@pzh.nl <mailto:personenvervoer@pzh.nl> .

* Ben je het afgelopen jaar verhuisd, zorg dan dat je adreswijziging doorgevoerd is in YouForce, het adres in YouForce is leidend voor de verlenging van je abonnement.

* Als je abonnement verlengd is door de provincie en je hebt de wijzigingen niet tijdig doorgegeven voor 8 november 2019 dan beschik je na 1 december 2019 niet over een geldig vervoersbewijs.

* Let op; mocht je buiten je zonegrens reizen, zorg dan dat je voldoende saldo hebt op je Ov-chipkaart. Dit voorkomt dat je abonnement geblokkeerd word!

Het Loket zal de komende weken in november alle HTM abonnementen verlengen. Let op; je ontvangt een e-mail van de HTM vervoerder met het bericht dat je abonnement verlengt is en dat je je product binnen de gestelde dagen op moet halen. Dit doe je door je abonnement op te halen bij Ã©Ã©n van de oplaadpunten. Pas, op het moment dat je dit hebt gedaan, kun je vanaf 1 december 2019 reizen binnen jouw zones door in- en uit te checken in de bus, tram of metro.

Wij hopen je hiermee voldoende te hebben geÃ¯nformeerd. Voor vragen kun je op Intranet kijken bij Personenvervoer of contact opnemen met Het Loket op 7777 (optie 2) of mailen naar personenvervoer@pzh.nl <mailto:personenvervoer@pzh.nl>

Voor vragen over de OV-chipkaart kun je terecht op www.ov-chipkaart.nl <http://www.ov-chipkaart.nl>

Hartelijk groet,

art 5 1-2e

Sectiehoofd

Aanwezig:Maandag,Dinsdag,Woensdag en Donderdag

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=02%7C01% Buiten reikwijdte Woo-verz 40pzh.nl%7C9fa0766e2d13424f067208d6ef357e5b%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C636959410368570302&sdata=3gdkzPGzQQwDf%2BJJ5JkiPeTORLN9I9YzIC9FRAABixw%3D&reserved=0>

-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://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Feformulieren.zuid-holland.nl%2FDefault.aspx%3FscenarioID%3DscContact&data=02%7C01% art 5 1-2e 40pzh.nl%7C9fa0766e2d13424f067208d6ef357e5b%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C636959410368570302&sdata=OxgVqKRyrtg2mbTQiZzQ3LqBI08cDV4PdVN45a8VCZU%3D&reserved=0> .
"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-11-13 15:47:05.567000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Advies DL
"
Ha art 5 1-2e

Heb je even tijd om mee te denken over een mogelijk datalek?

Er is vanuit het Loket een mail gestuurd aan collega's over hun OV abonnement met alle e-mailadressen leesbaar in het Aan-veld.

Er staan ook privé mail adressen van collega's tussen (heeft iets te maken met de manier waarop het OV-abonnement is geregistreerd).

Een van de personen met een privé e-mailadres heeft geprotesteerd.

Als we onze lijn handhaven, lijkt me dit technisch gezien een datalek maar een die niet meldingswaardig is bij de AP (en betrokkenen).

We vinden het onwaarschijnlijk dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht.

De melding en de mail staan hier: ""2019-11-12"" kan via de volgende koppeling worden geopend: http://idms/otcs/llisapi.dll/properties/715417949

Ik bel je hier even over.

Mvg, art 5 1-2e
"

"Van: art 5 1-2e
Verzonden: 2019-11-14 10:45:08.157000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: 20191112 Advies in kader van meldplicht datalekken.docx
"
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 < art 5 1-2e pzh.nl>
Verzonden: donderdag 14 november 2019 10:44
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Re: 20191112 Advies in kader van meldplicht datalekken.docx

Kun je het mailen? Ik kan niet bij iDMS komen op mijn mobiel.

Groet art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Thu, Nov 14, 2019 at 10:42 AM +0100, "" art 5 1-2e " < art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> > wrote:

> Ha art 5 1-2e
>
> Wil je nog even laten weten of je je kunt vinden in het 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/>

Van: art 5 1-2e
Verzonden: woensdag 13 november 2019 17:55
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> >
Onderwerp: 20191112 Advies in kader van meldplicht datalekken.docx

""20191112 Advies in kader van meldplicht datalekken.docx"" kan via de volgende koppeling worden geopend: http://idms/otcs/llisapi.dll/properties/PZH-2019-715420276

Graag per ommegaande jullie opmerkingen en aanvullingen in het document.

@ art 5 1-2e kun jij aanvullen waarom er door Het Loket privé e-mailadressen geregistreerd zijn? Had te maken met de privé OV-kaart, maar dat heb ik niet meer scherp.

Daarna stuur ik het door aan art 5 1-2e en Willy.

Mvg, art 5 1-2e
"


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 en 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.

<u>Analyse van dit specifieke geval</u>
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: 2019-11-14 11:12:07+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: Re: 20191112 Advies in kader van meldplicht datalekken.docx
"
Akkoord

Met vriendelijke groet art 5 1-2e Provincie Zuid-Holland

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Thu, Nov 14, 2019 at 11:08 AM +0100, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Ha art 5 1-2e

Ik verstuur de mail aan art 5 1-2e Willy om 11:20, daarna ga ik naar een externe afspraak.

Wil je voor die tijd iets laten weten?

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: donderdag 14 november 2019 10:45
Aan: art 5 1-2e <art 5 1-2e pzh.nl>
Onderwerp: RE: 20191112 Advies in kader van meldplicht datalekken.docx

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 <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: donderdag 14 november 2019 10:44
Aan: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Re: 20191112 Advies in kader van meldplicht datalekken.docx

Kun je het mailen? Ik kan niet bij iDMS komen op mijn mobiel.

Groet art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Thu, Nov 14, 2019 at 10:42 AM +0100, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

Ha art 5 1-2e

Wil je nog even laten weten of je je kunt vinden in het 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/>

Van: art 5 1-2e
Verzonden: woensdag 13 november 2019 17:55
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> >
Onderwerp: 20191112 Advies in kader van meldplicht datalekken.docx

""20191112 Advies in kader van meldplicht datalekken.docx"" kan via de volgende koppeling worden geopend:
http://idms/otcs/llisapi.dll/properties/PZH-2019-715420276

Graag per ommegaande jullie opmerkingen en aanvullingen in het document.

@ art 5 1-2e kun jij aanvullen waarom er door Het Loket privé e-mailadressen geregistreerd zijn? Had te maken met de privé OV-kaart, maar dat heb ik niet meer scherp.

Daarna stuur ik het door aan art 5 1-2e en Willy.

Mvg, art 5 1-2e
"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2019-11-14 11:27:15.454000+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	:	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 en 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.

<u>Analyse van dit specifieke geval</u>
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: 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 en 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.

<u>Analyse van dit specifieke geval</u>
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: Zoete - van der Hout, WH, de"
Verzonden: 2019-11-15 10:19:38+00:00
"Aan: art 5 1-2e art 5 1-2e
"CC: art 5 1-2e
Onderwerp: Re: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Dank beiden, in een volgend poho kom ik er graag op terug

Willy de Zoete

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Thu, Nov 14, 2019 at 5:36 PM +0100, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

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

"Van: art 5 1-2e
Verzonden: 2019-11-15 16:33:48.929000+00:00
"Aan: art 5 1-2e art 5 1-2e
"CC: art 5 1-2e
Onderwerp: RE: Ter info: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
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 < art 5 1-2e pzh.nl>
Verzonden: vrijdag 15 november 2019 13:20
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: RE: Ter info: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Dat is inderdaad portefeuillehouderoverleg art 5 1-2e

Volgens PO is 25 november 2019 om 11 uur. Nodige documenten moeten uiterlijk a.s. woensdag aan het eind van de dag bij art 5 1-2e zijn aangeleverd. Om die reden heb ik haar in CC opgenomen.

Groeten,
art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: vrijdag 15 november 2019 13:17
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: Ter info: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Ter info een afgehandeld datalek.

Willy wil er in een volgend poho (= portefeuilleoverleg?) op terugkomen.

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: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl
<mailto:wh.de.zoete@pzh.nl> >
Verzonden: vrijdag 15 november 2019 10:20
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> >
CC: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Re: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Dank beiden, in een volgend poho kom ik er graag op terug

Willy de Zoete

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Thu, Nov 14, 2019 at 5:36 PM +0100, "" art 5 1-2e " < art 5 1-2e pzh.nl
<mailto: art 5 1-2e pzh.nl> > wrote:

> 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

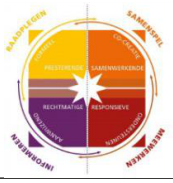
Postbus 90602, 2509 LP

Den Haag

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

"

Oplegnotitie portefeuille-overleg

Portefeuille:	Bedrijfsvoering		
Gedeputeerde:	De Zoete		
Datum overleg:	25 november		
Dossier:	Privacy		
Onderwerp:	Afhandeling datalek		
Behandelend Ambtenaar:	art 5 1-2e	Ambtelijk Opdrachtgever:	
Doel:	☐ Ter kennisname ☐ Ter besluitvorming ☐ (Concept) beantwoording (Staten)vragen/moties		Participatie-Proces? ☐ Ja ☐ Nee
Agendering in GS:	☐ Conformstuk ☐ Bespreekstuk ☐ N.v.t.		

1. BESLISPUNT / ESSENTIE VAN HET VOORSTEL

Puntsgewijs vermelden wat je aan de Gedeputeerde vraagt.

2. KORTE VOORGESCHIEDENIS

Wat ging vooraf aan deze notitie/dit punt? Wat was de voorgaande relevante besluitvorming?

Er is een datalek opgetreden. De gedeputeerde is conform de procedure voor afhandeling van datalekken geïnformeerd over het advies van het privacyteam aan de concerndirecteur.

De gedeputeerde heeft aangegeven hier in het portefeuilleoverleg op terug te willen komen.

3. AANDACHTSPUNTEN GS

- *N.v.t.*

4. CONSEQUENTIES

- *Geen.*

5. BIJGAAND(E) STUK(KEN)

- Het advies van het privacyteam
- De reactie (e-mail) van de concerndirecteur.

6. VERDERE PROCEDURE + COMMUNICATIE

- *N.v.t.*

7. INTEGRALITEIT

N.v.t.


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 en 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.

<u>Analyse van dit specifieke geval</u>
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: Zoete - van der Hout, WH, de"
Verzonden: 2019-11-15 10:19:38+00:00
"Aan: art 5 1-2e art 5 1-2e
"CC: art 5 1-2e
Onderwerp: Re: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Dank beiden, in een volgend poho kom ik er graag op terug

Willy de Zoete

Outlook voor Android downloaden <https://aka.ms/ghei36>

On Thu, Nov 14, 2019 at 5:36 PM +0100, "" art 5 1-2e " < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> > wrote:

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

"Van: art 5 1-2e
Verzonden: 2019-12-06 14:34:45.338000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: AVG proof maken TopDesk
"
Graag wat druk hierop zetten. Ik vind dat het allemaal best traag gaat. Mijn memo van 2 maanden terug was bedoeld om de urgentie aan te geven.

Het doel is om zo snel mogelijk te zorgen dat er geen nieuwe datalekken in Topdesk ontstaan.

Er hoeft net als de vorige keer maar 1 alerte medewerker tussen te zitten die meldt dat hij persoonsgegevens aantreft die hij voor het uitvoeren van zijn deeltaak niet nodig heeft, en I&A is in problemen.

We zijn nu 2 maanden verder en men is nog bezig een berg data door te spitten. Dat is leuk omdat we daarvan leren hoe dat moet, maar m.i. niet nodig voor dit doel.

Gisteren is dit onderwerp pas op de verkenningstafel geland.

Een hoop mensen hebben hun hand opgestoken om erbij betrokken te zijn, maar een praktische aanpak is er nog niet (wat niet aan art 5 1-2e ligt, want die is er net mee bezig)

M.i. moet men gewoon contact zoeken met de Topdesk contactpersonen van de diverse afdelingen om het gesprek aan te gaan welke persoonsgegevens er worden verwerkt en waarom.

Data analyse kan daarbij ondersteunend zijn, maar hoeft niet leidend te zijn.

mvg art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: vrijdag 6 december 2019 14:18
Aan: art 5 1-2e <art 5 1-2e pzh.nl>
Onderwerp: AVG proof maken TopDesk

Dit onderwerp is a.s. maandag in vergadering MT geagendeerd art 5 1-2e Als jij een reactie bij de memo hebt (zie IDMS map MT a.s. maandag), verneem ik dat graag.

Groeten,
art 5 1-2e
"

"Van: art 5 1-2e
Verzonden: 2019-12-16 12:15:45.315000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: FW: Kick Off - TOPdesk opschonen & aanpassen
"
Ha art 5 1-2e

Dit is nog als follow-up van het Topdesk datalek rond de aanmelding van Statenleden.

Ik hoop dat je aanwezig kunt zijn.

mvgEJ

-----Oorspronkelijke afspraak-----
Van: art 5 1-2e
Verzonden: maandag 16 december 2019 12:08
Aan: Buiten reikwijdte Woo-verzoek
Onderwerp: Geaccepteerd: Kick Off - TOPdesk opschonen & aanpassen
Tijd: donderdag 9 januari 2020 09:00-10:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
Locatie: D1.40 - Vergaderruimte
"

"Van: art 5 1-2e
Verzonden: 2019-12-20 10:10:43.323000+00:00
"Aan: art 5 1-2e art 5 1-2e art 5 1-2e
CC:
Onderwerp: Afgehandeld: Er is een melding van een Datalek ontvangen. (M19 12 02950)
"
Afgehandeld.

19-12-2019: Gesprek art 5 1-2e art 5 1-2e , art 5 1-2e art 5 1-2e heeft de situatie toegelicht.
Het betreft een door de RDW geleverd .csv bestand op de R-schijf.
Het bestand is alleen in te zien door data-analisten (functiegebonden toegang).
Er is geen sprake van een beveiligingsincident of een datalek.
Call wordt gesloten.
art 5 1-2e

Van: loket@pzh.nl
Verzonden: woensdag 18 december 2019 15:20
Aan: art 5 1-2e ; art 5 1-2e ; art 5 1-2e
Onderwerp: Er is een melding van een Datalek ontvangen. (M19 12 02950)

Beste collega,

Er is een melding van een Datalek ontvangen.

Melden datalek: M19 12 02950

Je kunt deze hier <https://loket.pzh.nl/tas/secure/contained/incident?unid=ced481410b8d4f3eb6bb14244dd66773> behandelen.

Met vriendelijke groet,

Het Loket

<HTTPS://loket.pzh.nl/tas/images/email_footer.jpg>

Het Loket telefoon 070 4417777 loket.pzh.nl <https://loket.pzh.nl>
"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: Definitief

Melding gegevens

Naam melder	:	art 5 1-2e via art 5 1-2e (Functionaris gegevensbescherming)
Registratienummer van het incident	:	
Datum en tijdstip van de melding	:	Maandag 1 april 13:00
Route van de melding	:	Telefonisch en per e-mail

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	03-12-2018 (concept)
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e privacyjurist), art 5 1-2e (P&O)
Advies ter kennisgeving gedeeld met	:	

Situatie

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

Geachte art 5 1-2e

Zoals zojuist besproken stuur ik hierbij de mail die zonder mijn medeweten is gepubliceerd door de pronincie. https://staten.zuid-holland.nl/migratie/Statencommissie_Mobiliteit_Kennis_en_Economie_MKE/2008/Statencommissie_Mobiliteit_Kennis_en_Economie_9_april_2008/Onderliggende_stukken/Comm_Stuk_ter_kennisname/32_5b_brief_van_dhr_Brands_inzake_intentieverklaring_corridorstraat_N207_pdf.org

Tevens heb ik besproken dat ik na verzenden van deze mail de Autoriteit Persoonsgegevens hiervan op de hoogte ga stellen.

Tevens wil ik het verzoek bij u indienen het bewuste document per direct van het internet te verwijderen.

Graag verneem ik van u hoe dit proces in gang zal worden gezet zodat ik daarvan geen hinder meer kan ondervinden.

