GROEP GEGEVENSBESCHERMING ARTIKEL 29

18/NL

WP250rev.01

Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679

Goedgekeurd op 3 oktober 2017

Laatstelijk herzien en goedgekeurd op 6 februari 2018

Deze Groep is opgericht krachtens artikel 29 van Richtlijn 95/46/EG. Zij is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en privacy. Haar taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en artikel 15 van Richtlijn 2002/58/EG.

Het secretariaat wordt verzorgd door directoraat C (Grondrechten en burgerschap van de Unie) van het directoraat-generaal Justitie van de Europese Commissie, 1049 Brussel, België, kamer MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_nl.htm

DE GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS

ingesteld bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995,

gezien de artikelen 29 en 30,

gezien het reglement van orde van de groep,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD:

INHOUDSOPGAVE

INLEIDING

Met de algemene verordening gegevensbescherming (de AVG) wordt de verplichting ingevoerd om een inbreuk in verband met persoonsgegevens (hierna "inbreuk" genoemd) te melden aan de bevoegde nationale toezichthoudende autoriteit[1] (of, in het geval van een grensoverschrijdende inbreuk, aan de leidende toezichthoudende autoriteit) en, in bepaalde gevallen, om de inbreuk mee te delen aan de personen op wier persoonsgegevens de inbreuk betrekking heeft.

Momenteel bestaan er voor bepaalde organisaties, zoals aanbieders van openbare elektronische-communicatiediensten (zoals gespecificeerd in Richtlijn 2009/136/EG en Verordening (EU) nr. 611/2013), kennisgevingsverplichtingen in geval van inbreuken[2]. Er zijn ook enkele EU-lidstaten die al een eigen nationale meldingsplicht voor inbreuken hebben. Dit kan de verplichting omvatten om inbreuken te melden waarbij naast aanbieders van openbare elektronische-communicatiediensten bepaalde categorieën van verwerkingsverantwoordelijken betrokken zijn (bijvoorbeeld in Duitsland en Italië), of een verplichting om alle inbreuken waarbij persoonsgegevens betrokken zijn te melden (zoals in Nederland). In andere lidstaten kunnen relevante praktijkcodes bestaan (bijvoorbeeld in Ierland[3]). Hoewel een aantal gegevensbeschermingsautoriteiten in de EU verwerkingsverantwoordelijken momenteel aanmoedigen om inbreuken te melden, bevat gegevensbeschermingsrichtlijn 95/46/EG[4], die door de AVG wordt vervangen, geen specifieke verplichting om inbreuken te melden. Een dergelijke verplichting zal dus voor veel organisaties nieuw zijn. De AVG legt nu een meldingsplicht op aan alle verwerkingsverantwoordelijken, tenzij het onwaarschijnlijk is dat een inbreuk een risico voor de rechten en vrijheden van natuurlijke personen inhoudt[5]. Verwerkers hebben ook een belangrijke rol te spelen en moeten elke inbreuk aan hun verwerkingsverantwoordelijke melden[6].

De Groep gegevensbescherming artikel 29 (WP29) is van mening dat de nieuwe meldingsplicht een aantal voordelen heeft. Bij de melding aan de toezichthoudende autoriteit kunnen verwerkingsverantwoordelijken advies inwinnen over de vraag of de getroffen personen moeten worden geïnformeerd. De toezichthoudende autoriteit kan de verwerkingsverantwoordelijke immers gelasten om deze personen van de inbreuk in kennis te stellen[7]. Wanneer een verwerkingsverantwoordelijke een inbreuk aan personen meedeelt, kan hij informatie verstrekken over de risico's die de inbreuk met zich meebrengt en over de maatregelen die deze personen kunnen nemen om zich tegen de mogelijke gevolgen ervan te beschermen. Elk reactieplan voor inbreuken moet vooral gericht zijn op de bescherming van personen en hun persoonsgegevens. Melding van

[1] Zie artikel 4, lid 21, van de AVG.

[2] Zie http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:32009L0136 en http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32013R0611

[3] Zie https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] Zie http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:31995L0046

[5] De rechten die zijn verankerd in het Handvest van de grondrechten van de Europese Unie, dat beschikbaar is op http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:12012P/TXT

[6] Zie artikel 33, lid 2. Dit is qua concept vergelijkbaar met artikel 5 van Verordening (EU) nr. 611/2013, waarin is bepaald dat een aanbieder aan wie de levering van een deel van een elektronische-communicatiedienst wordt uitbesteed (zonder een directe contractuele relatie met abonnees te hebben) verplicht is een inbreuk in verband met persoonsgegevens aan de uitbestedende aanbieder te melden.

[7] Zie artikel 34, lid 4, en artikel 58, lid 2, onder e).

inbreuken moet dan ook worden gezien als een middel om de naleving van de regels in verband met de bescherming van persoonsgegevens te verbeteren. Tegelijkertijd dient te worden opgemerkt dat het niet melden van een inbreuk aan een natuurlijk persoon of een toezichthoudende autoriteit kan betekenen dat op grond van artikel 83 een mogelijke sanctie van toepassing is op de verwerkingsverantwoordelijke.

Verwerkingsverantwoordelijken en verwerkers worden daarom aangemoedigd vooraf te plannen en procedures op te zetten om een inbreuk te kunnen opsporen en onmiddellijk in te perken, het risico voor personen te beoordelen[8], en vervolgens te bepalen of het nodig is de bevoegde toezichthoudende autoriteit daarvan in kennis te stellen en de inbreuk zo nodig aan de betrokkenen mee te delen. Kennisgeving aan de toezichthoudende autoriteit dient deel uit te maken van dat reactieplan voor inbreuken.

De AVG bevat bepalingen met betrekking tot wanneer en aan wie een inbreuk moet worden gemeld en welke informatie in het kader van de melding moet worden verstrekt. De voor de melding vereiste informatie kan in stappen worden verstrekt, maar de verwerkingsverantwoordelijken moeten in elk geval tijdig op elke inbreuk reageren.

In zijn advies 03/2014 over de melding van inbreuken in verband met persoonsgegevens[9] heeft de WP29 richtsnoeren verstrekt om verwerkingsverantwoordelijken te helpen beslissen of betrokkenen in geval van een inbreuk daarvan in kennis moeten worden gesteld. In het advies werd ingegaan op de verplichting voor aanbieders van elektronische-communicatiediensten met betrekking tot Richtlijn 2002/58/EG. Daarnaast werden in het advies voorbeelden uit meerdere sectoren gegeven, in de context van het toenmalige ontwerpvoorstel voor de AVG, en werden goede praktijken voor alle verwerkingsverantwoordelijken gepresenteerd.

De huidige richtsnoeren bevatten een toelichting van de in de AVG opgenomen verplichting om inbreuken te melden en mee te delen en van enkele stappen die verwerkingsverantwoordelijken en verwerkers kunnen nemen om aan deze nieuwe verplichtingen te voldoen. In die richtsnoeren worden ook voorbeelden gegeven van verschillende soorten inbreuken en wordt vermeld wie in de verschillende scenario's in kennis dient te worden gesteld.

I. Melding van inbreuken in verband met persoonsgegevens krachtens de AVG

A. Basisbeschouwingen inzake veiligheid

Een van de vereisten van de AVG is dat persoonsgegevens met behulp van passende technische en organisatorische maatregelen op zodanige wijze worden verwerkt dat een passende beveiliging van de persoonsgegevens wordt gewaarborgd, met inbegrip van bescherming tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging[10].

[8] Dit kan worden gewaarborgd in het kader van de monitoring- en evaluatieverplichting van een gegevensbeschermingseffectbeoordeling, die vereist is voor verwerkingen die waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen inhouden (artikel 35, art.5.1 -1e en 11).

[9] Zie advies 03/2014 over de melding van inbreuken in verband met persoonsgegevens: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] Zie artikel 5, lid 1, onder f), en artikel 32.

Daarom vereist de AVG dat zowel verwerkingsverantwoordelijken als verwerkers passende technische en organisatorische maatregelen nemen om een beveiligingsniveau te waarborgen dat is afgestemd op het risico dat aan de verwerking van de persoonsgegevens is verbonden. Zij dienen rekening te houden met de stand van de techniek, de uitvoeringskosten, de aard, omvang, context en verwerkingsdoeleinden alsook de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen[11]. Krachtens de AVG moeten ook alle passende technische en organisatorische maatregelen worden genomen om onmiddellijk vast te stellen of een inbreuk heeft plaatsgevonden, op basis waarvan vervolgens wordt bepaald of de meldingsplicht van toepassing is.[12]

Een essentieel element van elk gegevensbeveiligingsbeleid is dat men in staat is een inbreuk waar mogelijk te voorkomen en, wanneer toch een inbreuk plaatsvindt, er tijdig op te reageren.

B. Wat is een inbreuk in verband met persoonsgegevens?

1. Definitie

Een verwerkingsverantwoordelijke kan pas een poging ondernemen om een inbreuk aan te pakken als hij in staat is er een te herkennen. In artikel 4, lid 12, van de AVG wordt een "inbreuk in verband met persoonsgegevens" als volgt gedefinieerd:

> "een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens".

Wat wordt bedoeld met "vernietiging" van persoonsgegevens zou heel duidelijk moeten zijn: dit betekent dat de gegevens niet langer bestaan, of niet langer bestaan in een vorm die voor de verwerkingsverantwoordelijke van nut is. "Beschadiging" zou ook relatief duidelijk moeten zijn: dit betekent dat de persoonsgegevens zijn gewijzigd, gecorrumpeerd of niet langer volledig zijn. "Verlies" van persoonsgegevens betekent dat de gegevens mogelijk nog steeds bestaan, maar dat de verwerkingsverantwoordelijke niet langer controle heeft over of toegang heeft tot de gegevens of dat hij ze niet langer in zijn bezit heeft. Ten slotte kan ongeoorloofde of onrechtmatige verwerking betrekking hebben op de verstrekking van persoonsgegevens aan (of de toegang tot persoonsgegevens door) ontvangers die niet gemachtigd zijn om de gegevens te ontvangen (of er toegang toe te hebben), of enige andere vorm van verwerking die in strijd is met de AVG.

Voorbeeld:

Een voorbeeld van verlies van persoonsgegevens is wanneer een apparaat met daarop een kopie van het klantenbestand van een verwerkingsverantwoordelijke is zoekgeraakt of gestolen. Een ander voorbeeld van verlies is als de enige kopie van een verzameling persoonsgegevens door gijzelsoftware ("ransomware") is versleuteld, of door de verwerkingsverantwoordelijke is versleuteld met behulp van een sleutel die hij niet langer in zijn bezit heeft.

Wat duidelijk moet zijn, is dat een inbreuk een soort veiligheidsincident is. Zoals aangegeven in artikel 4, lid 12, is de AVG echter alleen van toepassing wanneer er sprake is van een inbreuk op *persoonsgegevens*. Het gevolg van een dergelijke inbreuk is dat de verwerkingsverantwoordelijke niet zal kunnen waarborgen dat de beginselen met betrekking tot de verwerking van persoonsgegevens als

[11] Artikel 32; zie ook overweging 83

[12] Zie overweging 87.

omschreven in artikel 5 van de AVG worden nageleefd. Dit benadrukt het verschil tussen een veiligheidsincident en een inbreuk in verband met persoonsgegevens – het komt er in wezen op neer dat alle inbreuken in verband met persoonsgegevens veiligheidsincidenten zijn, maar dat niet alle veiligheidsincidenten noodzakelijkerwijs inbreuken in verband met persoonsgegevens zijn[13].

De mogelijke nadelige gevolgen van een inbreuk voor personen worden hieronder behandeld.

2. Soorten inbreuken in verband met persoonsgegevens

In zijn advies 03/2014 betreffende de melding van inbreuken heeft de WP29 uitgelegd dat inbreuken kunnen worden ingedeeld volgens de volgende drie bekende informatiebeveiligingsprincipes[14]:

- "Inbreuk op de vertrouwelijkheid" – als er sprake is van ongeoorloofde of onbedoelde verstrekking van of toegang tot persoonsgegevens.
- "Inbreuk op de integriteit" – als er sprake is van een ongeoorloofde of onopzettelijke wijziging van persoonsgegevens.
- "Inbreuk op de beschikbaarheid" – als er sprake is van een onopzettelijk of ongeoorloofd verlies van toegang tot persoonsgegevens of een onopzettelijke of ongeoorloofde vernietiging van persoonsgegevens.[15]

Er zij ook op gewezen dat, afhankelijk van de omstandigheden, een inbreuk tegelijkertijd betrekking kan hebben op de vertrouwelijkheid, de integriteit en de beschikbaarheid van persoonsgegevens, alsook op elke combinatie daarvan.

Terwijl het relatief duidelijk is of er sprake is van een inbreuk op de vertrouwelijkheid of integriteit, kan het minder voor de hand liggen of er sprake is van een inbreuk op de beschikbaarheid. Een inbreuk wordt altijd beschouwd als een inbreuk op de beschikbaarheid als persoonsgegevens permanent verloren zijn of zijn vernietigd.

Voorbeeld:

Voorbeelden van verlies van beschikbaarheid zijn wanneer gegevens per ongeluk of door een onbevoegde persoon zijn verwijderd of wanneer, in het geval van veilig versleutelde gegevens, de decodeersleutel is verloren gegaan. Als de verwerkingsverantwoordelijke de toegang tot de gegevens niet kan herstellen, bijvoorbeeld vanaf een back-up, dan wordt dit beschouwd als een permanent verlies van beschikbaarheid.

[13] Opgemerkt dient te worden dat een veiligheidsincident niet beperkt is tot dreigingsmodellen waarbij een organisatie van buitenaf wordt aangevallen, maar ook incidenten omvat die voortvloeien uit interne verwerking en een inbreuk vormen op beveiligingsprincipes.

[14] Zie advies 03/2014.

[15] Het is een vaststaand feit dat "toegang" fundamenteel deel uitmaakt van "beschikbaarheid". Zie bijvoorbeeld NIST SP800-53rev4, waarin beschikbaarheid als volgt wordt gedefinieerd: "Het verzekeren van tijdige en betrouwbare toegang tot en een tijdig en betrouwbaar gebruik van informatie", beschikbaar op http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. In CNSSI-4009 wordt ook verwezen naar: "Tijdige en betrouwbare toegang tot gegevens en informatiediensten voor gemachtigde gebruikers." Zie https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. In ISO/IEC 27000:2016 wordt "beschikbaarheid" ook gedefinieerd als "Op verzoek van een gemachtigde entiteit toegankelijk en bruikbaar zijn": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Er kan ook sprake zijn van verlies van beschikbaarheid als de normale dienstverlening van een organisatie ernstig is verstoord, bijvoorbeeld in het geval van een stroomstoring of een "denial of service"-aanval (DoS-aanval), waardoor persoonsgegevens niet beschikbaar zijn.

De vraag kan worden gesteld of een tijdelijk verlies van beschikbaarheid van persoonsgegevens moet worden beschouwd als een inbreuk en, zo ja, als een inbreuk die moet worden gemeld. In artikel 32 van de AVG, "Beveiliging van de verwerking", wordt uitgelegd dat bij de uitvoering van technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, onder meer aandacht moet worden besteed aan "het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen" en "het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen".

Een veiligheidsincident dat tot gevolg heeft dat persoonsgegevens gedurende een bepaalde periode niet beschikbaar zijn, is bijgevolg ook een vorm van inbreuk, aangezien de ontoegankelijkheid van de gegevens aanzienlijke gevolgen kan hebben voor de rechten en vrijheden van natuurlijke personen. Voor alle duidelijkheid: indien persoonsgegevens niet beschikbaar zijn als gevolg van de uitvoering van gepland systeemonderhoud, is dat geen "inbreuk op de beveiliging" zoals gedefinieerd in artikel 4, lid 12.

Net als bij een permanent verlies of vernietiging van persoonsgegevens (of enige andere vorm van inbreuk) moet een inbreuk die een tijdelijk verlies van beschikbaarheid meebrengt, worden gedocumenteerd overeenkomstig artikel 33, lid 5. Dit helpt de verwerkingsverantwoordelijke om verantwoording af te leggen aan de toezichthoudende autoriteit, die om inzage in deze documenten kan vragen[16]. Afhankelijk van de omstandigheden van de inbreuk kan het echter al dan niet verplicht zijn de inbreuk aan de toezichthoudende autoriteit te melden en aan de getroffen personen mee te delen. De verwerkingsverantwoordelijke zal moeten beoordelen hoe waarschijnlijk en ernstig de gevolgen van de onbeschikbaarheid van persoonsgegevens voor de rechten en vrijheden van natuurlijke personen zijn. Overeenkomstig artikel 33 moet de verwerkingsverantwoordelijke de inbreuk melden, tenzij het onwaarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van natuurlijke personen inhoudt. Uiteraard moet dit per geval worden beoordeeld.

Voorbeelden

In de context van een ziekenhuis kan de onbeschikbaarheid van cruciale medische gegevens over patiënten, zelfs tijdelijk, een risico voor de rechten en vrijheden van natuurlijke personen inhouden. Het kan bijvoorbeeld tot gevolg hebben dat operaties worden geannuleerd en dat levens in gevaar komen.

Indien daarentegen de systemen van een mediabedrijf een aantal uren niet beschikbaar zijn (bijvoorbeeld als gevolg van een stroomstoring), is het onwaarschijnlijk dat de onmogelijkheid van het bedrijf om zijn abonnees nieuwsbrieven te sturen een risico voor de rechten en vrijheden van natuurlijke personen inhoudt.