Met vriendelijke groet,
art 5 1-2e

P.S. Ik heb nu een ander e-mailadres dan in mijn eerder verzonden e-mail.

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 één e-mail die in 2008 in het Staten Informatie Systeem integraal als ingezonden stuk is gepubliceerd en daarmee publiek toegankelijk is geworden.

Vraag	Antwoord
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend. Het document zijn gepubliceerd in het provinciale Staten Informatie Systeem, dat via internet toegankelijk is.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Documenten zijn in het Staten Informatie Systeem als PDF gepubliceerd. De documenten kunnen worden gelezen en gekopieerd, maar niet worden gewijzigd of verwijderd.
Welke persoonsgegevens betreft het?	E-mailadres, naam, adres, telefoonnummer.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee. Onderzoek heeft uitgewezen dat het de categorie normale persoonsgegevens betreft (geen bijzondere / hoog risico gegevens).
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Onbekend. De documenten zijn gepubliceerd in het provinciale Staten Informatie Systeem, dat via internet toegankelijk is.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	De aard van de persoonsgegevens is niet van dien aard dat er sprake is van een risico voor de rechten en vrijheden van de betrokken persoon. Daarentegen ervaart de betrokkene het datalek als een forse inbreuk op zijn privéleven.
Betreft het een beveiligingsincident?	Ja
Betreft het een datalek?	Ja
Ondernomen beperkende maatregelen.	De e-mail is gedepubliceerd en uit het Staten Informatie Systeem verwijderd.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	art 5 1-2e s op 2 april 2019 geïnformeerd dat de e-mail uit het Staten Informatie Systeem is verwijderd. Nadat de melding bij de Autoriteit Persoonsgegevens is gedaan, zal de functionaris gegevensbescherming Buiten reikwijdte Woo-verzoek hierover informeren. De provincie gaat zich beraden of SIS informatie van collegeperioden in het verdere verleden op de website moeten blijven staan.

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

[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.

Advies
De conclusie is dat er sprake is van een beveiligingslek en dat er sprake is van een te melden datalek.

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 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: Secretariaat VEERO [mailto art 5 1-2e
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 beste 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.

AUTORITEIT
PERSOONSGEGEVENS

Voorbeeldlijst wel/niet melden datalek

Heeft uw organisatie een datalek? Dan kan het zijn dat u dit moet melden aan de Autoriteit Persoonsgegevens (AP) en aan de betrokken personen. Dit hangt af van het risico op schade. U moet dit zelf inschatten. De voorbeelden in dit overzicht kunt u gebruiken als hulpmiddel. In het dossier 'Meldplicht datalekken' op onze website vindt u meer informatie over het beoordelen van de risico's.

VOORBEELD	MELDEN AAN AP	MEEDELEN AAN BETROKKENEN?	OPMERKINGEN / AANBEVELINGEN
Een verwerkingsverantwoordelijke heeft een back-up van een archief van persoonsgegevens op een USB-stick opgeslagen. De USB-stick wordt gestolen tijdens een inbraak.	NEE	NEE	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.
Een verwerkingsverantwoordelijke exploiteert een online dienst. Als gevolg van een cyberaanval op die dienst worden persoonsgegevens geëxtraheerd. De verwerkingsverantwoordelijke heeft klanten in een enkele lidstaat.	JA Meld deze inbreuk aan de toezichthoudende autoriteit als er waarschijnlijk gevolgen zijn voor personen.	JA Deel deze inbreuk mee aan personen afhankelijk van de aard van de betrokken persoonsgegevens en of de waarschijnlijke gevolgen voor personen zeer ernstig zijn.	

Deze voorbeelden zijn gebaseerd op de voorbeeldlijst uit de 'Guidelines voor melding van inbreuken in verband met persoonsgegevens', opgesteld door de Europese privacytoezichthouders.

VOORBEELD	MELDEN AAN AP*	MEEDELEN AAN BETROKKENEN?	OPMERKINGEN / AANBEVELINGEN
Een stroomstoring van enkele minuten in het callcenter van een verwerkingsverantwoordelijke heeft tot gevolg dat klanten de verwerkings-verantwoordelijke niet kunnen bellen en geen toegang hebben tot hun gegevens.	NEE	NEE	Dit is geen te melden inbreuk, maar wel een te registreren incident overeenkomst artikel 33, lid 5. De verwerkingsverantwoordelijke dient de nodige gegevens te registreren en bij te houden.
Een verwerkingsverantwoordelijke wordt het slachtoffer van een ransomware-aanval. Het gevolg is dat al zijn gegevens zijn versleuteld. Er zijn geen back-ups beschikbaar en de gegevens kunnen niet worden hersteld. Tijdens het onderzoek wordt duidelijk dat de enige functionaliteit van de ransomware het versleutelen van de gegevens was en dat er geen andere malware in het systeem aanwezig was.	JA Meld deze inbreuk aan de toezichthoudende autoriteit als er waarschijnlijk gevolgen zijn voor personen, aangezien dit een verlies van beschikbaarheid is.	JA Deel deze inbreuk mee aan personen afhankelijk van de aard van de betrokken persoonsgegevens en de mogelijke gevolgen van het niet beschikbaar zijn van de gegevens, alsmede andere waarschijnlijke gevolgen.	Als een back-up beschikbaar was en de gegevens tijdig konden worden hersteld, moest deze inbreuk niet aan de toezichthoudende autoriteit worden gemeld noch aan personen worden meegedeeld aangezien er geen permanent verlies van beschikbaarheid of vertrouwelijkheid zou zijn geweest. Als de toezichthoudende autoriteit echter op een andere wijze kennis heeft gekregen van het incident, kan zij een onderzoek overwegen om na te gaan of aan de ruimere veiligheidseisen van artikel 32 is voldaan.
Een persoon belt naar het callcenter van een bank om een inbreuk in verband met persoonsgegevens te melden. De persoon heeft een maandoverzicht van iemand anders ontvangen. De verwerkingsverantwoordelijke voert een kort onderzoek uit (het onderzoek wordt binnen de 24 uur afgerond) en stelt met een redelijke mate van zekerheid vast dat er zich een inbreuk in verband met persoonsgegevens heeft voorgedaan. Hij vraagt zich af of er zich ergens een systeemstoring voordoet, in welk geval dit mogelijk gevolgen heeft gehad of zou kunnen hebben voor andere personen.	JA	De inbreuk wordt alleen meegedeeld aan de getroffen personen als er een hoog risico is en het duidelijk is dat anderen niet zijn getroffen.	Indien na nader onderzoek wordt vastgesteld dat er meer personen getroffen zijn, moet de toezichthoudende autoriteit hiervan in kennis worden gesteld en moet de verwerkingsverant-woordelijke de inbreuk meedelen aan andere personen indien er een groot risico voor hen bestaat.

VOORBEELD	MELDEN AAN AP*	MEEDELEN AAN BETROKKENEN?	OPMERKINGEN / AANBEVELINGEN
Een verwerkingsverantwoordelijke exploiteert een onlinemarktplaats en heeft klanten in meerdere lidstaten. De marktplaats wordt getroffen door een cyberaanval, en de aanvaller publiceert gebruikersnamen, wachtwoorden en aankoopoverzichten op het internet.	JA Meld de inbreuk aan de leidende toezichthoudende autoriteit als het gaat om grensoverschrijdende verwerking.	JA Aangezien dit tot een groot risico zou kunnen leiden.	De verwerkingsverantwoordelijke dient actie te ondernemen, bijvoorbeeld door de getroffen accounts te verplichten hun wachtwoorden te wijzigen, evenals andere stappen om het risico te beperken. De verwerkingsverantwoordelijke dient ook andere kennisgevingsverplichtingen in overweging te nemen, bijvoorbeeld op grond van de NIS-richtlijn als digitale dienstverlener.
Een als gegevensverwerker optredend hostingbedrijf constateert een fout in de code voor de autorisatie van gebruikers. Het gevolg van de fout is dat elke gebruiker toegang kan krijgen tot de accountgegevens van elke andere gebruiker.	Als verwerker moet het hostingbedrijf zijn getroffen klanten (de verwerkingsverantwoordelijken) onverwijld hiervan in kennis stellen. In de veronderstelling dat het hostingbedrijf zijn eigen onderzoek heeft verricht, zouden de getroffen verwerkingsverantwoordelijken redelijke zekerheid moeten hebben over de vraag of ze het slachtoffer zijn geworden van een inbreuk. Bijgevolg wordt het waarschijnlijk geacht dat ze "kennis" hebben gekregen van de inbreuk zodra ze door het hostingbedrijf (de verwerker) daarvan in kennis zijn gesteld. De verwerkings-verantwoordelijke dient de inbreuk vervolgens te melden aan de toezichthoudende autoriteit.	Als er waarschijnlijk geen hoog risico voor de personen is, moet de inbreuk niet aan hen worden meegedeeld.	Het hostingbedrijf (verwerker) moet alle andere kennisgevingsverplichtingen (bijvoorbeeld op grond van de NIS-richtlijn als een digitale dienstverlener) in overweging nemen. Als er geen aanwijzingen zijn dat er bij een van de verwerkingsverantwoordelijken misbruik wordt gemaakt van deze kwetsbaarheid, is er mogelijk geen sprake van een te melden inbreuk. Wel zal deze inbreuk waarschijnlijk moeten worden geregistreerd of worden beschouwd als een geval van niet-naleving overeenkomstig artikel 32.

VOORBEELD	MELDEN AAN AP*	MEEDELEN AAN BETROKKENEN?	OPMERKINGEN / AANBEVELINGEN
Als gevolg van een cyberaanval zijn de medische dossiers in een ziekenhuis gedurende 30 uur niet beschikbaar.	JA Het ziekenhuis is verplicht om te melden dat de inbreuk een hoog risico kan inhouden voor het welzijn en de patiënt	JA Deel deze inbreuk mee aan de getroffen personen.	
Persoonsgegevens van een groot aantal studenten worden per ongeluk naar de verkeerde mailinglijst gestuurd ... een lijst met meer dan 1 000 ontvangers.	JA Meld deze inbreuk aan de toezichthoudende autoriteit.	JA Deel deze inbreuk mee aan personen, afhankelijk van de omvang en het type persoonsgegevens en de ernst van de mogelijke gevolgen.	
Een direct-marketingmail wordt verzonden naar ontvangers in het veld "Aan" of "CC", waardoor elke ontvanger het e-mailadres van de andere ontvangers kan zien.	JA Het kan verplicht zijn om deze inbreuk te melden aan de toezichthoudende autoriteit als een groot aantal personen erdoor getroffen is, als er gevoelige gegevens zijn onthuld (bijvoorbeeld een mailinglijst van een psychotherapeut) of als andere factoren hoge risico's inhouden (bijvoorbeeld als de mail de oorspronkelijke wachtwoorden bevat).	JA Deel deze inbreuk mee aan personen, afhankelijk van de omvang en het type persoonsgegevens en de ernst van de mogelijke gevolgen.	Mogelijk dient de inbreuk niet te worden gemeld/meegedeeld als er geen gevoelige gegevens zijn onthuld en als er slechts een klein aantal e-mailadressen is onthuld.

"Van: art 5 1-2e
Verzonden: 2020-01-08 12:54:54.399000+00:00
"Aan: art 5 1-2e art 5 1-2e
"CC: art 5 1-2e
Onderwerp: Jullie mening: Datalek?
"
""Oorspronkelijke aanvraag.pdf"" kan via de volgende koppeling worden geopend: http://idms/otcs/llisapi.dll/properties/PZH-2020-722572987

Bijgaand een datalek melding die vandaag is gedaan.

Voordat ik art 5 1-2e hierover bel hoor ik graag jullie mening.

Voor zover ik het nu begrijp heeft art 5 1-2e een lijst gemaild met aangemelde personen voor de nieuwjaarsreceptie.

De bedoeling van deze alleen intern te delen, maar hij heeft deze per ongeluk aan 1 oud-Statenlid en 1 huidig Statenlid gemaild.

Het oud-Statenlid heeft hierover contact opgenomen.

Mijn mening:

Het betreft relaties van de provincie Zuid-Holland die naar een openbare receptie komen.

De ontvanger is een oud-Statenlid, de gegevens zijn niet gevoelig en de inhoud van de e-mail is niet gevoelig en geeft geen aanleiding tot misbruik.

Gezien deze context achten wij het hiermee verbonden risico voor de betrokkenen laag.

Wel is er feitelijk sprake van een datalek, omdat de persoonsgegevens zijn gemaild aan een persoon die niet meer werkzaam is in de provinciale organisatie en die deze informatie niet had horen ontvangen.

Betrokkenen hebben ook geen expliciete toestemming gegeven voor het delen van hun persoonsgegevens buiten de provincie.

Conclusie: 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.

En:

* het oud-Statenlid dient te worden bedankt voor zijn oplettendheid. Zou mooi zijn als de FG dit voor zijn rekening neemt
* Terugkoppeling aan art 5 1-2e et dank doo r art 5 1-2e
"

"Van: art 5 1-2e
Verzonden: 2020-01-10 10:36:50.746000+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 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 heeft 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: 2020-01-10 10:58:28+00:00
"Aan: art 5 1-2e
"CC: Zoete - van der Hout, WH, de; art 5 1-2e
Onderwerp: Re: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Ik ben akkoord met dit advies. Groet, art 5 1-2e

Outlook voor Android downloaden <https://aka.ms/ghei36>

From: art 5 1-2e <art 5 1-2e pzh.nl>
Sent: Friday, January 10, 2020 10:36:50 AM
To: 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>
Subject: 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


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2020-01-24 10:53:52.896000+00:00
"Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet
"
Heren,

Mogelijk een datalek bij Microsoft.

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

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

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

Staat inmiddels weer dicht.

Betreft mogelijk de volgende gegevens:

* System generated data related to support cases such as:

o Resource location

* Contact information provided to support agents or contained in customer support requests:

o Email addresses

o Telephone numbers

o Internet Protocol (IP) addresses

* Information shared with support agents as part of the support case interaction such as:

o Descriptions of technical issues

o Issue reproduction steps

Information shared to assist support agents with troubleshooting

Gisteren bij ons gemeld, dus vandaag afhandelen.

We hebben opgevraagd welke informatie het van PZH betreft (zie bijlage).

Graag jullie mening.

Mvg, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: donderdag 23 januari 2020 15:14
Aan: art 5 1-2e < art 5 1-2e pzh.nl> ; art 5 1-2e pzh.nl>
CC: art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Dag art 5 1-2e

Dit zojuist met art 5 1-2e al besproken. Ik had een verkeerd antwoord naar art 5 1-2e gestuurd, ik dacht dat het om de melding ging die ik naar jou had gestuurd.

Deze ligt nu bij mij.

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 23 januari 2020 13:48
Aan: art 5 1-2e pzh.nl <mailt o 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> >; art 5 1-2e < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> >
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Hallo art 5 1-2e

Om te beoordelen of dit ook voor ons een datalek is en hoe we hier mee om willen gaan is het nodig om exact te weten welke persoonsgegevens van PZH het betreft.

Wellicht heb je dat al gedaan, maar wil jij daartoe een Azure support request indienen?

Affected customers are being notified of this event. To obtain the data specific to your organization that were potentially exposed, please submit an Azure support request <https://eur03.safeli tlook.com/?url=https%3A%2F%2Faka.ms%2FAzSCSupport&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229520464&sdata=Bhn5UN9hwdRveR5hXyV5cj0ei5sUCyF%2BuyG7NBP6PeU%3D&reserved=0>

Ik hoor graag.

Mvg, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: donderdag 23 januari 2020 10:22
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 pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Dag art 5 1-2e

Deze is besproken met de betreffende specialist. Dit betreft de ontwikkelomgeving van het omgevingsbeleid. art 5 1-2e is op de hoogte.

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 23 januari 2020 10:02
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> >
CC: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> > ; art 5 1-2e <ra. art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Beste art 5 1-2een art 5 1-2e

Hierbij wil ik even melden dat ik onderstaande email heb gekregen, ihkv security.

Ik kan niet zo goed inschatten wat ik hiermee moet.

Ik heb begrepen dat art 5 1-2e binnen ons team ook een identieke email heeft gehad.

Ik heb geprobeerd om onderstaand gegeven (Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256) op te zoeken

maar ik kan niet vinden waarvoor ik de id gebruik.