Er zij op gewezen dat ook indien de systemen van een verwerkingsverantwoordelijke slechts tijdelijk niet beschikbaar zijn en dit geen gevolgen heeft voor personen, het belangrijk is dat de verwerkingsverantwoordelijke alle mogelijke gevolgen van een inbreuk in overweging neemt, aangezien het nog steeds verplicht kan zijn de inbreuk om andere redenen te melden.

Voorbeeld:

[16] Zie artikel 33, lid 5.

Infectie door gijzelsoftware (kwaadaardige software die de gegevens van de verwerkingsverantwoordelijke versleutelt tot losgeld is betaald) kan leiden tot een tijdelijk verlies van beschikbaarheid indien de gegevens vanaf een back-up kunnen worden hersteld. Er is echter nog steeds sprake van netwerkinbraak en een melding kan verplicht zijn als het incident wordt gekwalificeerd als een inbreuk op de vertrouwelijkheid (d.w.z. als de aanvaller toegang heeft gekregen tot persoonsgegevens) en dit een risico voor de rechten en vrijheden van natuurlijke personen inhoudt.

3. De mogelijke gevolgen van een inbreuk in verband met persoonsgegevens

Een inbreuk kan diverse aanzienlijke negatieve gevolgen voor personen hebben, wat kan leiden tot lichamelijke, materiële of immateriële schade. In de AVG wordt uitgelegd dat dit onder meer het volgende kan inhouden: verlies van controle over hun persoonsgegevens, de beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaanmaking van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de personen in kwestie[17].

Dienovereenkomstig is in de AVG bepaald dat de verwerkingsverantwoordelijke verplicht is een inbreuk aan de bevoegde toezichthoudende autoriteit te melden, tenzij het onwaarschijnlijk is dat de inbreuk zal leiden tot het risico dat dergelijke nadelige effecten zich voordoen. Wanneer het risico dat deze nadelige gevolgen zich voordoen waarschijnlijk groot is, is de verwerkingsverantwoordelijke krachtens de AVG verplicht om de inbreuk zo snel als redelijkerwijs haalbaar is aan de getroffen personen mee te delen[18].

In overweging 87 van de AVG wordt benadrukt hoe belangrijk het is dat een inbreuk kan worden vastgesteld, dat het risico voor personen wordt beoordeeld en dat de inbreuk indien nodig wordt gemeld:

"Nagegaan moet worden of alle passende technische en organisatorische maatregelen zijn genomen om vast te stellen of een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, en om de toezichthoudende autoriteit en de betrokkene daarvan onverwijld in kennis te stellen. Het feit dat de kennisgeving is gedaan zonder onredelijke vertraging moet worden vastgesteld, met name rekening houdend met de aard en de ernst van de inbreuk in verband met persoonsgegevens en de gevolgen en negatieve effecten voor de betrokkene. Die kennisgeving kan ertoe leiden dat de toezichthoudende autoriteit optreedt overeenkomstig haar in deze verordening neergelegde taken en bevoegdheden."

Nadere richtsnoeren voor de beoordeling van het risico op nadelige gevolgen voor personen zijn opgenomen in deel IV.

Indien een verwerkingsverantwoordelijke nalaat een inbreuk in verband met persoonsgegevens ter kennis te brengen van ofwel de toezichthoudende autoriteit, ofwel de betrokkenen, ofwel beide, ondanks het feit dat aan de vereisten van artikel 33 en/of artikel 34 is voldaan, wordt de toezichthoudende autoriteit een keuze geboden waarin alle tot haar beschikking staande corrigerende maatregelen moeten worden overwogen, waaronder de oplegging van een passende administratieve

[17] Zie ook de overwegingen 85 en 75.

[18] Zie ook overweging 86.

geldboete[19], hetzij bovenop een corrigerende maatregel op grond van artikel 58, lid 2, hetzij op zichzelf. Indien voor een administratieve geldboete wordt gekozen, kan het bedrag ervan maximaal 10 000 000 EUR bedragen, of maximaal 2 % van de totale wereldwijde jaaromzet van een onderneming krachtens artikel 83, lid 4, onder a), van de AVG. Het is ook belangrijk om in gedachten te houden dat in sommige gevallen het niet melden van een inbreuk kan wijzen op het ontbreken van veiligheidsmaatregelen of op de ontoereikendheid van de bestaande veiligheidsmaatregelen. In de richtlijnen van de WP29 met betrekking tot administratieve geldboeten is het volgende bepaald: "Indien verscheidene inbreuken samen in een bepaald geval zijn gepleegd, kan de toezichthoudende autoriteit de administratieve geldboeten toepassen op een niveau dat doeltreffend, evenredig en afschrikkend is binnen de grenzen van de zwaarste inbreuk". In dat geval zal de toezichthoudende autoriteit ook de mogelijkheid hebben sancties op te leggen voor het niet melden of meedelen van de inbreuk (artikelen 33 en 34) enerzijds en voor het ontbreken van (adequate) veiligheidsmaatregelen (artikel 32) anderzijds, aangezien het twee afzonderlijke inbreuken betreft.

II. **Artikel 33 - Melding aan de toezichthoudende autoriteit**

A. Wanneer melden

1. Vereisten van artikel 33

In artikel 33, lid 1, is het volgende bepaald:

> "Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging."

Overweging 87 luidt als volgt[20]:

> "Nagegaan moet worden of alle passende technische en organisatorische maatregelen zijn genomen om vast te stellen of een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, en om de toezichthoudende autoriteit en de betrokkene daarvan onverwijld in kennis te stellen. Het feit dat de kennisgeving is gedaan zonder onredelijke vertraging moet worden vastgesteld, met name rekening houdend met de aard en de ernst van de inbreuk in verband met persoonsgegevens en de gevolgen en negatieve effecten voor de betrokkene. Die kennisgeving kan ertoe leiden dat de toezichthoudende autoriteit optreedt overeenkomstig haar in deze verordening neergelegde taken en bevoegdheden."

2. Wanneer heeft een verwerkingsverantwoordelijke er "kennis" van gekregen?

[19] Voor meer details wordt verwezen naar de WP29-richtsnoeren voor de toepassing en vaststelling van administratieve geldboeten, die hier beschikbaar zijn: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[20] Overweging 85 is in dit verband ook belangrijk.

Zoals hierboven is uiteengezet, is in de AVG bepaald dat de verwerkingsverantwoordelijke in geval van een inbreuk verplicht is de inbreuk zonder onredelijke vertraging te melden en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft gekregen. Dit kan de vraag doen rijzen wanneer een verwerkingsverantwoordelijke kan worden geacht "kennis" te hebben gekregen van een inbreuk. De WP29 is van mening dat een verwerkingsverantwoordelijke moet worden geacht "kennis" te hebben gekregen wanneer hij een redelijke mate van zekerheid heeft dat zich een veiligheidsincident heeft voorgedaan dat tot de compromittering van persoonsgegevens heeft geleid.

Zoals eerder aangegeven, is de verwerkingsverantwoordelijke op grond van de AVG echter verplicht alle passende technische en organisatorische maatregelen te nemen om onmiddellijk vast te stellen of een inbreuk heeft plaatsgevonden en om de toezichthoudende autoriteit en de betrokkenen daarvan onverwijld in kennis te stellen. In de AVG wordt ook gesteld dat het feit dat de kennisgeving is gedaan zonder onredelijke vertraging moet worden vastgesteld, met name rekening houdend met de aard en de ernst van de inbreuk en de gevolgen en negatieve effecten voor de betrokkene[21]. Hiermee wordt de verwerkingsverantwoordelijke de verplichting opgelegd om ervoor te zorgen dat hij tijdig "kennis" krijgt van inbreuken zodat hij de nodige maatregelen kan nemen.

Wanneer precies een verwerkingsverantwoordelijke kan worden geacht "kennis" te hebben gekregen van een bepaalde inbreuk, hangt af van de omstandigheden van de specifieke inbreuk. In sommige gevallen zal het van meet af aan vrij duidelijk zijn dat er sprake is van een inbreuk, terwijl het in andere gevallen enige tijd kan duren om vast te stellen of persoonsgegevens zijn gecompromitteerd. De nadruk moet echter liggen op onmiddellijke actie om een incident te onderzoeken teneinde vast te stellen of er inderdaad sprake is van een inbreuk op persoonsgegevens en, indien dat het geval is, corrigerende maatregelen te nemen en de inbreuk te melden indien nodig.