Ik weet wel dat ik gebruik maak van een gratis MSDN subscription die komt bij Visual Studio, om te oefen met Azure.

Daarnaast heeft art 5 1-2e mij aangemeld bij Microsoft support om call aan te kunnen maken.

Kunnen jullie laten weten of ik nog aanvullende acties moet ondernemen tgv deze email?

Alvast bedankt,

Groetjes

art 5 1-2e

art 5 1-2e

Tactisch Dataspecialist

Afdeling I&A | bureau Bedrijfsinformatie

T 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/>

I&A heeft een groep op het Binnenplein! De â€˜groep I&Aâ€™ biedt nieuws, antwoorden op veelgestelde vragen en geeft tips.

Ook kun je bijvoorbeeld lezen over de projectboard en actuele I&A-projecten. Klik op het icoon om naar de groep te gaan en meld je aan als volger! Wil je meer weten over I&A-producten? Klik dan op het vraagtekenicoon waarmee je in de LearningGuide komt.
<http://binnenplein.pzh.nl/groepen/groep-i-en-a/>
<http://learningguide.pzh.local/html/introduction.htm>

Van: Microsoft Azure <azure-noreply@microsoft.com <mailto:azure-noreply@microsoft.com> >
Verzonden: woensdag 22 januari 2020 14:43
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019.

Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019. This issue was specific to an internal database used for support case analytics and does not represent an exposure of our commercial cloud services. Once identified, Microsoft mitigated the issue, and our security teamâ€™s investigation found no indication of malicious use of the database records. Our analysis of the support information indicates that specific personal or organizational identifiable information related to your support case was potentially visible.

You are receiving this message as an Azure account administrator or subscription administrator for this subscription. As a result of this issue, the support data exposed may include the following:

* System generated data related to support cases such as:

o Resource location

* Contact information provided to support agents or contained in customer support requests:

o Email addresses

o Telephone numbers

o Internet Protocol (IP) addresses

* Information shared with support agents as part of the support case interaction such as:

o Descriptions of technical issues

o Issue reproduction steps

o Information shared to assist support agents with troubleshooting

Affected customers are being notified of this event. To obtain the data specific to your organization that were potentially exposed, please submit an Azure support request <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAzSCSupport&data=02%7C01% art 5 1-2e 40pzh.nl %7C636fec8244e54efacb6608d79f41117e %7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229520464&sdata=Bhn5UN9hwdRveR5hXyV5cj0ei5sUCyF%2BuyG7NBP6PeU%3D&reserved=0> .

Summary of event

During the investigation, we determined that this information was potentially exposed due to a misconfiguration of network security group security rules.

Microsoft engineers determined that a change made to the database's network security group <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229530460&sdata=9kKkQLjMfEJ3MyDYkPLbr1PlrOcAiyMcq30Ept%2FTgYI%3D&reserved=0> on December 5, 2019 contained misconfigured security rules <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview%23security-rules&data=02%7C01 art 5 1-2e %40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=l9Md4n%2B6v2zgYrKVfL%2BdMSy%2BCahpIxcqq8DZ5TjbNF8%3D&reserved=0> that enabled exposure of the database information. Upon notification of the issue, engineers remediated the configuration on December 31, 2019 to restrict the database and prevent unauthorized access.

As part of Microsoftâ€™s standard operating procedures, data stored in the database is redacted using automated tools to remove personal information. Our investigation confirmed that the vast majority of records were redacted as intended. In some scenarios, the data may have remained unredacted if it met specific conditions. An example of this occurs if the information is in a non-standard format, such as an email address separated with spaces instead of written in a standard format â€œXYZ @contoso comâ€ vs â€œXYZ@contoso.com <mailto:XYZ@contoso.com> â€. We have begun notifications to customers whose data was present in this redacted database.

We are committed to the privacy and security of your data and are taking action to prevent future occurrences of this issue. These actions include:

* Audit the established network security rules for internal resources.

* Expand the scope of the mechanisms that detect security rule misconfigurations.

* Add additional alerting to service teams when security rule misconfigurations are detected.

* Implement additional redaction automation.

Misconfigurations are unfortunately a common error across the industry. We have solutions to help prevent this kind of mistake, but unfortunately, they were not enabled for this database. As weâ€™ve learned, it is good to periodically review your configurations and ensure your own configurations and ensure you are taking advantage of all protections available.

This documentation is included as general guidance and is not intended to be all-inclusive for how to configure your environment.

* Governing your Azure Workloads <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fazure.microsoft.com%2Fresources%2Fgoverning-your-azure-workloads%2F&data=02%7C01% art 5 1-2e %40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=w1J92sQy8TyywrpHaAURm4G3QNBoKvFSZUUPuJnG5dk%3D&reserved=0>

* Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=r7EzLvU%2FUftoDMNljzntMdRoakx%2F24ns5I50dLk5GCw%3D&reserved=0>

* Managing Network Security Groups
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fmanage-network-security-
group&data=02%7C01% art 5 1-2e %40pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=UqHOt9DuE
CkE5QPUtxnoitvegUlGjVTUMBy%2B2JCaK7k%3D&reserved=0>

* Network Security Group Security Rules
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview%23security-
rules&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=4Tbs3JjNe
7CRNMYR32FnphgUL8k1RfWZkCSY41iULLY%3D&reserved=0>

* Enabling Logging on Network Security Groups
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fvirtual-network-nsg-manage-
log&data=02%7C01%7 art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229560441&sdata=cp1XF2Am8
jBspkJduR1DPZY41rVTvfdSeqcqngUVyLE%3D&reserved=0>

Account information

Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256

This message from Microsoft is an important part of a program, service, or
product that you or your company purchased or participates in. Microsoft
respects your privacy. Please read our Privacy Statement
<https://eur03.safelinks.protection.outlook.com/?url=http art 5 1-2e
%2Fprivacy.microsoft.com%2Fprivacystatement&data=02%7C01%
%40pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229560441&sdata=8LsJ7tItQ
yN8D2h6941QfVX%2FW8hsC1873OF4LoOh0UY%3D&reserved=0> .

This is a mandatory service communication. To set your contact preferences for
other communications, visit the Promotional Communications Manager
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Faccount.microsoft.com%2Fprofile%2Fcontact-info&data=02%7C01% art 5 1-2e
%40pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229570437&sdata=pdUZHtu0M
uwXi%2F1XYPMM6Lh1%2B16gojSc1iV3UNFBjXQ%3D&reserved=0> .

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoMicrosoftGrey.png>

"

"Van: art 5 1-2e
Verzonden: 2020-01-23 16:13:16+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: FW: Case 120012322002761 Your question was successfully submitted to Microsoft Support
"
Van: Microsoft Support <support@mail.support.microsoft.com>
Verzonden: donderdag 23 januari 2020 16:05
Aan: art 5 1-2e <art 5 1-2e pzh.nl>
Onderwerp: Case 120012322002761 Your question was successfully submitted to Microsoft Support

Having trouble viewing this email? View your request online <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fportal.azure.com%2F%23resource%2Fsubscriptions%2F8265fcc1-efed-4eb3-bf99-557dade18709%2Fproviders%2Fmicrosoft.support%2Fsupporttickets%2F120012322002761&data=02%7C01%7C art 5 1-2e 40pzh.nl%7Cbf362403af11452df9ba08d7a0158db4%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637153886744793426&sdata=%2BV4LGyGRCyO6ge7Yr0rjcrCXaWbey4NKJ3Pnty4qn00%3D&reserved=0>

<https://msegceporticoprodassets.blob.core.windows.net/asset-blobs/4077967_en-us_1>

Support

Your question was successfully submitted to Microsoft Support using your Unified Support - Advanced plan. A Microsoft support professional will contact you within 4 business hours*.

Incident title:

Impact due to e-mail about Custom Support database accessible to the internet

Support request number:

120012322002761

Severity rating:

B

Expect response within:

4 business hours*

Contact preference:

Email

Name:

art 5 1-2e

Email address:

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

Contact numbers:

* Business hours exclude weekends and holidays. Learn More <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fazure.microsoft.com%2Fsupport%2Fplans%2Fresponse%2F&data=02%7C01%7C art 5 1-2e %40pzh.nl%7Cbf362403af11452df9ba08d7a0158db4%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637153886744803416&sdata=rjdBzcYIR5PduVFMIVhbgdc5BDJ38IbBylgbdUfdcOQ%3D&reserved=0> about support response times.

You can contact us again about this incident at any time on the Microsoft Azure portal <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fportal.azure.com%2F%23resource%2Fsubscriptions%2F8265fcc1-efed-4eb3-bf99-557dade18709%2Fproviders%2Fmicrosoft.support%2Fsupporttickets%2F120012322002761&data=02%7C01%7C art 5 1-2e 40pzh.nl%7Cbf362403af11452df9ba08d7a0158db4%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637153886744803416&sdata=fZQdtpJ6LKMJXZ8wvyD2ePEh0kotXBrhdYtorLZpgjw%3D&reserved=0> . See the Azure Support FAQ <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fazure.microsoft.com%2Fsupport%2Ffaq%2F&data=02%7C01%7C art 5 1-2e 40pzh.nl%7Cbf362403af11452df9ba08d7a0158db4%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637153886744813411&sdata=66e0zXicsG%2BKfWFskMBYrh9%2Bfg5ja1b9OZeE4HvRrvY%3D&reserved=0> for additional information about Azure Support, including terms and conditions.

This email is generated from an unmonitored account. Please do not reply.

Thank you,
Microsoft Azure Support

Additional Information

Product: Subscription management

Azure Subscription: pzh-productie

Azure Subscription ID: 8265fcc1-efed-4eb3-bf99-557dade18709

This message from Microsoft is an important part of a program, service, or product that you or your company purchased or participates in. Microsoft respects your privacy. Please read our Privacy Statement <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fazure.microsoft.com%2Fsupport%2Ftrust-center%2Fprivacy%2F&data=02%7C01%7 art 5 1-2e 40pzh.nl%7Cbf362403af11452df9ba08d7a0158db4%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637153886744813411&sdata=MuBtSobyXvJVBvy%2FpMzWWCBoWzM3wx5Rv2%2BpwhK5ZQk%3D&reserved=0> .

One Microsoft Way, Redmond, WA 98052 USA

<https://msegceporticoprodassets.blob.core.windows.net/asset-blobs/4294266_en_3>

refid-4294256
"

"Van: art 5 1-2e
Verzonden: 2020-01-24 16:09:42.116000+00:00
"Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet
"
De vraag is in hoeverre we het statement van Microsoft geloven.

We mogen m.i. aannemen dat hun onderzoek grondig is uitgevoerd.

Als dat zo is, is het dan aannemelijk dat er persoonsgegevens in verkeerde handen zijn gekomen?

art 5 1-2e e hebben nog geen antwoord van Microsoft welke persoonsgegevens het van ons betreft en hoe veel.

Anyway, het levert hoe dan ook geen hoog risico op voor de betrokkenen.

Het is allemaal zakelijk gerelateerde info.

Ik maak wel een datalek adviesrapportje.

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: vrijdag 24 januari 2020 15:30
Aan: art 5 1-2e <art 5 1-2e pzh.nl>; art 5 1-2e <art 5 1-2e pzh.nl>
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Daar verschillen we toch van mening. Het is m.i. wel een datalek, maar niet een die gemeld hoeft te worden aan de AP. Althans niet op grond van deze informatie. Ik begreep dat art 5 1-2e nog zit te wachten op nadere informatie van Microsoft.

Art 4, lid 12 AVG zegt dat een inbreuk in verband met persoonsgegevens ook is “de ongeoorloofde toegang tot , opgeslagen of anderszins verwerkte gegevens”. In dit geval is niet uit te sluiten dat er toegang is geweest. De database heeft 3 weken open gestaan.

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 art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 24 januari 2020 13:37
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> >
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Mag ik uit het onderstaande afleiden dat er niets met de persoonsgegevens is gebeurd? Zo dat het geval is, dan reikt het toch niet verder dan een beveiligingsincident. Verwijs ook naar de eerdere discussie rondom Citrix.

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 24 januari 2020 10:54
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 <mailt o art 5 1-2e pzh.nl> >
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet
Urgentie: Hoog

Heren,

Mogelijk een datalek bij Microsoft.

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

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

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

Staat inmiddels weer dicht.

Betreft mogelijk de volgende gegevens:

* System generated data related to support cases such as:

o Resource location

* Contact information provided to support agents or contained in customer support requests:

o Email addresses

o Telephone numbers

o Internet Protocol (IP) addresses

* Information shared with support agents as part of the support case interaction such as:

o Descriptions of technical issues

o Issue reproduction steps

Information shared to assist support agents with troubleshooting

Gisteren bij ons gemeld, dus vandaag afhandelen.

We hebben opgevraagd welke informatie het van PZH betreft (zie bijlage).

Graag jullie mening.

Mvg, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: donderdag 23 januari 2020 15:14
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 <mailt o art 5 1-2e pzh.nl> >
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: Microsoft database containing Customer Support data was accessible from the Internet

Dag art 5 1-2e

Dit zojuist met art 5 1-2e al besproken. Ik had een verkeerd antwoord naar art 5 1-2e gestuurd, ik dacht dat het om de melding ging die ik naar jou had gestuurd.

Deze ligt nu bij mij.

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 23 januari 2020 13:48
Aan: art 5 1-2e pzh.nl <mailt o 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> >; art 5 1-2e < art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> >
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Hallo art 5 1-2e

Om te beoordelen of dit ook voor ons een datalek is en hoe we hier mee om willen gaan is het nodig om exact te weten welke persoonsgegevens van PZH het betreft.

Wellicht heb je dat al gedaan, maar wil jij daartoe een Azure support request indienen?

Affected customers are being notified of this event. To obtain the data specific to your organization that were potentially exposed, please submit an Azure support request <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAzSCSupport&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229520464&sdata=Bhn5UN9hwdRveR5hXyV5cj0ei5sUCyF%2BuyG7NBP6PeU%3D&reserved=0>

Ik hoor graag.

Mvg, art 5 1-2e

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

Verzonden: donderdag 23 januari 2020 10:22
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 pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Dag art 5 1-2e

Deze is besproken met de betreffende specialist. Dit betreft de ontwikkelomgeving van het omgevingsbeleid. art 5 1-2e is op de hoogte.

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 23 januari 2020 10:02
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> >
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 <mailt o art 5 1-2e pzh.nl> >
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Beste art 5 1-2een art 5 1-2e

Hierbij wil ik even melden dat ik onderstaande email heb gekregen, ihkv security.

Ik kan niet zo goed inschatten wat ik hiermee moet.

Ik heb begrepen dat art 5 1-2e binnen ons team ook een identieke email heeft gehad.

Ik heb geprobeerd om onderstaand gegeven (Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256) op te zoeken

maar ik kan niet vinden waarvoor ik de id gebruik.

Ik weet wel dat ik gebruik maak van een gratis MSDN subscription die komt bij Visual Studio, om te oefen met Azure.

Daarnaast heeft art 5 1-2e mij aangemeld bij Microsoft support om call aan te kunnen maken.

Kunnen jullie laten weten of ik nog aanvullende acties moet ondernemen tgv deze email?

Alvast bedankt,

Groetjes

art 5 1-2e

art 5 1-2e

Tactisch Dataspecialist

Afdeling I&A | bureau Bedrijfsinformatie

T 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/>

I&A heeft een groep op het Binnenplein! De ‘groep I&A’ biedt nieuws, antwoorden op veelgestelde vragen en geeft tips.

Ook kun je bijvoorbeeld lezen over de projectboard en actuele I&A-projecten. Klik op het icoon om naar de groep te gaan en meld je aan als volger! Wil je meer weten over I&A-producten? Klik dan op het vraagtekenicoon waarmee je in de LearningGuide komt.
<http://binnenplein.pzh.nl/groepen/groep-i-en-a/>
<http://learningguide.pzh.local/html/introduction.htm>

Van: Microsoft Azure <azure-noreply@microsoft.com <mailto:azure-noreply@microsoft.com> >
Verzonden: woensdag 22 januari 2020 14:43
Aan: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019.

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoAzureGrey.png>

Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019. This issue was specific to an internal database used for support case analytics and does not represent an exposure of our commercial cloud services. Once identified, Microsoft mitigated the issue, and our security team’s investigation found no indication of malicious use of the database records. Our analysis of the support information indicates that specific personal or organizational identifiable information related to your support case was potentially visible.

You are receiving this message as an Azure account administrator or subscription administrator for this subscription. As a result of this issue, the support data exposed may include the following:

* System generated data related to support cases such as:

o Resource location

* Contact information provided to support agents or contained in customer support requests:

o Email addresses

o Telephone numbers

o Internet Protocol (IP) addresses

* Information shared with support agents as part of the support case interaction such as:

o Descriptions of technical issues

o Issue reproduction steps

o Information shared to assist support agents with troubleshooting

Affected customers are being notified of this event. To obtain the data specific

to your organization that were potentially exposed, please submit an Azure support request <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAzSCSupport&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229520464&sdata=Bhn5UN9hwdRveR5hXyV5cj0ei5sUCyF%2BuyG7NBP6PeU%3D&reserved=0> .

Summary of event

During the investigation, we determined that this information was potentially exposed due to a misconfiguration of network security group security rules.

Microsoft engineers determined that a change made to the database's network security group <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01%7 art 5 1-2e 0pzh.nl%7C636fec8244e54efacb66%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229530460&sdata=9kKkQLjMfEJ3MyDYkPLbr1PlrOcAiyMcq30Ept%2FTgYI%3D&reserved=0> on December 5, 2019 contained misconfigured security rules <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview%23security-rules&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=l9Md4n%2B6v2zgYrKVfL%2BdMSy%2BCahpIxcqq8DZ5TjbNF8%3D&reserved=0> that enabled exposure of the database information. Upon notification of the issue, engineers remediated the configuration on December 31, 2019 to restrict the database and prevent unauthorized access.

As part of Microsoft’s standard operating procedures, data stored in the database is redacted using automated tools to remove personal information. Our investigation confirmed that the vast majority of records were redacted as intended. In some scenarios, the data may have remained unredacted if it met specific conditions. An example of this occurs if the information is in a non-standard format, such as an email address separated with spaces instead of written in a standard format “XYZ @contoso com” vs “XYZ@contoso.com <mailto:XYZ@contoso.com> ”. We have begun notifications to customers whose data was present in this redacted database.

We are committed to the privacy and security of your data and are taking action to prevent future occurrences of this issue. These actions include:

* Audit the established network security rules for internal resources.

* Expand the scope of the mechanisms that detect security rule misconfigurations.

* Add additional alerting to service teams when security rule misconfigurations are detected.

* Implement additional redaction automation.

Misconfigurations are unfortunately a common error across the industry. We have solutions to help prevent this kind of mistake, but unfortunately, they were not enabled for this database. As we’ve learned, it is good to periodically review your configurations and ensure your own configurations and ensure you are taking

advantage of all protections available.

This documentation is included as general guidance and is not intended to be all-inclusive for how to configure your environment.

* Governing your Azure Workloads <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fazure.microsoft.com%2Fresources%2Fgoverning-your-azure-workloads%2F&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=w1J92sQy8TyywrpHaAURm4G3QNBoKvFSZUUPuJnG5dk%3D&reserved=0>

* Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=r7EzLvU%2FUftoDMNljzntMdRoakx%2F24ns5I50dLk5GCw%3D&reserved=0>

* Managing Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fmanage-network-security-group&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=UqHOt9DuECkE5QPUtxnoitvegUlGjVTUMBy%2B2JCaK7k%3D&reserved=0>

* Network Security Group Security Rules <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.co tual-network%2Fsecurity-overview%23security-rules&data=02%7C01%7 art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=4Tbs3JjNe7CRNMYR32FnphgUL8k1RfWZkCSY41iULLY%3D&reserved=0>

* Enabling Logging on Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fvirtual-network-nsg-manage-log&data=02%7C01%7 art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a7 0%7C1%7C0%7C637152974229560441&sdata=cp1XF2Am8jBspkJduR1DPZY41rVTvfdSeqcqngUVyLE%3D&reserved=0>

Account information

Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256

This message from Microsoft is an important part of a program, service, or product that you or your company purchased or participates in. Microsoft respects your privacy. Please read our Privacy Statement <https://eur03.safelinks.protection.outlook.com/?url=https%2Fprivacy.microsoft.com%2Fprivacystatement&data=02%7C01% art 5 1-2e %40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229560441&sdata=8LsJ7tItQ

yN8D2h6941QfVX%2FW8hsC1873OF4LoOh0UY%3D&reserved=0> .

This is a mandatory service communication. To set your contact preferences for other communications, visit the Promotional Communications Manager <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2 %2Faccount.microsoft.com%2Fprofile%2Fcontact-info&data=02%7C01% art 5 1-2e %40pzh.nl%7C636fec8244e54efacb6608d79f41117e %7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229570437&sdata=pdUZHtu0M uwXi%2F1XYPMM6Lh1%2B16gojSc1iV3UNFBjXQ%3D&reserved=0> .

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoMicrosoftGrey.png>

"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2020-01-24 16:24:39.925000+00:00
"Aan: art 5 1-2e ; art 5 1-2e
CC:
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet
"
Hallo art 5 1-2e en art 5 1-2e

Om te bepalen wat de omvang is, wil ik graag weten hoeveel van onze medewerkers meldingen over Azure doen bij Microsoft.

En als je dat zo weet op te lepelen wat de frequentie is; dagelijks 1, 10, 100 en de verwachte hoeveelheid meldingen?

Deze gegevens hebben we ook opgevraagd bij Microsoft, maar dat duurt even.

Besteed er weinig tijd aan. Als je het zo voor me kunt oplepelen dan is het goed.

Mvg, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: donderdag 23 januari 2020 12:58
Aan: art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Hi art 5 1-2e

Waren jullie in het privacyteam al op de hoogte van onderstaand bericht van art 5 1-2e

Naar aanleiding van art 5 1-2e s reactie: Volgens mij maakt het niet uit of het de ontwikkelomgeving is, maar als er persoonsgegevens worden verwerkt in deze omgeving, hebben we volgens mij mogelijk een AVG datalek?

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering en Automatisering | bureau Advies en Beleid

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

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 < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: donderdag 23 januari 2020 10:22
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 @pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Dag art 5 1-2e

Deze is besproken met de betreffende specialist. Dit betreft de ontwikkelomgeving van het omgevingsbeleid. art 5 1-2e is op de hoogte.

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 23 januari 2020 10:02
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> >
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 <mailt o art 5 1-2e @pzh.nl> >
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Beste art 5 1-2een art 5 1-2e

Hierbij wil ik even melden dat ik onderstaande email heb gekregen, ihkv security.

Ik kan niet zo goed inschatten wat ik hiermee moet.

Ik heb begrepen dat art 5 1-2e art 5 1-2e binnen ons team ook een identieke email heeft gehad.

Ik heb geprobeerd om onderstaand gegeven (Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256) op te zoeken

maar ik kan niet vinden waarvoor ik de id gebruik.

Ik weet wel dat ik gebruik maak van een gratis MSDN subscription die komt bij Visual Studio, om te oefen met Azure.

Daarnaast heeft art 5 1-2e mij aangemeld bij Microsoft support om call aan te kunnen maken.

Kunnen jullie laten weten of ik nog aanvullende acties moet ondernemen tgv deze email?

Alvast bedankt,

Groetjes

art 5 1-2e

art 5 1-2e

Tactisch Dataspecialist

Afdeling I&A | bureau Bedrijfsinformatie

T 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/>

I&A heeft een groep op het Binnenplein! De ‘groep I&A’ biedt nieuws, antwoorden op veelgestelde vragen en geeft tips.

Ook kun je bijvoorbeeld lezen over de projectboard en actuele I&A-projecten. Klik op het icoon om naar de groep te gaan en meld je aan als volger! Wil je meer weten over I&A-producten? Klik dan op het vraagtekenicoon waarmee je in de LearningGuide komt.
<http://binnenplein.pzh.nl/groepen/groep-i-en-a/>
<http://learningguide.pzh.local/html/introduction.htm>

Van: Microsoft Azure <azure-noreply@microsoft.com <mailto:azure-noreply@microsoft.com> >
Verzonden: woensdag 22 januari 2020 14:43
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019.

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoAzureGrey.png>

Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019. This issue was specific to an internal database used for support case analytics and does not represent an exposure of our commercial cloud services. Once identified, Microsoft mitigated the issue, and our security team’s investigation found no indication of malicious use of the database records. Our analysis of the support information indicates that specific personal or organizational identifiable information related to your support case was potentially visible.

You are receiving this message as an Azure account administrator or subscription administrator for this subscription. As a result of this issue, the support data exposed may include the following:

* System generated data related to support cases such as:

o Resource location

* Contact information provided to support agents or contained in customer support requests:

o Email addresses

o Telephone numbers

o Internet Protocol (IP) addresses

* Information shared with support agents as part of the support case interaction such as:

o Descriptions of technical issues

o Issue reproduction steps

o Information shared to assist support agents with troubleshooting

Affected customers are being notified of this event. To obtain the data specific to your organization that were potentially exposed, please submit an Azure support request <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAzSCSupport&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229520464&sdata=Bhn5UN9hwdRveR5hXyV5cj0ei5sUCyF%2BuyG7NBP6PeU%3D&reserved=0> .

Summary of event

During the investigation, we determined that this information was potentially exposed due to a misconfiguration of network security group security rules.

Microsoft engineers determined that a change made to the database's network security group <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb66%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229530460&sdata=9kKkQLjMfEJ3MyDYkPLbr1PlrOcAiyMcq30Ept%2FTgYI%3D&reserved=0> on December 5, 2019 contained misconfigured security rules <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.co tual-network%2Fsecurity-overview%23security-rules&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=l9Md4n%2B6v2zgYrKVfL%2BdMSy%2BCahpIxcqq8DZ5TjbNF8%3D&reserved=0> that enabled exposure of the database information. Upon notification of the issue, engineers remediated the configuration on December 31, 2019 to restrict the database and prevent unauthorized access.

As part of Microsoft’s standard operating procedures, data stored in the database is redacted using automated tools to remove personal information. Our investigation confirmed that the vast majority of records were redacted as intended. In some scenarios, the data may have remained unredacted if it met specific conditions. An example of this occurs if the information is in a non-standard format, such as an email address separated with spaces instead of written in a standard format “XYZ @contoso com” vs “XYZ@contoso.com <mailto:XYZ@contoso.com> ”. We have begun notifications to customers whose data was present in this redacted database.

We are committed to the privacy and security of your data and are taking action to prevent future occurrences of this issue. These actions include:

* Audit the established network security rules for internal resources.

* Expand the scope of the mechanisms that detect security rule misconfigurations.

* Add additional alerting to service teams when security rule misconfigurations are detected.

* Implement additional redaction automation.

Misconfigurations are unfortunately a common error across the industry. We have solutions to help prevent this kind of mistake, but unfortunately, they were not enabled for this database. As we've learned, it is good to periodically review your configurations and ensure your own configurations and ensure you are taking advantage of all protections available.

This documentation is included as general guidance and is not intended to be all-inclusive for how to configure your environment.

* Governing your Azure Workloads
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fazure.microsoft.com%2Fresources%2Fgoverning-your-azure-workloads%2F&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=w1J92sQy8TyywrpHaAURm4G3QNBoKvFSZUUPuJnG5dk%3D&reserved=0>

* Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs. Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=r7EzLvU%2FUftoDMNljzntMdRoakx%2F24ns5I50dLk5GCw%3D&reserved=0>

* Managing Network Security Groups
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fmanage-network-security-group&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=UqHOt9DuECkE5QPUtxnoitvegUlGjVTUMBy%2B2JCaK7k%3D&reserved=0>

* Network Security Group Security Rules
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.co ual-network%2Fsecurity-overview%23security-rules&data=02%7C01%7 art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=4Tbs3JjNe7CRNMYR32FnphgUL8k1RfWZkCSY41iULLY%3D&reserved=0>

* Enabling Logging on Network Security Groups
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft. irtual-network%2Fvirtual-network-nsg-manage-log&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229560441&sdata=cp1XF2Am8jBspkJduR1DPZY41rVTvfdSeqcqngUVyLE%3D&reserved=0>

Account information

Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256

%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229560441&sdata=8LsJ7tItQyN8D2h6941QfVX%2FW8hsC1873OF4LoOh0UY%3D&reserved=0> .

This is a mandatory service communication. To set your contact preferences for other communications, visit the Promotional Communications Manager <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faccount.microsoft.com%2Fprofile%2Fcontact-info&data=02%7C01%40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229570437&sdata=pdUZHtu0MuwXi%2F1XYPMM6Lh1%2B16gojSc1iV3UNFBjXQ%3D&reserved=0> .

art 5 1-2e

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoMicrosoftGrey.png>

"

"Van: art 5 1-2e
Verzonden: 2020-01-24 16:52:14.368000+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 , 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 die 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

"Van: art 5 1-2e
Verzonden: 2020-01-24 17:14:38.560000+00:00
"Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: Adviesrapport datalek
"
Hallo art 5 1-2een art 5 1-2e

Bijgaand het adviesrapport over het datalek.

Dit is afgestemd met de privacyjurist en wordt voorgelegd aan concerndirecteur art 5 1-2e

Dat is de procedure die we altijd volgen.

Aan hem is het om het advies te volgen danwel af te wijken.

Graag jullie op/aanmerking.

Ik begrijp dat het laat op de middag is. Vanavond stuur ik door aan de directeur.

Als ik nog geen reactie van jullie heb, zal ik dat er bij vermelden.

Met vriendelijke groet,

art 5 1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

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

art 5 1-2epzh.nl <mailto : art 5 1-2epzh.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 03516
Datum en tijdstip van de melding	:	Vrijdag 24 januari 2020 14:01
Route van de melding	:	Datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 24 januari 2020
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e privacy jurist)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerker art 5 1-2e afdelingshoofd)

Situatie

(*Korte beschrijving van de inbreuk op de beveiliging waarbij persoonsgegevens betrokken zijn)*
De secretaresses van Water en Groen hebben een gezamenlijk e-mail account.
Zij hebben in Outlook een lijst met (388) contactpersonen aangelegd, waar alleen zij 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 die 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.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	In totaal zijn er 388 contactpersonen opgevoerd onder het Outlook account van secrwaterengroen. Een steekproef toonde aan dat er persoonsgegevens in de notitievelden zijn opgevoerd, terwijl dat niet de bedoeling is. De situatie is met het afdelingshoofd besproken. Er is geen uitputtende analyse gedaan.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	6 secretaresses
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen
Welke persoonsgegevens betreft het?	Varieert per contactpersoon:

Vraag	Antwoord
	Inloggegevens, e-sign code, geboortedatum.
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.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Gezien de zakelijke context, goede bedoelingen en beperkte groep die toegang heeft gehad 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.	De secretaresses en het afedelingshoofd zijn er van op de hoogte gesteld dat het delen van dergelijke persoonsgegevens niet de bedoeling is.
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.

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] 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 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.
Gezien deze context
Gezien de zakelijke context, goede bedoelingen en beperkte groep die toegang heeft gehad achten wij de kans op misbruik en 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: 2020-01-24 17:24:54.888000+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e
Onderwerp: RE: Adviesrapport datalek
"
art 5 1-2e

Het is een nogal formele procedure, maar dat zijn we wettelijk verplicht.

Dit heeft geen negatieve consequenties voor jullie.

Alleen maar goed dat jullie dit soort dingen signaleren zodat we er iets aan kunnen doen!

Van: art 5 1-2e
Verzonden: vrijdag 24 januari 2020 17:15
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e @pzh.nl>
Onderwerp: Adviesrapport datalek

Hallo art 5 1-2een art 5 1-2e

Bijgaand het adviesrapport over het datalek.

Dit is afgestemd met de privacyjurist en wordt voorgelegd aan concerndirecteur art 5 1-2e

Dat is de procedure die we altijd volgen.

Aan hem is het om het advies te volgen danwel af te wijken.

Graag jullie op/aanmerking.

Ik begrijp dat het laat op de middag is. Vanavond stuur ik door aan de directeur.

Als ik nog geen reactie van jullie heb, zal ik dat er bij vermelden.