Voorbeelden

1. Bij verlies van een USB-stick met onversleutelde persoonsgegevens is het vaak niet mogelijk om na te gaan of onbevoegden toegang hebben gekregen tot die gegevens. Hoewel de verwerkingsverantwoordelijke misschien niet kan vaststellen of een inbreuk op de vertrouwelijkheid heeft plaatsgevonden, moet een dergelijk geval toch worden gemeld aangezien er een redelijke mate van zekerheid is dat een inbreuk op de beschikbaarheid heeft plaatsgevonden; de verwerkingsverantwoordelijke zou "kennis" hebben gekregen toen hij zich realiseerde dat de USB-stick verloren was geraakt.

2. Een derde stelt een verwerkingsverantwoordelijke ervan in kennis dat hij per ongeluk de persoonsgegevens van een van de klanten van de verwerkingsverantwoordelijke heeft ontvangen en levert het bewijs van de ongeoorloofde verstrekking. Aangezien de verwerkingsverantwoordelijke duidelijke bewijzen van een inbreuk op de vertrouwelijkheid heeft ontvangen, kan er geen twijfel over bestaan dat hij daarvan "kennis" heeft gekregen.

3. Een verwerkingsverantwoordelijke ontdekt dat er mogelijk in zijn netwerk is ingebroken. Hij controleert zijn systemen om na te gaan of in dat netwerk opgeslagen persoonsgegevens zijn gecompromitteerd en stelt vast dat dit het geval is. Ook hier kan er geen twijfel over bestaan dat de verwerkingsverantwoordelijke "kennis" heeft gekregen van die inbreuk aangezien hij er duidelijke bewijzen van heeft.

4. Een cybercrimineel hackt het systeem van een verwerkingsverantwoordelijke en neemt vervolgens contact met hem op om losgeld te vragen. In dat geval beschikt de verwerkingsverantwoordelijke, nadat hij zijn systeem heeft gecontroleerd om na te gaan of het is aangevallen, over duidelijk bewijs

[21] Zie overweging 87.

dat er een inbreuk heeft plaatsgevonden en bestaat er geen twijfel dat hij daarvan "kennis" heeft gekregen.

Nadat de verwerkingsverantwoordelijke voor het eerst door een persoon, een mediaorganisatie of een andere bron op de hoogte is gebracht van een mogelijke inbreuk, of wanneer hij zelf een veiligheidsincident heeft ontdekt, kan hij een kort onderzoek instellen om vast te stellen of er al dan niet daadwerkelijk een inbreuk heeft plaatsgevonden. Zolang dit onderzoek loopt, kan de verwerkingsverantwoordelijke niet worden geacht "kennis" te hebben gekregen. Er wordt echter verwacht dat het eerste onderzoek zo spoedig mogelijk begint en dat op basis daarvan met een redelijke mate van zekerheid wordt vastgesteld of een inbreuk heeft plaatsgevonden; daarna kan een gedetailleerder onderzoek volgen.

Zodra de verwerkingsverantwoordelijke "kennis" heeft gekregen, moet een te melden inbreuk zonder onredelijke vertraging en, indien mogelijk, binnen 72 uur worden gemeld. Gedurende deze periode dient de verwerkingsverantwoordelijke het waarschijnlijke risico voor personen te beoordelen om na te gaan of de meldingsplicht geldt en welke actie(s) nodig is (zijn) om de inbreuk aan te pakken. Een verwerkingsverantwoordelijke kan echter al een eerste beoordeling hebben van het potentiële risico dat uit een inbreuk zou kunnen voortvloeien op basis van een gegevensbeschermingseffectbeoordeling[22] die vóór de uitvoering van de verwerking in kwestie is uitgevoerd. De gegevensbeschermingseffectbeoordeling kan echter algemener zijn dan de specifieke omstandigheden van een daadwerkelijke inbreuk, zodat in elk geval een aanvullende beoordeling moet worden uitgevoerd waarin met die omstandigheden rekening wordt gehouden. Voor nadere bijzonderheden over de beoordeling van risico's wordt verwezen naar deel IV.

In de meeste gevallen moeten deze voorbereidende acties kort na de eerste waarschuwing worden uitgevoerd (d.w.z. wanneer de verwerkingsverantwoordelijke of de verwerker vermoedt dat zich een veiligheidsincident heeft voorgedaan waarbij persoonsgegevens betrokken kunnen zijn). – het zou slechts in uitzonderlijke gevallen meer tijd moeten vergen.

Voorbeeld:

Een natuurlijke persoon stelt de verwerkingsverantwoordelijke ervan in kennis dat hij een e-mail heeft ontvangen van iemand die zich uitgeeft voor de verwerkingsverantwoordelijke. Deze e-mail bevat persoonsgegevens die betrekking hebben op het (werkelijke) gebruik van de dienst van de verwerkingsverantwoordelijke door de natuurlijke persoon, waaruit blijkt dat de veiligheid van de verwerkingsverantwoordelijke is gecompromitteerd. De verwerkingsverantwoordelijke stelt een kort onderzoek in, constateert dat er in zijn netwerk is ingebroken en vindt bewijs dat iemand op ongeoorloofde wijze toegang tot persoonsgegevens heeft verkregen. De verwerkingsverantwoordelijke wordt nu geacht "kennis" te hebben gekregen en is verplicht de inbreuk aan de toezichthoudende autoriteit te melden, tenzij het onwaarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van personen inhoudt. De verwerkingsverantwoordelijke zal passende corrigerende maatregelen moeten nemen om de inbreuk aan te pakken.

De verwerkingsverantwoordelijke dient derhalve over interne processen te beschikken om een inbreuk te kunnen opsporen en aanpakken. Zo kan de verwerkingsverantwoordelijke of de verwerker voor de vaststelling van bepaalde onregelmatigheden in de gegevensverwerking gebruikmaken van bepaalde technische maatregelen zoals tools voor het analyseren van gegevensstromen en logboeken, waarmee

[22] Zie de richtsnoeren van de WP29 met betrekking tot gegevensbeschermingseffectbeoordelingen: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

gebeurtenissen en waarschuwingen kunnen worden geïdentificeerd door loggegevens te correleren[23]. Het is van belang dat wanneer een inbreuk wordt vastgesteld deze aan het juiste managementniveau wordt gerapporteerd, zodat de inbreuk kan worden aangepakt en, indien nodig, gemeld in overeenstemming met artikel 33 en, indien nodig, artikel 34. Dergelijke maatregelen en rapportagemechanismen zouden nader kunnen worden uitgewerkt in de reactieplannen voor inbreuken en/of governanceregelingen van de verwerkingsverantwoordelijke. Deze helpen de verwerkingsverantwoordelijke om effectief te plannen en vast te stellen wie binnen de organisatie de operationele verantwoordelijkheid heeft voor het beheer van een inbreuk en of en hoe een incident indien nodig dient te worden geëscaleerd (d.w.z. aan een hoger niveau gerapporteerd en overgedragen).

De verwerkingsverantwoordelijke dient ook regelingen te treffen met verwerkers die hij inschakelt, die zelf verplicht zijn de verwerkingsverantwoordelijke in kennis te stellen van een inbreuk (zie hieronder).

Hoewel het de verantwoordelijkheid van de verwerkingsverantwoordelijken en verwerkers is om passende maatregelen te nemen teneinde in staat te zijn een inbreuk te voorkomen, erop te reageren en aan te pakken, zijn er in alle gevallen een aantal praktische stappen die moeten worden genomen.

- Informatie over alle veiligheidsgerelateerde gebeurtenissen moet terechtkomen bij een of meer verantwoordelijke personen die tot taak hebben incidenten aan te pakken, het bestaan van een inbreuk vast te stellen en de risico's te beoordelen.
- Vervolgens moet het risico voor personen als gevolg van een inbreuk worden beoordeeld (waarschijnlijkheid dat er geen risico, wel een risico of een hoog risico is) en moeten de relevante geledingen van de organisatie op de hoogte worden gebracht.
- De inbreuk moet worden gemeld aan de toezichthoudende autoriteit en moet eventueel worden meegedeeld de getroffen personen, indien nodig.
- Tegelijkertijd dient de verwerkingsverantwoordelijke op te treden om de inbreuk in te perken en te herstellen.
- De inbreuk moet worden gedocumenteerd naarmate ze zich ontwikkelt.

Het dient dan ook duidelijk te zijn dat de verwerkingsverantwoordelijke verplicht is op te treden naar aanleiding van een eerste waarschuwing en vast te stellen of er al dan niet een inbreuk heeft plaatsgevonden. Deze korte periode biedt de verwerkingsverantwoordelijke de gelegenheid een onderzoek in te stellen en bewijsmateriaal en andere relevante gegevens te verzamelen. Zodra de verwerkingsverantwoordelijke echter met een redelijke mate van zekerheid heeft vastgesteld dat een inbreuk heeft plaatsgevonden, moet hij, indien aan de voorwaarden van artikel 33, lid 1, is voldaan, de toezichthoudende autoriteit zonder onredelijke vertraging en, indien mogelijk, binnen 72 uur daarvan in kennis stellen[24]. Indien een verwerkingsverantwoordelijke niet tijdig handelt en het duidelijk wordt dat een inbreuk heeft plaatsgevonden, kan dit worden beschouwd als een verzuim om een inbreuk te melden overeenkomstig artikel 33.

Uit artikel 32 blijkt duidelijk dat de verwerkingsverantwoordelijke en verwerker over passende technische en organisatorische maatregelen dienen te beschikken om een passend niveau van beveiliging van persoonsgegevens te waarborgen: het vermogen om een inbreuk tijdig op te sporen,

[23] Opgemerkt zij dat loggegevens die het makkelijker maken om bijvoorbeeld de opslag, wijziging of wissing van gegevens te controleren mogelijk ook kwalificeren als persoonsgegevens van de persoon die het initiatief tot de betrokken verwerking heeft genomen.

[24] Zie Verordening (EEG, Euratom) nr. 1182/71 houdende vaststelling van de regels die van toepassing zijn op termijnen, data en aanvangs- en vervaltijden, beschikbaar op: http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:31971R1182&from=EN

aan te pakken en te melden moet worden beschouwd als een essentieel onderdeel van deze maatregelen.

3. Gezamenlijke verwerkingsverantwoordelijken

Artikel 26 heeft betrekking op gezamenlijke verwerkingsverantwoordelijken. In dat artikel is bepaald dat gezamenlijke verwerkingsverantwoordelijken hun respectieve verantwoordelijkheden voor de naleving van de AVG moeten bepalen[25]. Dit houdt onder meer in dat wordt vastgesteld welke partij verantwoordelijk is voor de nakoming van de verplichtingen uit hoofde van de artikelen 33 en 34. De WP29 beveelt aan dat de contractuele regelingen tussen gezamenlijke verwerkingsverantwoordelijken bepalingen bevatten waarin is vastgelegd welke verwerkingsverantwoordelijke de leiding neemt of verantwoordelijk is voor de nakoming van de in de AVG opgenomen verplichtingen om inbreuken te melden.

4. Verplichtingen van de verwerker

De verwerkingsverantwoordelijke blijft algemeen verantwoordelijk voor de bescherming van persoonsgegevens, maar de verwerker heeft een belangrijke rol te vervullen om de verwerkingsverantwoordelijke in staat te stellen zijn verplichtingen na te komen; dit geldt ook voor de melding van inbreuken. In artikel 28, lid 3, is bepaald dat de verwerking door een verwerker moet worden geregeld in een overeenkomst of andere rechtshandeling. In artikel 28, lid 3, onder f), is bepaald dat in de overeenkomst of andere rechtshandeling moet worden vastgelegd dat de verwerker "rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36".

In artikel 33, lid 2, wordt verduidelijkt dat indien een door een verwerkingsverantwoordelijke ingeschakelde verwerker kennis krijgt van een inbreuk op de persoonsgegevens die hij namens de verwerkingsverantwoordelijke verwerkt, de verwerker de verwerkingsverantwoordelijke daarvan "zonder onredelijke vertraging" in kennis moet stellen. Er zij op gewezen dat de verwerker niet eerst de waarschijnlijkheid van risico's die voortvloeien uit een inbreuk hoeft te beoordelen voordat hij de verwerkingsverantwoordelijke in kennis stelt; het is de verwerkingsverantwoordelijke die deze inschatting moet maken zodra hij "kennis" heeft gekregen van de inbreuk. De verwerker hoeft alleen maar vast te stellen of er een inbreuk heeft plaatsgevonden, waarna hij de verwerkingsverantwoordelijke hiervan in kennis dient te stellen. De verwerkingsverantwoordelijke gebruikt de verwerker om zijn doelen te bereiken; derhalve dient de verwerkingsverantwoordelijke in beginsel te worden geacht "kennis" te hebben gekregen zodra de verwerker hem van de inbreuk in kennis heeft gesteld. Doordat de verwerker verplicht is zijn verwerkingsverantwoordelijke in kennis te stellen, kan de verwerkingsverantwoordelijke de inbreuk aanpakken en bepalen of hij al dan niet verplicht is de toezichthoudende autoriteit overeenkomstig artikel 33, lid 1, en de getroffen personen overeenkomstig artikel 34, lid 1, in kennis te stellen. De verwerkingsverantwoordelijke kan ook een onderzoek naar de inbreuk instellen, aangezien de verwerker mogelijk niet in staat is alle relevante feiten met betrekking tot de zaak te kennen, en bijvoorbeeld niet weet of de verwerkingsverantwoordelijke nog steeds beschikt over een kopie of back-up van persoonsgegevens die door de verwerker zijn vernietigd of verloren. Dit kan van invloed zijn op de vraag of de verwerkingsverantwoordelijke de inbreuk moet melden.

In de AVG wordt geen specifieke termijn vermeld waarbinnen de verwerker de verwerkingsverantwoordelijke moet waarschuwen, behalve dat hij dit "zonder onredelijke vertraging" moet doen. Daarom beveelt de WP29 aan dat de verwerker de verwerkingsverantwoordelijke onverwijld in kennis stelt, waarbij nadere informatie over de inbreuk in stappen wordt verstrekt

[25] Zie ook overweging 79.

naarmate meer details beschikbaar komen. Dit is van belang om de verwerkingsverantwoordelijke te helpen zijn verplichting om de inbreuk binnen 72 uur aan de toezichthoudende autoriteit te melden na te komen.

Zoals hierboven is uiteengezet, dient in het contract tussen de verwerkingsverantwoordelijke en de verwerker te worden gespecificeerd hoe aan de in artikel 33, lid 2, gestelde eisen, naast andere bepalingen in de AVG, moet worden voldaan. Dit kan onder meer inhouden dat de verwerker de verwerkingsverantwoordelijke in een vroeg stadium in kennis moet stellen, wat op zijn beurt de verplichting van de verwerkingsverantwoordelijke om de inbreuk binnen 72 uur aan de toezichthoudende autoriteit te melden, ondersteunt.

Indien de verwerker diensten levert aan meerdere verwerkingsverantwoordelijken die alle te maken hebben met hetzelfde incident, moet de verwerker aan elke verwerkingsverantwoordelijke bijzonderheden over het incident melden.

Een verwerker zou een inbreuk namens de verwerkingsverantwoordelijke kunnen melden indien de verwerkingsverantwoordelijke de verwerker de juiste machtiging heeft verleend en dit deel uitmaakt van de contractuele regelingen tussen de verwerkingsverantwoordelijke en de verwerker. Een dergelijke melding moet worden gedaan in overeenstemming met de artikelen 33 en 34. Het is echter belangrijk op te merken dat de verwerkingsverantwoordelijke wettelijk verantwoordelijk blijft voor de melding van een inbreuk.

B. Verstrekking van informatie aan de toezichthoudende autoriteit

1. Te verstrekken informatie

Wanneer een verwerkingsverantwoordelijke een inbreuk aan de toezichthoudende autoriteit meldt, is in artikel 33, lid 3, bepaald dat in de melding ten minste het volgende moet worden omschreven of meegedeeld:

> "a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
>
> b) de naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
>
> c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
>
> d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

In de AVG worden geen categorieën van betrokkenen of persoonsgegevensregisters gedefinieerd. De WP29 stelt echter categorieën van betrokkenen voor om te verwijzen naar de verschillende soorten personen van wie de persoonsgegevens het voorwerp van een inbreuk zijn: afhankelijk van de gebruikte omschrijvingen kan dit onder meer kinderen en andere kwetsbare groepen, mensen met een handicap, werknemers of klanten omvatten. Evenzo kunnen categorieën van persoonsgegevensregisters betrekking hebben op de verschillende soorten registers die de verwerkingsverantwoordelijke kan verwerken, zoals gegevens die verband houden met gezondheid, onderwijs en sociale zorg, financiële gegevens, bankrekeningnummers, paspoortnummers enz.

In overweging 85 wordt duidelijk gemaakt dat een van de doelstellingen van de melding erin bestaat de schade voor personen te beperken. Indien de soorten betrokkenen of de soorten persoonsgegevens wijzen op een risico van bijzondere schade als gevolg van een inbreuk (bijvoorbeeld

identiteitsdiefstal, fraude, financieel verlies, bedreiging van het beroepsgeheim), is het bijgevolg belangrijk dat deze categorieën in de melding worden vermeld. Op die manier is dit gekoppeld aan de vereiste om de waarschijnlijke gevolgen van de inbreuk te beschrijven.