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

"Van: art 5 1-2e
Verzonden: 2020-01-24 18:07:06.700000+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
Onderwerp: RE: Aankondiging: adviesrapporten 2 datalekken komen er aan
"
Hallo art 5 1-2e

Bijgaand de bijbehorende adviesrapporten.

Ik hoor graag of je de adviezen volgt.

art 5 1-2e

Ik heb deze lijn van afhandeling zoals in bijlage 2 opgenomen vanmiddag met art 5 1-2e besproken en hem toegezegd dat hij eerst nog een blik op het rapport kan werpen.

Hij heeft daarvoor nog geen gelegenheid gehad.

Groet, art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 24 januari 2020 16:52
Aan: art 5 1-2e <art 5 1-2e pzh.nl>; 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>; art 5 1-2e < art 5 1-2e pzh.nl> ; art 5 1-2e
art 5 1-2e pzh.nl>
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 die 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

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 03548
Datum en tijdstip van de melding	:	Donderdag 23 januari 2020 10:02
Route van de melding	:	Eerst per e-mail. Later opnieuw geregistreerd via het Datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 24 januari 2020 18:00
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)*
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.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Nog onbekend.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Microsoft heeft geen misbruik kunnen constateren.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Nog onbekend
Welke persoonsgegevens betreft het?	We hebben bij Microsoft opgevraagd welke informatie het van PZH betreft, maar hebben nog geen antwoord. Volgens opgave van Microsoft betreft het mogelijk de volgende gegevens:

Vraag	Antwoord
	• System generated data related to support cases such as: o Resource location • Contact information provided to support agents or contained in customer support requests: o Email addresses o Telephone numbers o Internet Protocol (IP) addresses • Information shared with support agents as part of the support case interaction such as: o Descriptions of technical issues o Issue reproduction steps • Information shared to assist support agents with troubleshooting
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?	Microsoft heeft geen misbruik kunnen constateren.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Microsoft heeft geen misbruik kunnen constateren. 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 laag risico.
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 die in de betreffende database staan.
Betreft het een datalek?	Ja. Microsoft heeft geen misbruik kunnen constateren. Daarom achten wij onrechtmatige verwerking (misbruik van de

[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
	persoonsgegevens) onwaarschijnlijk, maar het kan niet uitgesloten worden, zodat er strikt genomen sprake is van een inbreuk in verband met persoonsgegevens (datalek) .
Ondernomen beperkende maatregelen.	Geen.
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.

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
Slechts enkele I&A medewerkers (<10) plaatsen wel eens support vragen bij Microsoft. De persoonsgegevens zijn niet gevoelig. Geregistreerd wordt naam, locatie, ip-adres en dergelijke. In de zakelijke context is dit ongevaarlijk en voor de betrokken persoon een laag risico.

In deze context achten wij de kans op misbruik en het hiermee verbonden risico voor de betrokkenen laag.

Microsoft geen misbruik kunnen constateren, maar geeft niet aan dat dit niet gebeurd is. Onrechtmatige verwerking is daarom 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.

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 03516
Datum en tijdstip van de melding	:	Vrijdag 24 januari 2020 14:01
Route van de melding	:	Datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 24 januari 2020
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e (privacy jurist)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerker art 5 1-2e del ingshoofd)

Situatie

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

De secretaresses van Water en Groen hebben een gezamenlijk e-mail account.
Zij hebben in Outlook een lijst met (388) contactpersonen aangelegd, waar alleen zij 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 bi art 5 1-2e e 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.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	In totaal zijn er 388 contactpersonen opgevoerd onder het Outlook account van secrwaterengroen. Een steekproef toonde aan dat er persoonsgegevens in de notitievelden zijn opgevoerd, terwijl dat niet de bedoeling is. De situatie is met het afdelingshoofd besproken. Er is geen uitputtende analyse gedaan.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	6 secretaresses
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen
Welke persoonsgegevens betreft het?	Varieert per contactpersoon:

Vraag	Antwoord
	Inloggegevens, e-sign code, geboortedatum.
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.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Gezien de zakelijke context, goede bedoelingen en beperkte groep die toegang heeft gehad 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.	De secretaresses en het afdelingshoofd zijn er van op de hoogte gesteld dat het delen van dergelijke persoonsgegevens niet de bedoeling is.
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.

[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
De persoonsgegevens zijn niet gevoelig.
Gezien de zakelijke context, goede bedoelingen en beperkte groep die toegang heeft gehad achten wij de kans op misbruik en 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 Privacy team 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: 2020-01-24 18:08:36.524000+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e ; art 5 1-2e art 5 1-2e ; art 5 1-2e
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet
"
Hallo art 5 1-2e

Dankjewel voor deze melding.

We hebben de situatie in het Privacy Team besproken en komen tot onderstaande conclusie.

Deze heb ik zojuist conform de procedure voor het afhandelen van datalekken aan de concerdirecteur voorgelegd.

Analyse van dit specifieke geval

Slechts enkele I&A medewerkers (<10) plaatsen wel eens support vragen bij Microsoft. De persoonsgegevens zijn niet gevoelig. Geregistreerd wordt naam, locatie, ip-adres en dergelijke. In de zakelijke context is dit ongevaarlijk en voor de betrokken persoon een laag risico.

In deze context achten wij de kans op misbruik en het hiermee verbonden risico voor de betrokkenen laag.

Microsoft geen misbruik kunnen constateren, maar geeft niet aan dat dit niet gebeurd is. Onrechtmatige verwerking is daarom 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.

Mvg, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: donderdag 23 januari 2020 10:02
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>; art 5 1-2e art 5 1-2e)pzh.nl>
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Beste art 5 1-2een art 5 1-2e

Hierbij wil ik even melden dat ik onderstaande email heb gekregen, ihkv security.

Ik kan niet zo goed inschatten wat ik hiermee moet.

Ik heb begrepen da art 5 1-2e innen ons team ook een identieke email heeft gehad.

Ik heb geprobeerd om onderstaand gegeven (Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256) op te zoeken

maar ik kan niet vinden waarvoor ik de id gebruik.

Ik weet wel dat ik gebruik maak van een gratis MSDN subscription die komt bij Visual Studio, om te oefen met Azure.

Daarnaast heeft art 5 1-2e mij aangemeld bij Microsoft support om call aan te kunnen maken.

Kunnen jullie laten weten of ik nog aanvullende acties moet ondernemen tgv deze email?

Alvast bedankt,

Groetjes

art 5 1-2e

art 5 1-2e

Tactisch Dataspecialist

Afdeling I&A | bureau Bedrijfsinformatie

T 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/>

I&A heeft een groep op het Binnenplein! De ‘groep I&A’ biedt nieuws, antwoorden op veelgestelde vragen en geeft tips.

Ook kun je bijvoorbeeld lezen over de projectboard en actuele I&A-projecten. Klik op het icoon om naar de groep te gaan en meld je aan als volger! Wil je meer weten over I&A-producten? Klik dan op het vraagtekenicoon waarmee je in de LearningGuide komt.
<http://binnenplein.pzh.nl/groepen/groep-i-en-a/>
<http://learningguide.pzh.local/html/introduction.htm>

Van: Microsoft Azure <azure-noreply@microsoft.com <mailto:azure-noreply@microsoft.com> >
Verzonden: woensdag 22 januari 2020 14:43
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019.

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoAzureGrey.png>

Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019. This issue was specific to an internal database used for support case analytics and does not represent an exposure of our commercial

cloud services. Once identified, Microsoft mitigated the issue, and our security team’s investigation found no indication of malicious use of the database records. Our analysis of the support information indicates that specific personal or organizational identifiable information related to your support case was potentially visible.

You are receiving this message as an Azure account administrator or subscription administrator for this subscription. As a result of this issue, the support data exposed may include the following:

* System generated data related to support cases such as:

o Resource location

* Contact information provided to support agents or contained in customer support requests:

o Email addresses

o Telephone numbers

o Internet Protocol (IP) addresses

* Information shared with support agents as part of the support case interaction such as:

o Descriptions of technical issues

o Issue reproduction steps

o Information shared to assist support agents with troubleshooting

Affected customers are being notified of this event. To obtain the data specific to your organization that were potentially exposed, please submit an Azure support request <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAzSCSupport&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229520464&sdata=Bhn5UN9hwdRveR5hXyV5cj0ei5sUCyF%2BuyG7NBP6PeU%3D&reserved=0> .

Summary of event

During the investigation, we determined that this information was potentially exposed due to a misconfiguration of network security group security rules.

Microsoft engineers determined that a change made to the database's network security group <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb66%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229530460&sdata=9kKkQLjMfEJ3MyDYkPLbr1PlrOcAiyMcq30Ept%2FTgYI%3D&reserved=0> on December 5, 2019 contained misconfigured security rules <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview%23security-rules&data=02%7C01%7 art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=l9Md4n%2B6v2zgYrKVfL%2BdMSy%2BCahpIxcqq8DZ5TjbNF8%3D&reserved=0> that enabled

exposure of the database information. Upon notification of the issue, engineers remediated the configuration on December 31, 2019 to restrict the database and prevent unauthorized access.

As part of Microsoft's standard operating procedures, data stored in the database is redacted using automated tools to remove personal information. Our investigation confirmed that the vast majority of records were redacted as intended. In some scenarios, the data may have remained unredacted if it met specific conditions. An example of this occurs if the information is in a non-standard format, such as an email address separated with spaces instead of written in a standard format "XYZ @contoso com" vs "XYZ@contoso.com <mailto:XYZ@contoso.com> ". We have begun notifications to customers whose data was present in this redacted database.

We are committed to the privacy and security of your data and are taking action to prevent future occurrences of this issue. These actions include:

* Audit the established network security rules for internal resources.

* Expand the scope of the mechanisms that detect security rule misconfigurations.

* Add additional alerting to service teams when security rule misconfigurations are detected.

* Implement additional redaction automation.

Misconfigurations are unfortunately a common error across the industry. We have solutions to help prevent this kind of mistake, but unfortunately, they were not enabled for this database. As we've learned, it is good to periodically review your configurations and ensure your own configurations and ensure you are taking advantage of all protections available.

This documentation is included as general guidance and is not intended to be all-inclusive for how to configure your environment.

* Governing your Azure Workloads <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fazure.microsoft.com%2Fresources%2Fgoverning-your-azure-workloads%2F&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=w1J92sQy8TyywrpHaAURm4G3QNBoKvFSZUUPuJnG5dk%3D&reserved=0>

* Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01%7 art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=r7EzLvU%2FUftoDMNljzntMdRoakx%2F24ns5I50dLk5GCw%3D&reserved=0>

* Managing Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fmanage-network-security-group&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=UqHOt9DuECkE5QPUtxnoitvegUlGjVTUMBy%2B2JCaK7k%3D&reserved=0>

* Network Security Group Security Rules <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview%23security-

rules&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a 7C1%7C0%7C637152974229550447&sdata=4Tbs3JjNe
7CRNMYR32FnphgUL8k1RfWZkCSY41iULLY%3D&reserved=0>

* Enabling Logging on Network Security Groups
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Fdocs.microsoft rtual-network%2Fvirtual-network-nsg-manage-
log&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a7 0%7C1%7C0%7C637152974229560441&sdata=cp1XF2Am8
jBspkJduR1DPZY41rVTvfdSeqcqngUVyLE%3D&reserved=0>

Account information

Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256

This message from Microsoft is an important part of a program, service, or product that you or your company purchased or participates in. Microsoft respects your privacy. Please read our Privacy Statement <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Fprivacy.microsoft.com%2Fprivacystatement&data=02%7C01 art 5 1-2e
%40pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229560441&sdata=8LsJ7tItQ
yN8D2h6941QfVX%2FW8hsC1873OF4LoOh0UY%3D&reserved=0> .

This is a mandatory service communication. To set your contact preferences for other communications, visit the Promotional Communications Manager <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Faccount.microsoft.com%2Fprofile%2Fcontact-info&data=02%7C01% art 5 1-2e
%40pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229570437&sdata=pdUZHtu0M
uwXi%2F1XYPMM6Lh1%2B16gojSc1iV3UNFBjXQ%3D&reserved=0> .

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoMicrosoftGrey.png>

"

"Van: art 5 1-2e
Verzonden: 2020-01-24 18:42:53.613000+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
Onderwerp: Re: Aankondiging: adviesrapporten 2 datalekken komen er aan
"
Heel scherp. Je hebt gelijk.

Outlook voor Android downloaden <https://aka.ms/ghei36>

_____

From: art 5 1-2e <art 5 1-2e pzh.nl>
Sent: Friday, January 24, 2020 6:27:11 PM
To: art 5 1-2e <art 5 1-2e pzh.nl>; 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>; art 5 1-2e <art 5 1-2e pzh.nl>
Subject: RE: Aankondiging: adviesrapporten 2 datalekken komen er aan

Dag art 5 1-2e

Bijna akkoord. Op zich volg ik je adviezen, maar in die mbt de secretaresses staat een inconsistentie: in de tekst lees ik “moet nog wel hersteld worden”, maar in de onderste regel van de tabel staat “verdere maatregelen niet nodig”. Ik ga ervanuit dat dit laatste een vergissing is en dat er wél hersteld wordt.

Hartelijke groet, art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: vrijdag 24 januari 2020 18:07
Aan: art 5 1-2e <art 5 1-2e pzh.nl>; 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>; art 5 1-2e art 5 1-2e pzh.nl>
Onderwerp: RE: Aankondiging: adviesrapporten 2 datalekken komen er aan

Hallo art 5 1-2e

Bijgaand de bijbehorende adviesrapporten.

Ik hoor graag of je de adviezen volgt.

art 5 1-2e

Ik heb deze lijn van afhandeling zoals in bijlage 2 opgenomen vanmiddag met art 5 1-2e besproken en hem toegezegd dat hij eerst nog een blik op het rapport kan werpen.

Hij heeft daarvoor nog geen gelegenheid gehad.

Groet, art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 24 januari 2020 16:52
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> >
CC: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl <mailto: art 5 1-2e pzh.nl>
>; art 5 1-2e <art 5 1-2e pzh.nl <mail t > >; 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 <mailt o art 5 1-2e pzh.nl> >
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 1-2 art 5 1-2edie 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


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2020-01-27 08:58:50.405000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet
"
Hallo art 5 1-2e dat klopt. Geen aanvullende actie nodig.

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: maandag 27 januari 2020 08:45
Aan: art 5 1-2e <art 5 1-2e pzh.nl>
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

art 5 1-2e

Bedankt voor je reactie.

Ik begrijp, obv van jou reactie, dat ik geen aanvullende actie hoe uit te voeren, tgv gemelde email van Microsoft.

Groetjes

art 5 1-2e

art 5 1-2e

Tactisch Dataspecialist

Afdeling I&A | bureau Bedrijfsinformatie

T 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/>

I&A heeft een groep op het Binnenplein! De ‘groep I&A’ biedt nieuws, antwoorden op veelgestelde vragen en geeft tips.

Ook kun je bijvoorbeeld lezen over de projectboard en actuele I&A-projecten. Klik op het icoon om naar de groep te gaan en meld je aan als volger! Wil je meer weten over I&A-producten? Klik dan op het vraagtekenicoon waarmee je in de LearningGuide komt.
<http://binnenplein.pzh.nl/groepen/groep-i-en-a/>
<http://learningguide.pzh.local/html/introduction.htm>

Van: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 24 januari 2020 18:09
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 <mail t >; art 5 1-2e <art 5 1-2e pzh.nl <mailto: art 5 1-2e pzh.nl> >; art 5 1-2e pzh.nl <mailto art 5 1-2e pzh.nl> >
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Hallo art 5 1-2e

Dankjewel voor deze melding.

We hebben de situatie in het Privacy Team besproken en komen tot onderstaande conclusie.

Deze heb ik zojuist conform de procedure voor het afhandelen van datalekken aan de concerdirecteur voorgelegd.

Analyse van dit specifieke geval

Slechts enkele I&A medewerkers (<10) plaatsen wel eens support vragen bij Microsoft. De persoonsgegevens zijn niet gevoelig. Geregistreerd wordt naam, locatie, ip-adres en dergelijke. In de zakelijke context is dit ongevaarlijk en voor de betrokken persoon een laag risico.