Indien geen precieze informatie beschikbaar is (bijv. het exacte aantal betrokkenen), mag dit geen belemmering vormen voor de tijdige melding van inbreuken. In de AVG wordt toegestaan dat het aantal betrokken personen en het aantal persoonsgegevensregisters bij benadering worden vermeld. De nadruk moet worden gelegd op het aanpakken van de negatieve effecten van de inbreuk in plaats van op het verstrekken van precieze cijfers. Wanneer dus duidelijk is geworden dat er sprake is van een inbreuk maar de omvang daarvan nog niet bekend is, is een melding in stappen (zie hieronder) een veilige manier om aan de meldingsplicht te voldoen.

In artikel 33, lid 3, is bepaald dat de verwerkingsverantwoordelijke in een melding "ten minste" deze informatie moet verstrekken, wat betekent dat een verwerkingsverantwoordelijke indien nodig kan besluiten nadere bijzonderheden te verstrekken. Voor verschillende soorten inbreuken (vertrouwelijkheid, integriteit of beschikbaarheid) kan het nodig zijn nadere informatie te verstrekken om de omstandigheden van elk geval volledig uit te leggen.

Voorbeeld:

In het kader van zijn melding aan de toezichthoudende autoriteit kan een verwerkingsverantwoordelijke het nuttig vinden zijn verwerker te noemen indien deze aan de basis van de inbreuk ligt, met name als dit heeft geleid tot een incident dat gevolgen heeft voor de persoonsgegevensregisters van vele andere verwerkingsverantwoordelijken die met dezelfde verwerker werken.

In elk geval kan de toezichthoudende autoriteit in het kader van haar onderzoek van een inbreuk meer details opvragen.

2. Melding in stappen

Afhankelijk van de aard van de inbreuk kan nader onderzoek door de verwerkingsverantwoordelijke nodig zijn om alle relevante feiten met betrekking tot het incident vast te stellen. In artikel 33, lid 4, is het volgende bepaald:

"Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt."

Dit betekent dat in de AVG wordt erkend dat verwerkingsverantwoordelijken niet altijd over alle noodzakelijke informatie met betrekking tot een inbreuk beschikken binnen 72 uur nadat zij daarvan kennis hebben gekregen, aangezien de volledige details van het incident tijdens deze eerste periode niet altijd beschikbaar zijn. Om die reden wordt in de AVG een melding in stappen toegestaan. Een melding in stappen komt vaker voor bij complexere inbreuken, zoals sommige soorten cyberincidenten waarbij bijvoorbeeld een diepgaand forensisch onderzoek nodig kan zijn om de aard van de inbreuk en de mate waarin persoonsgegevens zijn gecompromitteerd volledig vast te stellen. Bijgevolg zal de verwerkingsverantwoordelijke in veel gevallen op een later tijdstip meer onderzoek moeten verrichten en aanvullende informatie moeten verstrekken. Dit is toegestaan, mits de verwerkingsverantwoordelijke de redenen voor de vertraging opgeeft, overeenkomstig artikel 33, lid 1. De WP29 beveelt aan dat wanneer de verwerkingsverantwoordelijke de toezichthoudende autoriteit voor het eerst in kennis stelt, hij de toezichthoudende autoriteit ook dient te informeren als hij nog niet over alle vereiste informatie beschikt en later meer details zal verstrekken. De toezichthoudende autoriteit dient akkoord te gaan met de wijze en het tijdstip waarop aanvullende informatie dient te worden verstrekt. Dit belet de verwerkingsverantwoordelijke niet om op enig ander moment nadere

informatie te verstrekken indien hij kennis krijgt van aanvullende relevante details over de inbreuk die aan de toezichthoudende autoriteit moeten worden verstrekt.

De meldingsplicht is er vooral op gericht verwerkingsverantwoordelijken aan te moedigen om bij een inbreuk onmiddellijk op te treden, de inbreuk in te perken, de gecompromitteerde persoonsgegevens indien mogelijk te herstellen en de toezichthoudende autoriteit om advies te vragen. Door de inbreuk binnen de eerste 72 uur aan de toezichthoudende autoriteit te melden, kan de verwerkingsverantwoordelijke zich ervan vergewissen dat besluiten over het al dan niet in kennis stellen van personen correct zijn.

De melding aan de toezichthoudende autoriteit is echter niet uitsluitend bedoeld om advies te verkrijgen over het al dan niet in kennis stellen van de getroffen personen. In sommige gevallen zal het duidelijk zijn dat de verwerkingsverantwoordelijke, gezien de aard van de inbreuk en de ernst van het risico, de getroffen personen onverwijld in kennis moet stellen. Als er bijvoorbeeld een onmiddellijke dreiging van identiteitsdiefstal bestaat of als speciale categorieën persoonsgegevens[26] online worden verstrekt, dient de verwerkingsverantwoordelijke zonder onredelijke vertraging op te treden om de inbreuk in te perken en aan de betrokkenen mee te delen (zie deel III). In uitzonderlijke omstandigheden kan dit zelfs gebeuren voordat de inbreuk aan de toezichthoudende autoriteit wordt gemeld. Meer in het algemeen mag de melding aan de toezichthoudende autoriteit niet dienen als rechtvaardiging voor het niet meedelen van de inbreuk aan de betrokkenen indien zulks vereist is.

Het moet ook duidelijk zijn dat een verwerkingsverantwoordelijke na een eerste melding de toezichthoudende autoriteit op de hoogte kan brengen indien uit een vervolgonderzoek blijkt dat het veiligheidsincident onder controle is en er geen inbreuk heeft plaatsgevonden. Deze informatie kan dan worden toegevoegd aan de informatie die reeds aan de toezichthoudende autoriteit is verstrekt en het incident kan bijgevolg worden geregistreerd als zijnde geen inbreuk. Er is geen sanctie voor het melden van een incident dat uiteindelijk geen inbreuk blijkt te zijn.

Voorbeeld:

Een verwerkingsverantwoordelijke stelt de toezichthoudende autoriteit binnen 72 uur na de ontdekking van een inbreuk ervan in kennis dat hij een USB-stick met daarop een kopie van de persoonsgegevens van sommige van zijn klanten is verloren. De USB-stick wordt later teruggevonden bij de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke brengt de toezichthoudende autoriteit hiervan op de hoogte en vraagt om de melding te wijzigen.

Opgemerkt dient te worden dat een melding in stappen reeds bestaat in het kader van de bestaande verplichtingen van Richtlijn 2002/58/EG, Verordening (EU) nr. 611/2013 en andere zelf gemelde incidenten.

3. Melding met vertraging

In artikel 33, lid 1, wordt duidelijk gemaakt dat indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, zij vergezeld dient te gaan van een motivering voor de vertraging. Samen met het begrip "melding in stappen" wordt hiermee erkend dat een verwerkingsverantwoordelijke niet altijd in staat is een inbreuk binnen die termijn te melden en dat een melding met vertraging toegestaan kan zijn.

Een dergelijk scenario kan zich bijvoorbeeld voordoen wanneer een verwerkingsverantwoordelijke in korte tijd wordt geconfronteerd met meerdere, vergelijkbare inbreuken op de vertrouwelijkheid die grote aantallen betrokkenen op dezelfde wijze treffen. Een verwerkingsverantwoordelijke zou kennis

[26] Zie artikel 9.

kunnen krijgen van een inbreuk en zou, terwijl hij met zijn onderzoek begint en vóór de melding van de inbreuk, nog meer soortgelijke inbreuken kunnen ontdekken die verschillende oorzaken hebben. Afhankelijk van de omstandigheden kan het enige tijd duren voordat de verwerkingsverantwoordelijke de omvang van de inbreuken heeft vastgesteld. In plaats van elke inbreuk afzonderlijk te melden, stelt de verwerkingsverantwoordelijke een zinvolle melding op die verscheidene zeer vergelijkbare inbreuken met mogelijke verschillende oorzaken vertegenwoordigt. Dit zou ertoe kunnen leiden dat de melding aan de toezichthoudende autoriteit wordt uitgevoerd meer dan 72 uur nadat de verwerkingsverantwoordelijke voor het eerst kennis heeft gekregen van deze inbreuken.

Strikt genomen is elke individuele inbreuk een te melden incident. Om een te omslachtige procedure te vermijden, mag de verwerkingsverantwoordelijke echter een "gebundelde" melding indienen die al deze inbreuken vertegenwoordigt, mits deze betrekking hebben op hetzelfde type persoonsgegevens waarop op dezelfde wijze en binnen relatief korte tijd inbreuk is gemaakt. Indien een reeks inbreuken plaatsvindt die betrekking hebben op verschillende soorten persoonsgegevens waarop op verschillende manieren inbreuk is gemaakt, dient de melding op de normale wijze te gebeuren, waarbij elke inbreuk overeenkomstig artikel 33 wordt gemeld.

Hoewel in de AVG een zekere mate van vertraging bij de melding wordt toegestaan, mag dit niet worden gezien als iets dat regelmatig voorkomt. Er moet op worden gewezen dat gebundelde meldingen ook kunnen worden gedaan voor meerdere soortgelijke inbreuken die binnen 72 uur worden gemeld.

C. Grensoverschrijdende inbreuken en inbreuken bij vestigingen buiten de EU

1. Grensoverschrijdende inbreuken

Bij een grensoverschrijdende verwerking[27] van persoonsgegevens kan een inbreuk gevolgen hebben voor betrokkenen in meer dan één lidstaat. In artikel 33, lid 1, wordt duidelijk gemaakt dat wanneer een inbreuk heeft plaatsgevonden, de verwerkingsverantwoordelijke de overeenkomstig artikel 55 van de AVG competente toezichthoudende autoriteit daarvan in kennis moet stellen[28]. Artikel 55, lid 1, luidt als volgt:

> "Elke toezichthoudende autoriteit heeft de competentie op het grondgebied van haar lidstaat de taken uit te voeren die haar overeenkomstig deze verordening zijn opgedragen en de bevoegdheden uit te oefenen die haar overeenkomstig deze verordening zijn toegekend."

In artikel 56, lid 1, is echter het volgende bepaald:

> "Onverminderd artikel 55 is de toezichthoudende autoriteit van de hoofdvestiging of de enige vestiging van de verwerkingsverantwoordelijke of verwerker competent op te treden als leidende toezichthoudende autoriteit voor de grensoverschrijdende verwerking door die verwerkingsverantwoordelijke of verwerker overeenkomstig de procedure van artikel 60."

Voorts is in artikel 56, lid 6, het volgende bepaald:

[27] Zie artikel 4, lid 23.

[28] Zie ook overweging 122.

"De leidende toezichthoudende autoriteit is voor de verwerkingsverantwoordelijke of de verwerker de enige gesprekspartner bij grensoverschrijdende verwerking door die verwerkingsverantwoordelijke of verwerker."

Dit betekent dat telkens wanneer een inbreuk plaatsvindt in het kader van grensoverschrijdende verwerking en een melding vereist is, de verwerkingsverantwoordelijke de leidende toezichthoudende autoriteit daarvan in kennis moet stellen[29]. Daarom moet een verwerkingsverantwoordelijke bij het opstellen van zijn reactieplan voor inbreuken beoordelen welke toezichthoudende autoriteit de leidende toezichthoudende autoriteit is waaraan hij zijn melding moet richten[30]. Dit zal de verwerkingsverantwoordelijke in staat stellen snel op een inbreuk te reageren en zijn verplichtingen uit hoofde van artikel 33 na te komen. Het moet duidelijk zijn dat in het geval van een inbreuk waarbij sprake is van grensoverschrijdende verwerking, de melding moet worden gedaan aan de leidende toezichthoudende autoriteit, die zich niet noodzakelijk bevindt op de plaats waar de getroffen betrokkenen zich bevinden, of zelfs waar de inbreuk heeft plaatsgevonden. Bij melding aan de leidende toezichthoudende autoriteit dient de verwerkingsverantwoordelijke indien nodig aan te geven of de inbreuk betrekking heeft op vestigingen in andere lidstaten en in welke lidstaten betrokkenen waarschijnlijk door de inbreuk zijn getroffen. Indien de verwerkingsverantwoordelijke twijfels heeft over de identiteit van de leidende toezichthoudende autoriteit, dient hij de inbreuk ten minste te melden aan de toezichthoudende autoriteit van de plaats waar de inbreuk heeft plaatsgevonden.

2. Inbreuken bij vestigingen buiten de EU

Artikel 3 heeft betrekking op het territoriale toepassingsgebied van de AVG, met inbegrip van wanneer de AVG van toepassing is op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke of verwerker die niet in de EU is gevestigd. In artikel 3, lid 2, is met name het volgende bepaald[31]:

"Deze verordening is van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met:

a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of

b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt."

Artikel 3, lid 3, is ook relevant en luidt als volgt[32]:

"Deze verordening is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet in de Unie is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht het lidstatelijke recht van toepassing is."

---

[29] Zie de WP29-richtlijnen voor het bepalen van de leidende toezichthoudende autoriteit van de verwerkingsverantwoordelijke of de verwerker, die beschikbaar zijn op http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] Een lijst met contactgegevens van alle Europese nationale gegevensbeschermingsautoriteiten is te vinden op: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] Zie ook de overwegingen 23 en 24.

[32] Zie ook overweging 25.

Indien een niet in de EU gevestigde verwerkingsverantwoordelijke onder artikel 3, lid 2, of artikel 3, lid 3, valt en met een inbreuk wordt geconfronteerd, blijft hij derhalve gebonden aan de kennisgevingsverplichtingen op grond van de artikelen 33 en 34. Krachtens artikel 27 is een verwerkingsverantwoordelijke (en verwerker) verplicht een vertegenwoordiger in de EU aan te wijzen indien artikel 3, lid 2, van toepassing is. In dergelijke gevallen beveelt de WP29 aan dat de melding wordt gedaan aan de toezichthoudende autoriteit van de lidstaat waar de vertegenwoordiger van de verwerkingsverantwoordelijke in de EU is gevestigd[33]. Zo ook is een verwerker die onder artikel 3, lid 2, valt gebonden aan de verplichtingen die gelden voor verwerkers, met name de verplichting om de verwerkingsverantwoordelijke overeenkomstig artikel 33, lid 2, van een inbreuk in kennis te stellen.

D. Voorwaarden waaronder geen melding vereist is

In artikel 33, lid 1, wordt duidelijk gemaakt dat indien "het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen", het niet verplicht is de inbreuk aan de toezichthoudende autoriteit te melden. Een voorbeeld is wanneer persoonsgegevens reeds publiekelijk beschikbaar zijn en de verstrekking ervan geen waarschijnlijk risico voor de betrokkene vormt. Dit staat in contrast met bestaande verplichtingen inzake de melding van inbreuken voor aanbieders van openbare elektronische-communicatiediensten in Richtlijn 2009/136/EG, waarin wordt gesteld dat alle relevante inbreuken aan de bevoegde autoriteit moeten worden gemeld.

In zijn advies 03/2014 over de melding van inbreuken[34] heeft de WP29 uitgelegd dat een inbreuk op de vertrouwelijkheid van persoonsgegevens die met een geavanceerd algoritme zijn versleuteld nog steeds een inbreuk in verband met persoonsgegevens is en moet worden gemeld. Is de sleutel echter nog steeds vertrouwelijk – d.w.z. de sleutel is bij geen enkele inbreuk gecompromitteerd en is zodanig gegenereerd dat hij niet met beschikbare technische middelen kan worden achterhaald door iemand die niet bevoegd is om er toegang toe te hebben – dan zijn de gegevens in principe onbegrijpelijk. Het is in dat geval onwaarschijnlijk dat de inbreuk nadelige gevolgen heeft voor personen en daarom zou geen mededeling aan die personen vereist zijn[35]. Zelfs indien de gegevens zijn versleuteld, kan een verlies of wijziging echter negatieve gevolgen hebben voor de betrokkenen indien de verwerkingsverantwoordelijke geen adequate back-ups heeft. In dat geval zou de inbreuk aan de betrokkenen moeten worden meegedeeld, zelfs indien de gegevens zelf aan passende versleutelingsmaatregelen waren onderworpen.

De WP29 heeft ook uitgelegd dat dit op vergelijkbare wijze het geval zou zijn indien persoonsgegevens, zoals wachtwoorden, veilig zijn "gehasht" en "gesalt", de gehashte waarde is berekend met een geavanceerde hashfunctie met cryptografische sleutel, en de voor het hashen van de gegevens gebruikte sleutel bij geen enkele inbreuk is gecompromitteerd en zodanig is gegenereerd dat hij niet met beschikbare technologische middelen kan worden achterhaald door iemand die niet bevoegd is om er toegang toe te hebben.

Indien persoonsgegevens in wezen onbegrijpelijk zijn gemaakt voor onbevoegde partijen en indien de gegevens een kopie zijn of er een back-up van bestaat, is het bijgevolg mogelijk dat een inbreuk op de vertrouwelijkheid waarbij naar behoren versleutelde persoonsgegevens zijn betrokken niet aan de toezichthoudende autoriteit hoeft te worden gemeld. Het is namelijk onwaarschijnlijk dat een dergelijke inbreuk een risico voor de rechten en vrijheden van natuurlijke personen vormt. Dit

[33] Zie overweging 80 en artikel 27.