In deze context achten wij de kans op misbruik en het hiermee verbonden risico voor de betrokkenen laag.

Microsoft geen misbruik kunnen constateren, maar geeft niet aan dat dit niet gebeurd is. Onrechtmatige verwerking is daarom 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.

Mvg, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: donderdag 23 januari 2020 10:02
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> >
C 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: FW: Microsoft database containing Customer Support data was accessible from the Internet

Beste art 5 1-2een art 5 1-2e

Hierbij wil ik even melden dat ik onderstaande email heb gekregen, ihkv security.

Ik kan niet zo goed inschatten wat ik hiermee moet.

Ik heb begrepen dat art 5 1-2e binnen ons team ook een identieke email heeft gehad.

Ik heb geprobeerd om onderstaand gegeven (Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256) op te zoeken

maar ik kan niet vinden waarvoor ik de id gebruik.

Ik weet wel dat ik gebruik maak van een gratis MSDN subscription die komt bij

Visual Studio, om te oefen met Azure.

Daarnaast heeft art 5 1-2e mij aangemeld bij Microsoft support om call aan te kunnen maken.

Kunnen jullie laten weten of ik nog aanvullende acties moet ondernemen tgv deze email?

Alvast bedankt,

Groetjes

art 5 1-2e

art 5 1-2e

Tactisch Dataspecialist

Afdeling I&A | bureau Bedrijfsinformatie

T 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/>

I&A heeft een groep op het Binnenplein! De ‘groep I&A’ biedt nieuws, antwoorden op veelgestelde vragen en geeft tips.

Ook kun je bijvoorbeeld lezen over de projectboard en actuele I&A-projecten. Klik op het icoon om naar de groep te gaan en meld je aan als volger! Wil je meer weten over I&A-producten? Klik dan op het vraagtekenicoon waarmee je in de LearningGuide komt.
<http://binnenplein.pzh.nl/groepen/groep-i-en-a/>
<http://learningguide.pzh.local/html/introduction.htm>

Van: Microsoft Azure <azure-noreply@microsoft.com <mailto:azure-noreply@microsoft.com> >
Verzonden: woensdag 22 januari 2020 14:43
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019.

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoAzureGrey.png>

Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019. This issue was specific to an internal database used

for support case analytics and does not represent an exposure of our commercial cloud services. Once identified, Microsoft mitigated the issue, and our security team’s investigation found no indication of malicious use of the database records. Our analysis of the support information indicates that specific personal or organizational identifiable information related to your support case was potentially visible.

You are receiving this message as an Azure account administrator or subscription administrator for this subscription. As a result of this issue, the support data exposed may include the following:

* System generated data related to support cases such as:

o Resource location

* Contact information provided to support agents or contained in customer support requests:

o Email addresses

o Telephone numbers

o Internet Protocol (IP) addresses

* Information shared with support agents as part of the support case interaction such as:

o Descriptions of technical issues

o Issue reproduction steps

o Information shared to assist support agents with troubleshooting

Affected customers are being notified of this event. To obtain the data specific to your organization that were potentially exposed, please submit an Azure support request <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAzSCSupport&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229520464&sdata=Bhn5UN9hwdRveR5hXyV5cj0ei5sUCyF%2BuyG7NBP6PeU%3D&reserved=0> .

Summary of event

During the investigation, we determined that this information was potentially exposed due to a misconfiguration of network security group security rules.

Microsoft engineers determined that a change made to the database's network security group <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01%7 art 5 1-2e 0pzh.nl%7C636fec8244e54efacb66%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229530460&sdata=9kKkQLjMfEJ3MyDYkPLbr1PlrOcAiyMcq30Ept%2FTgYI%3D&reserved=0> on December 5, 2019 contained misconfigured security rules <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview%23security-rules&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=l9Md4n%2B6v2zgYrKVfL%2BdMSy%2BCahpIxcqq8DZ5TjbNF8%3D&reserved=0> that enabled exposure of the database information. Upon notification of the issue, engineers remediated the configuration on December 31, 2019 to restrict the database and prevent unauthorized access.

As part of Microsoft’s standard operating procedures, data stored in the database is redacted using automated tools to remove personal information. Our investigation confirmed that the vast majority of records were redacted as intended. In some scenarios, the data may have remained unredacted if it met specific conditions. An example of this occurs if the information is in a non-standard format, such as an email address separated with spaces instead of written in a standard format “XYZ @contoso com” vs “XYZ@contoso.com <mailto:XYZ@contoso.com> ”. We have begun notifications to customers whose data was present in this redacted database.

We are committed to the privacy and security of your data and are taking action to prevent future occurrences of this issue. These actions include:

* Audit the established network security rules for internal resources.

* Expand the scope of the mechanisms that detect security rule misconfigurations.

* Add additional alerting to service teams when security rule misconfigurations are detected.

* Implement additional redaction automation.

Misconfigurations are unfortunately a common error across the industry. We have solutions to help prevent this kind of mistake, but unfortunately, they were not enabled for this database. As we’ve learned, it is good to periodically review your configurations and ensure your own configurations and ensure you are taking advantage of all protections available.

This documentation is included as general guidance and is not intended to be all-inclusive for how to configure your environment.

* Governing your Azure Workloads <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fazure.microsoft s%2Fgoverning-your-azure-workloads%2F&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=w1J92sQy8TyywrpHaAURm4G3QNBoKvFSZUUPuJnG5dk%3D&reserved=0>

* Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=r7EzLvU%2FUftoDMNljzntMdRoakx%2F24ns5I50dLk5GCw%3D&reserved=0>

* Managing Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fmanage-network-security-group&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=UqHOt9DuECkE5QPUtxnoitvegUlGjVTUMBy%2B2JCaK7k%3D&reserved=0>

* Network Security Group Security Rules <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview%23security-rules&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=4Tbs3JjNe7CRNMYR32FnphgUL8k1RfWZkCSY41iULLY%3D&reserved=0>

* Enabling Logging on Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fvirtual-network-nsg-manage-

log&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229560441&sdata=cp1XF2Am8
jBspkJduR1DPZY41rVTvfdSeqcqngUVyLE%3D&reserved=0>

Account information

Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256

This message from Microsoft is an important part of a program, service, or product that you or your company purchased or participates in. Microsoft respects your privacy. Please read our Privacy Statement <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Fprivacy.microsoft.com%2Fprivacystatement&data=02%7C01 art 5 1-2e
%40pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229560441&sdata=8LsJ7tItQ
yN8D2h6941QfVX%2FW8hsC1873OF4LoOh0UY%3D&reserved=0> .

This is a mandatory service communication. To set your contact preferences for other communications, visit the Promotional Communications Manager <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Faccount.microsoft.com%2Fprofile%2Fcontact-info&data=02%7C01% art 5 1-2e
%40pzh.nl%7C636fec8244e54efacb6608d79f41117e
%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229570437&sdata=pdUZHtu0M
uwXi%2F1XYPMM6Lh1%2B16gojSc1iV3UNFBjXQ%3D&reserved=0> .

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoMicrosoftGrey.png>

"

"Van: art 5 1-2e
Verzonden: 2020-01-27 09:00:41.264000+00:00
"Aan: art 5 1-2e art 5 1-2e
CC:
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet
"
Microsoft heeft niets aangetroffen, maar is het daarmee uit te sluiten?

Tja, hoe gaan we daar mee om?

Ik wilde er vrijdagmiddag vanaf zijn en heb toch een advies opgesteld voor art 5 1-2e en dit vrijdagmiddag aan hem gemaild.

Hierin benoem ik het als datalek, maar wel met de opmerking dat we de gegevens van Microsoft nog niet hebben ontvangen.

Hij is akkoord.

Ik hoop niet dat ik hiermee een precedent heb veroorzaakt.

Mvg art 5 1-2e

Van: art 5 1-2e art 5 1-2e pzh.nl>
Verzonden: maandag 27 januari 2020 08:19
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Ik lees wat anders in deze definitiebepaling. Als we de verzekering krijgen dat er niets met persoonsgegevens is gebeurd is het m.i. geen datalek, maar een beveiligingsincident.

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 24 januari 2020 15:30
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 < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Daar verschillen we toch van mening. Het is m.i. wel een datalek, maar niet een die gemeld hoeft te worden aan de AP. Althans niet op grond van deze informatie. Ik begreep dat art 5 1-2e nog zit te wachten op nadere informatie van Microsoft.

Art 4, lid 12 AVG zegt dat een inbreuk in verband met persoonsgegevens ook is “de ongeoorloofde toegang tot , opgeslagen of anderszins verwerkte gegevens”. In dit geval is niet uit te sluiten dat er toegang is geweest. De database heeft 3 weken open gestaan.

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 <pem . art 5 1-2e pzh.nl <mailt o art 5 1-2e)pzh.nl> >
Verzonden: vrijdag 24 januari 2020 13:37
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> >
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Mag ik uit het onderstaande afleiden dat er niets met de persoonsgegevens is gebeurd? Zo dat het geval is, dan reikt het toch niet verder dan een beveiligingsincident. Verwijs ook naar de eerdere discussie rondom Citrix.

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: vrijdag 24 januari 2020 10:54
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> >
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet
Urgentie: Hoog

Heren,

Mogelijk een datalek bij Microsoft.

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

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

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

Staat inmiddels weer dicht.

Betreft mogelijk de volgende gegevens:

* System generated data related to support cases such as:

o Resource location

* Contact information provided to support agents or contained in customer support requests:

o Email addresses

o Telephone numbers

o Internet Protocol (IP) addresses

* Information shared with support agents as part of the support case interaction such as:

o Descriptions of technical issues

o Issue reproduction steps

Information shared to assist support agents with troubleshooting

Gisteren bij ons gemeld, dus vandaag afhandelen.

We hebben opgevraagd welke informatie het van PZH betreft (zie bijlage).

Graag jullie mening.

Mvg, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: donderdag 23 januari 2020 15:14
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 <mailt o art 5 1-2e pzh.nl> > 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> >
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Dag art 5 1-2e

Dit zojuist met art 5 1-2e al besproken. Ik had een verkeerd antwoord naar art 5 1-2e gestuurd, ik dacht dat het om de melding ging die ik naar jou had gestuurd.

Deze ligt nu bij mij.

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 23 januari 2020 13:48
Aan: art 5 1-2e pzh.nl <mailt o 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 <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> >
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Hallo art 5 1-2e

Om te beoordelen of dit ook voor ons een datalek is en hoe we hier mee om willen gaan is het nodig om exact te weten welke persoonsgegevens van PZH het betreft.

Wellicht heb je dat al gedaan, maar wil jij daartoe een Azure support request indienen?

Affected customers are being notified of this event. To obtain the data specific to your organization that were potentially exposed, please submit an Azure support request <https://eur03.safelin tlook.com/?url=https%3A%2F%2Faka.ms%2FAzSCSupport&data=02%7C01% art 5 1-2e 0pzh.nl %7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229520464&sdata=Bhn5UN9hwdRveR5hXyV5cj0ei5sUCyF%2BuyG7NBP6PeU%3D&reserved=0>

Ik hoor graag.

Mvg, art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: donderdag 23 januari 2020 10:22
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 pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Dag art 5 1-2e

Deze is besproken met de betreffende specialist. Dit betreft de ontwikkelomgeving van het omgevingsbeleid. art 5 1-2e is op de hoogte.

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 23 januari 2020 10:02
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> >
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 <mailt o art 5 1-2e pzh.nl> >
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Beste art 5 1-2en art 5 1-2e

Hierbij wil ik even melden dat ik onderstaande email heb gekregen, ihkv security.

Ik kan niet zo goed inschatten wat ik hiermee moet.

Ik heb begrepen dat art 5 1-2e binnen ons team ook een identieke email heeft gehad.

Ik heb geprobeerd om onderstaand gegeven (Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256) op te zoeken

maar ik kan niet vinden waarvoor ik de id gebruik.

Ik weet wel dat ik gebruik maak van een gratis MSDN subscription die komt bij Visual Studio, om te oefen met Azure.

Daarnaast heeft art 5 1-2e mij aangemeld bij Microsoft support om call aan te kunnen maken.

Kunnen jullie laten weten of ik nog aanvullende acties moet ondernemen tgv deze email?

Alvast bedankt,

Groetjes

art 5 1-2e

art 5 1-2e

Tactisch Dataspecialist

Afdeling I&A | bureau Bedrijfsinformatie

T 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/>

I&A heeft een groep op het Binnenplein! De ‘groep I&A’ biedt nieuws, antwoorden op veelgestelde vragen en geeft tips.

Ook kun je bijvoorbeeld lezen over de projectboard en actuele I&A-projecten. Klik op het icoon om naar de groep te gaan en meld je aan als volger! Wil je meer weten over I&A-producten? Klik dan op het vraagtekenicoon waarmee je in de LearningGuide komt.
<http://binnenplein.pzh.nl/groepen/groep-i-en-a/>
<http://learningguide.pzh.local/html/introduction.htm>

Van: Microsoft Azure <azure-noreply@microsoft.com <mailto:azure-noreply@microsoft.com> >
Verzonden: woensdag 22 januari 2020 14:43
Aan: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Onderwerp: Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019.

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoAzureGrey.png>

Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019. This issue was specific to an internal database used for support case analytics and does not represent an exposure of our commercial cloud services. Once identified, Microsoft mitigated the issue, and our security team’s investigation found no indication of malicious use of the database records. Our analysis of the support information indicates that specific personal or organizational identifiable information related to your support case was potentially visible.

You are receiving this message as an Azure account administrator or subscription administrator for this subscription. As a result of this issue, the support data exposed may include the following:

* System generated data related to support cases such as:

o Resource location

* Contact information provided to support agents or contained in customer support requests:

o Email addresses

o Telephone numbers

o Internet Protocol (IP) addresses

* Information shared with support agents as part of the support case interaction such as:

o Descriptions of technical issues

o Issue reproduction steps

o Information shared to assist support agents with troubleshooting

Affected customers are being notified of this event. To obtain the data specific to your organization that were potentially exposed, please submit an Azure support request <https://eur03.safeli utlook.com/?url=https%3A%2F%2Faka.ms%2FAzSCSupport&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229520464&sdata=Bhn5UN9hwdRveR5hXyV5cj0ei5sUCyF%2BuyG7NBP6PeU%3D&reserved=0> .

Summary of event

During the investigation, we determined that this information was potentially exposed due to a misconfiguration of network security group security rules.

Microsoft engineers determined that a change made to the database's network security group <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229530460&sdata=9kKkQLjMfEJ3MyDYkPLbr1PlrOcAiyMcq30Ept%2FTgYI%3D&reserved=0> on December 5, 2019 contained misconfigured security rules <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview%23security-rules&data=02%7C01%7 art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=l9Md4n%2B6v2zgYrKVfL%2BdMSy%2BCahpIxcqq8DZ5TjbNF8%3D&reserved=0> that enabled exposure of the database information. Upon notification of the issue, engineers remediated the configuration on December 31, 2019 to restrict the database and prevent unauthorized access.

As part of Microsoft’s standard operating procedures, data stored in the database is redacted using automated tools to remove personal information. Our investigation confirmed that the vast majority of records were redacted as intended. In some scenarios, the data may have remained unredacted if it met specific conditions. An example of this occurs if the information is in a non-standard format, such as an email address separated with spaces instead of written in a standard format “XYZ @contoso com” vs “XYZ@contoso.com <mailto:XYZ@contoso.com> ”. We have begun notifications to customers whose data was present in this redacted database.

We are committed to the privacy and security of your data and are taking action to prevent future occurrences of this issue. These actions include:

* Audit the established network security rules for internal resources.

* Expand the scope of the mechanisms that detect security rule misconfigurations.

* Add additional alerting to service teams when security rule misconfigurations are detected.

* Implement additional redaction automation.

Misconfigurations are unfortunately a common error across the industry. We have solutions to help prevent this kind of mistake, but unfortunately, they were not enabled for this database. As we've learned, it is good to periodically review your configurations and ensure your own configurations and ensure you are taking advantage of all protections available.

This documentation is included as general guidance and is not intended to be all-inclusive for how to configure your environment.

* Governing your Azure Workloads
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fazure.microsoft.com%2Fresources%2Fgoverning-your-azure-workloads%2F&data=02%7C01% art 5 1-2e 0pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229540454&sdata=w1J92sQy8TyywrpHaAURm4G3QNBoKvFSZUUPuJnG5dk%3D&reserved=0>

* Network Security Groups <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fsecurity-overview&data=02%7C01%7 art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=r7EzLvU%2FUftoDMNljzntMdRoakx%2F24ns5I50dLk5GCw%3D&reserved=0>

* Managing Network Security Groups
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fmanage-network-security-group&data=02%7C01%7 art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229550447&sdata=UqHOt9DuECkE5QPUtxnoitvegUlGjVTUMBy%2B2JCaK7k%3D&reserved=0>

* Network Security Group Security Rules
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.co tual-network%2Fsecurity-overview%23security-rules&data=02%7C01%7 art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a5 %7C1%7C0%7C637152974229550447&sdata=4Tbs3JjNe7CRNMYR32FnphgUL8k1RfWZkCSY41iULLY%3D&reserved=0>

* Enabling Logging on Network Security Groups
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fazure%2Fvirtual-network%2Fvirtual-network-nsg-manage-log&data=02%7C01% art 5 1-2e 40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229560441&sdata=cp1XF2Am8jBspkJduR1DPZY41rVTvfdSeqcqngUVyLE%3D&reserved=0>

Account information

Subscription Id: ed375c5a-f5d1-4069-90a9-c75052651256

%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229560441&sdata=8LsJ7tItQyN8D2h6941QfVX%2FW8hsC1873OF4LoOh0UY%3D&reserved=0> .

This is a mandatory service communication. To set your contact preferences for other communications, visit the Promotional Communications Manager <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2%2Faccount.microsoft.com%2Fprofile%2Fcontact-info&data=02%7C01% art 5 1-2e %40pzh.nl%7C636fec8244e54efacb6608d79f41117e%7C6d99bc288f284a73a50163a8e1eb3040%7C1%7C0%7C637152974229570437&sdata=pdUZHtu0MuwXi%2F1XYPMM6Lh1%2B16gojSc1iV3UNFBjXQ%3D&reserved=0> .

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

<https://cxpsncdn1.azureedge.net/cxpsnemail/LogoMicrosoftGrey.png>

"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2020-01-24 18:07:06.700000+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
Onderwerp: RE: Aankondiging: adviesrapporten 2 datalekken komen er aan
"

Hallo art 5 1-2e

Bijgaand de bijbehorende adviesrapporten.

Ik hoor graag of je de adviezen volgt.

art 5 1-2e

Ik heb deze lijn van afhandeling zoals in bijlage 2 opgenomen vanmiddag met art 5 1-2e besproken en hem toegezegd dat hij eerst nog een blik op het rapport kan werpen.

Hij heeft daarvoor nog geen gelegenheid gehad.

Groet, art 5 1-2e

Van: art 5 1-2e
Verzonden: vrijdag 24 januari 2020 16:52
Aan: art 5 1-2e <art 5 1-2e pzh.nl> ; art 5 1-2e art 5 1-2e pzh.nl>
CC: Zoete - van der Hout, WH, de <art 5 1-2e pzh. n
<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: 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 die 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

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 03548
Datum en tijdstip van de melding	:	Donderdag 23 januari 2020 10:02
Route van de melding	:	Eerst per e-mail. Later opnieuw geregistreerd via het Datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 24 januari 2020 18:00
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)*
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.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Nog onbekend.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Microsoft heeft geen misbruik kunnen constateren.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Nog onbekend
Welke persoonsgegevens betreft het?	We hebben bij Microsoft opgevraagd welke informatie het van PZH betreft, maar hebben nog geen antwoord. Volgens opgave van Microsoft betreft het mogelijk de volgende gegevens:

Vraag	Antwoord
	• System generated data related to support cases such as: o Resource location • Contact information provided to support agents or contained in customer support requests: o Email addresses o Telephone numbers o Internet Protocol (IP) addresses • Information shared with support agents as part of the support case interaction such as: o Descriptions of technical issues o Issue reproduction steps • Information shared to assist support agents with troubleshooting
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?	Microsoft heeft geen misbruik kunnen constateren.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Microsoft heeft geen misbruik kunnen constateren. 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 laag risico.
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 die in de betreffende database staan.
Betreft het een datalek?	Ja. Microsoft heeft geen misbruik kunnen constateren. Daarom achten wij onrechtmatige verwerking (misbruik van de

[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
	persoonsgegevens) onwaarschijnlijk, maar het kan niet uitgesloten worden, zodat er strikt genomen sprake is van een inbreuk in verband met persoonsgegevens (datalek) .
Ondernomen beperkende maatregelen.	Geen.
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.

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
Slechts enkele I&A medewerkers (<10) plaatsen wel eens support vragen bij Microsoft. De persoonsgegevens zijn niet gevoelig. Geregistreerd wordt naam, locatie, ip-adres en dergelijke. In de zakelijke context is dit ongevaarlijk en voor de betrokken persoon een laag risico.

In deze context achten wij de kans op misbruik en het hiermee verbonden risico voor de betrokkenen laag.

Microsoft geen misbruik kunnen constateren, maar geeft niet aan dat dit niet gebeurd is. Onrechtmatige verwerking is daarom 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.

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 03516
Datum en tijdstip van de melding	:	Vrijdag 24 januari 2020 14:01
Route van de melding	:	Datalek formulier (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Vrijdag 24 januari 2020
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e (privacy jurist)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerker, art 5 1-2e afdel ingshoofd)

Situatie

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

De secretaresses van Water en Groen hebben een gezamenlijk e-mail account.
Zij hebben in Outlook een lijst met (388) contactpersonen aangelegd, waar alleen zij 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 di e 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 me 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.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	In totaal zijn er 388 contactpersonen opgevoerd onder het Outlook account van secrwaterengroen. Een steekproef toonde aan dat er persoonsgegevens in de notitievelden zijn opgevoerd, terwijl dat niet de bedoeling is. De situatie is met het afdelingshoofd besproken. Er is geen uitputtende analyse gedaan.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	6 secretaresses
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen
Welke persoonsgegevens betreft het?	Varieert per contactpersoon:

Vraag	Antwoord
	Inloggegevens, e-sign code, geboortedatum.
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.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Gezien de zakelijke context, goede bedoelingen en beperkte groep die toegang heeft gehad 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.	De secretaresses en het afdelingshoofd zijn er van op de hoogte gesteld dat het delen van dergelijke persoonsgegevens niet de bedoeling is.
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.

[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
De persoonsgegevens zijn niet gevoelig.
Gezien de zakelijke context, goede bedoelingen en beperkte groep die toegang heeft gehad achten wij de kans op misbruik en 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 Privacy team 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.

art 5 1-2e

Van: art 5 1-2e
Verzonden: 0 10:40
Aan: art 5 1-2e art 5 1-2e
Onderwerp: o s contai ning Customer Support data was accessible from the Internet

Ok, helder.

Van: art 5 1-2e <art 5 1-2e @ pzh.nl>
Verzonden: maandag 27 januari 2020 10:19
Aan: art 5 1-2e <art 5 1-2e pzh.nl>; art 5 1-2e <art 5 1-2e @pzh.n l>
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Dag art 5 1-2e,

Ik heb hier zojuist met art 5 1-2e over gesproken.
Voor dit specifieke geval zijn wij tot de conclusie gekomen dat het een datalek betreft, omdat het openstaan van de database ontdekt is door een externe, derde partij. Hiermee is duidelijk dat het onbevoegde toegang betreft.
Het feit dat MS niets heeft aangetroffen geeft aan dat wij geen verdere melding bij de AP hoeven te doen.

Je kunt dus gerust zijn, je hebt geen precedent geschapen

Met vriendelijke groet,

art 5 1-2e
Functionaris voor Gegevensbescherming

M art 5 1-2e
art 5 1-2@pzh .nl

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

Van: art 5 1-2e <art 5 1-2e pzh. nl>
Verzonden: maandag 27 januari 2020 09:01
Aan: art 5 1-2e <art 5 1-2e @pzh.nl>; art 5 1-2e <art 5 1-2e @pzh. nl>
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Microsoft heeft niets aangetroffen, maar is het daarmee uit te sluiten?
Tja, hoe gaan we daar mee om?

Ik wilde er vrijdagmiddag vanaf zijn en heb toch een advies opgesteld voor art 5 1-2e en dit vrijdagmiddag aan hem gemaild.
Hierin benoem ik het als datalek, maar wel met de opmerking dat we de gegevens van Microsoft nog niet hebben ontvangen.
Hij is akkoord.

Ik hoop niet dat ik hiermee een precedent heb veroorzaakt.
Mvg art 5 1-2e

Van: art 5 1-2e art 5 1-2e pzh.nl>
Verzonden: maandag 27 januari 2020 08:19
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e @pzh.nl>
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Ik lees wat anders in deze definitiebepaling. Als we de verzekering krijgen dat er niets met persoonsgegevens is gebeurd is het m.i. geen datalek, maar een beveiligingsincident.

Van: art 5 1-2e < art 5 1-2e pzh.nl>
Verzonden: vrijdag 24 januari 2020 15:30
Aan: art 5 1-2e < art 5 1-2e zh.nl>; art 5 1-2e < art 5 1-2e pzh.nl >
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Daar verschillen we toch van mening. Het is m.i. wel een datalek, maar niet een die gemeld hoeft te worden aan de AP. Althans niet op grond van deze informatie. Ik begreep dat art 5 1-2e n og zit te wachten op nadere informatie van Microsoft.
Art 4, lid 12 AVG zegt dat een inbreuk in verband met persoonsgegevens ook is “de ongeoorloofde toegang tot … , opgeslagen of anderszins verwerkte gegevens”. In dit geval is niet uit te sluiten dat er toegang is geweest. De database heeft 3 weken open gestaan.

Met vriendelijke groet,

art 5 1-2e
Functionaris voor Gegevensbescherming

M art 5 1-2e
art 5 1-2e@pzh .nl

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

Van: art 5 1-2e < art 5 1-2e @pzh.nl>
Verzonden: vrijdag 24 januari 2020 13:37
Aan: art 5 1-2e < art 5 1-2e pzh.nl>; art 5 1-2e < art 5 1-2e @pzh .nl>
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Mag ik uit het onderstaande afleiden dat er niets met de persoonsgegevens is gebeurd? Zo dat het geval is, dan reikt het toch niet verder dan een beveiligingsincident. Verwijs ook naar de eerdere discussie rondom Citrix.

Van: art 5 1-2e < art 5 1-2e pzh. nl>
Verzonden: vrijdag 24 januari 2020 10:54
Aan: art 5 1-2e < art 5 1-2e @pzh.nl>; art 5 1-2e < art 5 1-2e @pzh.nl>
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet
Urgentie: Hoog

Heren,

Mogelijk een datalek bij Microsoft.

Betreft een interne database van Microsoft die ze gebruiken voor analyse over support calls die klanten over het Azure platform hebben ingediend bij Microsoft.
Die informatie wordt normaal gesproken geanonimiseerd opgenomen in de database, maar daar zijn uitzonderingen op.

De database stond een kleine maand open. Microsoft heeft onderzoek gedaan en geen misbruik kunnen constateren. Staat inmiddels weer dicht.

Betreft mogelijk de volgende gegevens:

- System generated data related to support cases such as:
  - Resource location
- Contact information provided to support agents or contained in customer support requests:
  - Email addresses
  - Telephone numbers
  - Internet Protocol (IP) addresses
- Information shared with support agents as part of the support case interaction such as:
  - Descriptions of technical issues
  - Issue reproduction steps

Information shared to assist support agents with troubleshooting

Gisteren bij ons gemeld, dus vandaag afhandelen.
We hebben opgevraagd welke informatie het van PZH betreft (zie bijlage).

Graag jullie mening.

Mvg, art 5 1-2e

Van: art 5 1-2e <art 5 1-2e @pzh.nl>
Verzonden: donderdag 23 januari 2020 15:14
Aan: art 5 1-2e <art 5 1-2e pzh.nl>; art 5 1-2e @pzh. nl>
CC: art 5 1-2e @pzh. nl>; art 5 1-2e <art 5 1-2e @pzh .nl>
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Dag art 5 1-2e

Dit zojuist met art 5 1-2e art 5 1-2e al besproken. Ik had een verkeerd antwoord naar art 5 1-2e gestuurd, ik dacht dat het om de melding ging die ik naar jou had gestuurd.

Deze ligt nu bij mij.

Groeten,

art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh. nl>
Verzonden: donderdag 23 januari 2020 13:48
Aan art 5 1-2e @ pzh.nl>
CC: art 5 1-2e <art 5 1-2e @pzh.nl >; art 5 1-2e @pzh.nl>; art 5 1-2e <art 5 1-2e @pzh.nl>
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Hallo art 5 1-2e

Om te beoordelen of dit ook voor ons een datalek is en hoe we hier mee om willen gaan is het nodig om exact te weten welke persoonsgegevens van PZH het betreft.
Wellicht heb je dat al gedaan, maar wil jij daartoe een Azure support request indienen?

Affected customers are being notified of this event. To obtain the data specific to your organization that were potentially exposed, please submit an Azure support request

Ik hoor graag.

Mvg, art 5 1-2e

Van: art 5 1-2e <art 5 1-2e @pzh.nl>
Verzonden: donderdag 23 januari 2020 10:22
Aan: 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>
CC: art 5 1-2e @pzh. nl>
Onderwerp: RE: Microsoft database containing Customer Support data was accessible from the Internet

Dag art 5 1-2e

Deze is besproken met de betreffende specialist. Dit betreft de ontwikkelomgeving van het omgevingsbeleid. art 5 1-2e is op de hoogte.

Groeten,

art 5 1-2e

Van: art 5 1-2e <art 5 1-2e @pz h.nl>
Verzonden: donderdag 23 januari 2020 10:02
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 <art 5 1-2e @pzh.nl > art 5 1-2e @pzh.nl>
Onderwerp: FW: Microsoft database containing Customer Support data was accessible from the Internet

Beste art 5 1-2e en art 5 1-2e art 5 1-2e

Hierbij wil ik even melden dat ik onderstaande email heb gekregen, ihkv security.
Ik kan niet zo goed inschatten wat ik hiermee moet.
Ik heb begrepen dat art 5 1-2e binnen ons team ook een identieke email heeft gehad.

Ik heb geprobeerd om onderstaand gegeven (**Subscription Id:** ed375c5a-f5d1-4069-90a9-c75052651256) op te zoeken
maar ik kan niet vinden waarvoor ik de id gebruik.
Ik weet wel dat ik gebruik maak van een gratis MSDN subscription die komt bij Visual Studio, om te oefen met Azure.
Daarnaast heeft art 5 1-2e mij aangemeld bij Micro soft support om call aan te kunnen maken.

Kunnen jullie laten weten of ik nog aanvullende acties moet ondernemen tgv deze email?

Alvast bedankt,

Groetjes

art 5 1-2e

art 5 1-2e
Tactisch Dataspecialist

Afdeling I&A | bureau Bedrijfsinformatie
T art 5 1-2e
art 5 1-2e @ pzh.nl

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

I&A heeft een groep op het Binnenplein! De 'groep I&A' biedt nieuws, antwoorden op veelgestelde vragen en geeft tips.

Ook kun je bijvoorbeeld lezen over de projectboard en actuele I&A-projecten. Klik op het icoon om naar de groep te gaan en meld je aan als volger! Wil je meer weten over I&A-producten? Klik dan op het vraagtekenicoon waarmee je in de LearningGuide komt.

Van: Microsoft Azure <azure-noreply@microsoft.com>
Verzonden: woensdag 22 januari 2020 14:43
Aan: art 5 1-2e <art 5 1-2e @pz_h.nl>
Onderwerp: Microsoft database containing Customer Support data was accessible from the Internet

Microsoft Azure

Microsoft database containing Customer Support data was accessible from the Internet

Microsoft has corrected an issue identified by a third-party security researcher where a database containing a subset of information related to customer support interactions was accessible to the internet between the dates of December 5, 2019 and December 31, 2019. This issue was specific to an internal database used for support case analytics and does not represent an exposure of our commercial cloud services. Once identified, Microsoft mitigated the issue, and our security team's investigation found no indication of malicious use of the database records. Our analysis of the support information indicates that specific personal or organizational identifiable information related to your support case was potentially visible.

You are receiving this message as an Azure account administrator or subscription administrator for this subscription. As a result of this issue, the support data exposed may include the following:

- System generated data related to support cases such as:
  - Resource location
- Contact information provided to support agents or contained in customer support requests:
  - Email addresses
  - Telephone numbers
  - Internet Protocol (IP) addresses
- Information shared with support agents as part of the support case interaction such as:
  - Descriptions of technical issues

- Issue reproduction steps
- Information shared to assist support agents with troubleshooting

Affected customers are being notified of this event. To obtain the data specific to your organization that were potentially exposed, please submit an Azure support request.

Summary of event

During the investigation, we determined that this information was potentially exposed due to a misconfiguration of network security group security rules.

Microsoft engineers determined that a change made to the database's network security group on December 5, 2019 contained misconfigured security rules that enabled exposure of the database information. Upon notification of the issue, engineers remediated the configuration on December 31, 2019 to restrict the database and prevent unauthorized access.

As part of Microsoft's standard operating procedures, data stored in the database is redacted using automated tools to remove personal information. Our investigation confirmed that the vast majority of records were redacted as intended. In some scenarios, the data may have remained unredacted if it met specific conditions. An example of this occurs if the information is in a non-standard format, such as an email address separated with spaces instead of written in a standard format "XYZ @contoso com" vs "XYZ@contoso.com". We have begun notifications to customers whose data was present in this redacted database.

We are committed to the privacy and security of your data and are taking action to prevent future occurrences of this issue. These actions include:

- Audit the established network security rules for internal resources.
- Expand the scope of the mechanisms that detect security rule misconfigurations.
- Add additional alerting to service teams when security rule misconfigurations are detected.
- Implement additional redaction automation.

Misconfigurations are unfortunately a common error across the industry. We have solutions to help prevent this kind of mistake, but unfortunately, they were not enabled for this database. As we've learned, it is good to periodically review your configurations and ensure your own configurations and ensure you are taking advantage of all protections available.

This documentation is included as general guidance and is not intended to be all-inclusive for how to configure your environment.

- Governing your Azure Workloads

- Network Security Groups
- Managing Network Security Groups
- Network Security Group Security Rules
- Enabling Logging on Network Security Groups

Account information

Subscription Id: art 5 1-2e

"Van: art 5 1-2e
Verzonden: 2020-03-17 14:25:22.339000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Er is een melding van een Datalek ontvangen. (M20 03 01909)
"
Ha art 5 1-2e weet je of 'de verkeerde art 5 1-2e le werkgeversverklaring heeft geopend?

Van: art 5 1-2e
Verzonden: dinsdag 17 maart 2020 11:43
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>; art 5 1-2e < art 5 1-2e pzh.nl>
Onderwerp: RE: Er is een melding van een Datalek ontvangen. (M20 03 01909)

Ha art 5 1-2e

Mee eens dat het een datalek is dat we intern afhandelen.

Ik stel het advies op, leg dit voor aan art 5 1-2e en registreer het in het logboek..

Wil jij de acties vanuit P&O richting beide dame art 5 1-2e organiseren?

* Vragen om verwijderen mail
* Aandringen op zorgvuldigheid bij de betreffende collega's die verantwoordelijk zijn voor werkgeversverklaringen
* Schriftelijk excuus (kan wat mij betreft per e-mail)

Mvg, art 5 1-2e

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: maandag 16 maart 2020 14:28
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> >
Onderwerp: RE: Er is een melding van een Datalek ontvangen. (M20 03 01909)

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

Ik verwacht hiervan geen risico voor betrokkenen

bsn-nummer is meest gevoelig item

nu extra bekent bij 1 andere medewerker via mail

Opvolging bestaat wat mij betreft uit diverse zaken

1 bij de andere art 5 1-2e econtroleerd documenten uit mail laten verwijderen (dus meekijken) en verslag hiervan naar de goede art 5 1-2e

2 nogmaals nadrukkelijk op Personeelsplein communiceren dat verzending aan verkeerde medewerker een datalek is en dat dit gemeld moet worden

3 registreren maar niet melden AP

4 schriftelijk excuus naar goede art 5 1-2e anuit P&O

Gelet op de huidige situatie kan ik 1 helaas niet uitvoeren (ik zit thuis en mag niet naar buiten)

Voor 2 zal ik een hoge urgentie mail naar leidinggevende sturen ter doorzending (graag meelezen)

Zijn

Met vriendelijke groet,

art 5 1-2e

Informatiebeheerder P&O,

Provincie Zuid-Holland.

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

Tel. Nummer: art 5 1-2e

Niet aanwezig op woensdagen

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: maandag 16 maart 2020 14:13
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> > ; 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: FW: Er is een melding van een Datalek ontvangen. (M20 03 01909)

Hallo art 5 1-2e

Er is een datalek melding gedaan door een collega m.b.t. het verzenden van een werkgeversverklaring aan de verkeerde persoon (intern).

De oorzaak ligt binnen P&O.

Zou jij deze willen oppakken en een advies geven hoe te handelen?

Mvg, art 5 1-2e

Van: loket@pzh.nl <mailto:loket@pzh.nl> <loket@pzh.nl <mailto:loket@pzh.nl> >
Verzonden: maandag 16 maart 2020 11:16
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 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)pzh.nl
<mailto: art 5 1-2e pzh.nl> >
Onderwerp: Er is een melding van een Datalek ontvangen. (M20 03 01909)

Beste collega,

Er is een melding van een Datalek ontvangen.

Melden datalek: M20 03 01909

Je kunt deze hier <https://loket.pzh.nl/tas/secure/contained/incident?unid=4eb9797ca0f842d0ab83d77c40144f04> behandelen.

Met vriendelijke groet,

Het Loket

<HTTPS://loket.pzh.nl/tas/images/email_footer.jpg>

Het Loket telefoon 070 4417777 loket.pzh.nl <https://loket.pzh.nl>

"Van: art 5 1-2e
Verzonden: 2020-03-17 15:03:43.527000+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 03 01909
Datum en tijdstip van de melding	:	Maandag 16 maart 2020 11:15
Route van de melding	:	Datalek formulier

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Dinsdag 17 maart 2020 13:40
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e (privacy jurist), art 5 1-2e (privacy officer P&O)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerker

Situatie

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

art 5 1-2e heeft bij P&O een werkgeversverklaring aangevraagd. Op 16 maart 2020 om 09:30 is de door haar aangevraagde verklaring door P&O aan de verkeerde collega met dezelfde achternaam gemaild.

Zij vermeld hierbij: “Dit is niet de eerste keer dat er vertrouwelijke,persoonlijke en financiële informatie naar haar is gestuurd, die voor mij bestemd was.”

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Naam, salarisgegevens, BSN
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?	Naam, salarisgegevens, BSN

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.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Het voor collega's zichtbaar zijn van salarisgegevens wordt niet beoordeeld als een hoog risico voor de betrokkenen. Deze informatie is indirect af te leiden uit de functie van de medewerker.
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.	De privacy officer van P&O heeft : - de P&O collega's gewezen op de noodzaak van zorgvuldig mailen van dergelijke informatie. - De ontvanger van de informatie gevraagd deze te verwijderen.
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.

[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.

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. Een provinciemedewerker heeft kennis kunnen nemen van de salarisinformatie en het BSN van een collega.
Salarisinformatie is indirect af te leiden uit de functie die iemand bij de provincie bekleed. Het risico is laag. Onrechtmatige verwerking van het BSN nummer door de PZH-collega die de e-mail ten onrechte heeft ontvangen en die hierover door de privacy officer is benaderd, achten wij onwaarschijnlijk en het hiermee verbonden risico voor de betrokkene niet 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 niet het geval.

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 niet te melden bij de Autoriteit Persoonsgegevens.

"Van: art 5 1-2e
Verzonden: 2020-03-17 16:30:32.450000+00:00
"Aan: art 5 1-2e
CC:
Onderwerp: RE: Er is een melding van een Datalek ontvangen. (M20 03 01909)
"
Dank, ik heb het advies inmiddels aan art 5 1-2e gemaild

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: dinsdag 17 maart 2020 16:29
Aan: art 5 1-2e <art 5 1-2e pzh.nl>
Onderwerp: RE: Er is een melding van een Datalek ontvangen. (M20 03 01909)

Ha art 5 1-2e

Ik was even weg de reden waarom is gelegen in het feit dat er maar 1 persoon bij betrokken is geweest. En op basis van de verstrekte info ook geen reden is om aan te nemen dat er meerdere mensen bij betrokken zijn geweest. Bij mijn weten zijn er ook geen meldingen aan de AP gemaakt van de verkeerd verzonden mails tussen art 5 1-2e

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 <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: dinsdag 17 maart 2020 14:35
Aan: art 5 1-2e <art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >; art 5 1-2e <pem. art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: RE: Er is een melding van een Datalek ontvangen. (M20 03 01909)

De AP zegt dit:

Met het BSN kan gemakkelijk een koppeling worden gemaakt tussen informatie uit verschillende bestanden. Onzorgvuldig gebruik van het BSN brengt daarom privacyrisico’s met zich mee. Bijvoorbeeld misbruik van persoonsgegevens en identiteitsfraude.

Van: art 5 1-2e
Verzonden: dinsdag 17 maart 2020 14:32
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 <mailt o art 5 1-2e pzh.nl> >
Onderwerp: RE: Er is een melding van een Datalek ontvangen. (M20 03 01909)

Wat is de reden om niet te melden aan de AP? Ik heb het nu als volgt geformuleerd.

Maar waarom onwaarschijnlijk?

Analyse van dit specifieke geval

Een provinciemedewerker heeft kennis kunnen nemen van de salarisinformatie en het BSN van een collega. Salarisinformatie is indirect af te leiden uit de functie die iemand bij de provincie bekleed. Het risico is laag.

Onrechtmatige verwerking van het BSN nummer door de PZH-collega achten wij onwaarschijnlijk en het hiermee verbonden risico voor de betrokkene niet hoog.

Onrechtmatige verwerking is echter nooit 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.
* De melding en beoordeling zoals gebruikelijk te administreren in het provinciale logboek.

Van: art 5 1-2e < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: maandag 16 maart 2020 16:40
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 art 5 1-2e pzh.nl <mailt o art 5 1-2e pzh.nl> >
Onderwerp: RE: Er is een melding van een Datalek ontvangen. (M20 03 01909)

Dag art 5 1-2e

Ik ben het ermee eens dat dit een datalek is dat ook als zodanig wordt geregistreerd.

Een melding aan de AP is niet noodzakelijk.

Naast de maatregelen die art 5 1-2e al heeft genoemd in haar laatste mail, van 14:28u, denk ik dat we ook in gesprek zouden moeten gaan met I&A over de naamgeving van de emailadressen. Er zijn meerdere gevallen bekend van (intern) de verwisseling van personen en emailadressen.

Buiten de excuses van P&O lijkt het mij ook goed dat we art 5 1-2e en wellicht ook art 5 1-2e , op de hoogte stellen van onze acties en maatregelen.

Wil jij dat voor je rekening nemen?

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 < art 5 1-2e pzh.nl <mailto : art 5 1-2e pzh.nl> >
Verzonden: maandag 16 maart 2020 14:13
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> > ; 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: FW: Er is een melding van een Datalek ontvangen. (M20 03 01909)

Hallo art 5 1-2e

Er is een datalek melding gedaan door een collega m.b.t. het verzenden van een werkgeversverklaring aan de verkeerde persoon (intern).

De oorzaak ligt binnen P&O.

Zou jij deze willen oppakken en een advies geven hoe te handelen?

Mvg, art 5 1-2e

Van: loket@pzh.nl <mailto:loket@pzh.nl> <loket@pzh.nl <mailto:loket@pzh.nl> >
Verzonden: maandag 16 maart 2020 11:16
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 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 pzh.nl <mailto: art 5 1-2e pzh.nl> >
Onderwerp: Er is een melding van een Datalek ontvangen. (M20 03 01909)

Beste collega,

Er is een melding van een Datalek ontvangen.

Melden datalek: M20 03 01909

Je kunt deze hier <https://loket.pzh.nl/tas/secure/contained/incident?unid=4eb9797ca0f842d0ab83d77c40144f04> behandelen.

Met vriendelijke groet,

Het Loket

<HTTPS://loket.pzh.nl/tas/images/email_footer.jpg>

Het Loket telefoon 070 4417777 loket.pzh.nl <https://loket.pzh.nl>
"


provincie
ZUID HOLLAND

"Van: art 5 1-2e
Verzonden: 2020-03-17 16:36:19.401000+00:00
"Aan: art 5 1-2e ; art 5 1-2e gmail.com"
CC:
Onderwerp: FYI: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Ter info. Het advies ligt bij art 5 1-2e

Document staat in de PT map.

Van: art 5 1-2e
Verzonden: dinsdag 17 maart 2020 15:04
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 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

"Van: art 5 1-2e
Verzonden: 2020-03-17 19:09:56+00:00
"Aan: art 5 1-2e
"CC: art 5 1-2e Zoete - van der Hout, WH, de"
Onderwerp: FW: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Ha art 5 1-2e dankjulliewel!, ik volg jullie advies, hartelijke groet, art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: dinsdag 17 maart 2020 15:04
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 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 03 01909
Datum en tijdstip van de melding	:	Maandag 16 maart 2020 11:15
Route van de melding	:	Datalek formulier

Advies

Opgesteld door	:	art 5 1-2e
Datum en tijdstip advies	:	Dinsdag 17 maart 2020 13:40
Advies besproken met	:	art 5 1-2e (FG), art 5 1-2e (privacy jurist), art 5 1-2e (privacy officer P&O)
Strekking advies ter kennisgeving gedeeld met	:	Betrokken medewerker

Situatie

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

art 5 1-2e heeft bij P&O een werkgeversverklaring aangevraagd. Op 16 maart 2020 om 09:30 is de door haar aangevraagde verklaring door P&O aan de verkeerde collega met dezelfde achternaam gemaild.

Zij vermeld hierbij: “Dit is niet de eerste keer dat er vertrouwelijke,persoonlijke en financiële informatie naar haar is gestuurd, die voor mij bestemd was.”

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	Naam, salarisgegevens, BSN
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?	Naam, salarisgegevens, BSN

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.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. Het voor collega's zichtbaar zijn van salarisgegevens wordt niet beoordeeld als een hoog risico voor de betrokkenen. Deze informatie is indirect af te leiden uit de functie van de medewerker.
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.	De privacy officer van P&O heeft : - de P&O collega's gewezen op de noodzaak van zorgvuldig mailen van dergelijke informatie. - De ontvanger van de informatie gevraagd deze te verwijderen.
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.

[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.

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. Een provinciemedewerker heeft kennis kunnen nemen van de salarisinformatie en het BSN van een collega.
Salarisinformatie is indirect af te leiden uit de functie die iemand bij de provincie bekleed. Het risico is laag. Onrechtmatige verwerking van het BSN nummer door de PZH-collega die de e-mail ten onrechte heeft ontvangen en die hierover door de privacy officer is benaderd, achten wij onwaarschijnlijk en het hiermee verbonden risico voor de betrokkene niet 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 niet het geval.

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 niet te melden bij de Autoriteit Persoonsgegevens.

"Van: Zoete - van der Hout, WH, de"
Verzonden: 2020-03-17 19:10:58+00:00
"Aan: art 5 1-2e art 5 1-2e
"CC: art 5 1-2e
Onderwerp: Re: Advies aan concerndirecteur in het kader van de meldplicht datalekken
"
Snelle actie. Dank jullie wel

Willy de Zoete

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: dinsdag, maart 17, 2020 7:09 PM
Aan: art 5 1-2e
CC: art 5 1-2e Zoete - van der Hout, WH, de
Onderwerp: FW: Advies aan concerndirecteur in het kader van de meldplicht datalekken

Ha art 5 1-2e dankjulliewel!, ik volg jullie advies, hartelijke groet, art 5 1-2e

Van: art 5 1-2e <art 5 1-2e pzh.nl>
Verzonden: dinsdag 17 maart 2020 15:04
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 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