[34] WP29, Advies 03/2014 over de melding van inbreuken, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[35] Zie ook artikel 4, art.5.1-1 en 2, van Verordening (EU) nr. 611/2013.

betekent uiteraard dat de natuurlijke persoon evenmin hoeft te worden geïnformeerd, aangezien er waarschijnlijk geen hoog risico is. Er zij echter op gewezen dat hoewel het in eerste instantie mogelijk niet verplicht is een inbreuk te melden indien er waarschijnlijk geen risico voor de rechten en vrijheden van natuurlijke personen is, dit in de loop van de tijd kan veranderen en het risico opnieuw moet worden geëvalueerd. Als bijvoorbeeld achteraf blijkt dat de sleutel gecompromitteerd is of als een kwetsbaarheid in de versleutelingssoftware aan het licht komt, is het mogelijk dat de inbreuk toch nog moet worden gemeld.

Bovendien moet worden opgemerkt dat in geval van een inbreuk waarbij er geen back-ups van de versleutelde persoonsgegevens zijn, er sprake is van een inbreuk op de beschikbaarheid die risico's voor personen zou kunnen inhouden en bijgevolg eventueel moet worden gemeld. Evenzo kan een inbreuk die het verlies van versleutelde gegevens met zich meebrengt, zelfs als er een back-up van de persoonsgegevens bestaat, toch nog een te melden inbreuk zijn, afhankelijk van de tijd die nodig is om de gegevens uit die back-up te herstellen en afhankelijk van de gevolgen van dat gebrek aan beschikbaarheid voor personen. Zoals gesteld in artikel 32, lid 1, onder c), is een belangrijke veiligheidsfactor "het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen".

Voorbeeld:

Een inbreuk die niet aan de toezichthoudende autoriteit zou moeten worden gemeld, is het verlies van een veilig versleuteld mobiel apparaat dat door de verwerkingsverantwoordelijke en zijn personeel wordt gebruikt. Mits de encryptiesleutel in het veilige bezit van de verwerkingsverantwoordelijke blijft en dit niet de enige kopie van de persoonsgegevens is, zouden de persoonsgegevens ontoegankelijk zijn voor een aanvaller. Dit betekent dat het onwaarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van de betrokkenen inhoudt. Indien later blijkt dat de encryptiesleutel is gecompromitteerd of dat de versleutelingssoftware of het versleutelingsalgoritme kwetsbaar is, dan zal het risico voor de rechten en vrijheden van natuurlijke personen veranderen en kan het dus wel verplicht zijn de inbreuk te melden.

Er is echter sprake van niet-naleving van artikel 33 indien een verwerkingsverantwoordelijke de toezichthoudende autoriteit niet in kennis stelt van een situatie waarin de gegevens niet veilig zijn versleuteld. Daarom moeten verwerkingsverantwoordelijken bij het selecteren van versleutelingssoftware zorgvuldig de kwaliteit en de juiste implementatie van de aangeboden versleuteling afwegen en moeten ze begrijpen welk beschermingsniveau deze feitelijk biedt en of dat niveau passend is voor de betrokken risico's. Verwerkingsverantwoordelijken moeten ook goed vertrouwd zijn met de werking van hun versleutelingsproduct. Een apparaat kan bijvoorbeeld versleuteld zijn als het is uitgeschakeld, maar niet als het in de stand-bymodus staat. Sommige producten die met versleuteling werken, hebben "standaardsleutels" die door elke klant moeten worden gewijzigd opdat ze doeltreffend zouden zijn. Ook kan de versleuteling op een gegeven moment als adequaat worden beschouwd door veiligheidsdeskundigen, maar kan ze een paar jaar later achterhaald zijn, waardoor het niet langer zeker is dat het versleutelingsproduct de gegevens voldoende versleutelt en een passend beschermingsniveau biedt.

III. **Artikel 34 – Mededeling aan de betrokkene**

A. Personen in kennis stellen

In bepaalde gevallen moet de verwerkingsverantwoordelijke een inbreuk niet alleen melden aan de toezichthoudende autoriteit, maar moet hij ze ook meedelen aan de getroffen personen.

Artikel 34, lid 1, luidt als volgt:

"Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee".

Verwerkingsverantwoordelijken moeten onthouden dat de melding van een inbreuk aan de toezichthoudende autoriteit verplicht is, tenzij het onwaarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van natuurlijke personen inhoudt. Als het waarschijnlijk is dat een inbreuk resulteert in een hoog risico voor de rechten en vrijheden van natuurlijke personen, moeten natuurlijke personen ook worden geïnformeerd. De drempel voor het meedelen van een inbreuk aan personen ligt dus hoger dan die voor het melden van een inbreuk aan de toezichthoudende autoriteiten, en dus hoeven niet alle inbreuken aan personen te worden gemeld, waardoor ze worden beschermd tegen onnodige kennisgevingsmoeheid.

In de AVG wordt gesteld dat een inbreuk "onverwijld", d.w.z. zo snel mogelijk, aan personen moet worden meegedeeld. Het belangrijkste doel van de mededeling aan personen is specifieke informatie te verstrekken over de stappen die zij moeten ondernemen om zichzelf te beschermen[36]. Zoals hierboven vermeld, zal, afhankelijk van de aard van de inbreuk en het risico dat deze met zich meebrengt, tijdige communicatie personen helpen maatregelen te nemen om zich tegen eventuele negatieve gevolgen van de inbreuk te beschermen.

Bijlage B van deze richtsnoeren bevat een niet-uitputtende lijst met voorbeelden van gevallen waarin een inbreuk waarschijnlijk zal leiden tot een hoog risico voor personen en bijgevolg gevallen waarin een verwerkingsverantwoordelijke een inbreuk aan de getroffen betrokkenen zal moeten meedelen.

B. Te verstrekken informatie

Artikel 34, lid 2, luidt als volgt:

"De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen".

Volgens deze bepaling dient de verwerkingsverantwoordelijke ten minste de volgende informatie te verstrekken:

- een beschrijving van de aard van de inbreuk;
- de naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt;
- een beschrijving van de waarschijnlijke gevolgen van de inbreuk; en
- een beschrijving van de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk aan te pakken, met inbegrip van, in voorkomend geval, maatregelen om de mogelijke nadelige gevolgen ervan te beperken.

Als voorbeeld van de maatregelen die zijn genomen om de inbreuk aan te pakken en de mogelijke nadelige gevolgen ervan te beperken, zou de verwerkingsverantwoordelijke kunnen verklaren dat hij na de melding van de inbreuk aan de betrokken toezichthoudende autoriteit advies heeft ontvangen over het beheer van de inbreuk en de beperking van de gevolgen ervan. De verwerkingsverantwoordelijke dient indien passend ook specifiek advies te geven aan personen om zich te beschermen tegen mogelijke negatieve gevolgen van de inbreuk, zoals het wijzigen van wachtwoorden indien hun toegangsgegevens in het bezit zijn gekomen van derden. Nogmaals, een

[36] Zie ook overweging 86.

verwerkingsverantwoordelijke kan ervoor kiezen om informatie te verstrekken naast wat hier vereist is.

C. Contact opnemen met personen

In principe dient de inbreuk rechtstreeks aan de getroffen betrokkenen te worden meegedeeld, tenzij dit onevenredige inspanningen zou vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij de betrokkenen even doeltreffend worden geïnformeerd (artikel 34, lid 3, onder c)).

De mededeling van een inbreuk aan de betrokkenen moet plaatsvinden via specifieke berichten die niet samen met andere informatie, zoals regelmatige updates, nieuwsbrieven of standaardberichten, mogen worden verzonden. Dit helpt om de communicatie over de inbreuk duidelijk en transparant te maken.

Voorbeelden van transparante communicatiemethoden zijn direct messaging (bijvoorbeeld e-mail, sms, directe berichten), in het oog springende banners of berichten op websites, communicatie per post en opvallende advertenties in gedrukte media. Een mededeling die beperkt blijft tot een persbericht of bedrijfsblog zou geen effectief middel zijn om een inbreuk aan een persoon mee te delen. De WP29 raadt verwerkingsverantwoordelijken aan een middel te kiezen waarbij de kans dat de informatie naar behoren aan alle getroffen personen wordt meegedeeld, zo groot mogelijk is. Afhankelijk van de omstandigheden kan dat betekenen dat de verwerkingsverantwoordelijke verschillende communicatiemethoden gebruikt in plaats van één enkel contactkanaal.

Verwerkingsverantwoordelijken moeten er mogelijk ook voor zorgen dat de communicatie beschikbaar is in passende alternatieve formats en in de relevante talen zodat de getroffen personen de aan hen verstrekte informatie kunnen begrijpen. Bijvoorbeeld wanneer een inbreuk aan een persoon wordt meegedeeld, zal de taal waarin in het verleden gewoonlijk met die persoon werd gecommuniceerd over het algemeen passend zijn. Treft de inbreuk echter betrokkenen met wie de verwerkingsverantwoordelijke nog niet eerder contact heeft gehad of die in een andere lidstaat of een ander niet-EU-land verblijven dan het land waar de verwerkingsverantwoordelijke is gevestigd, kan communicatie in de lokale nationale taal aanvaardbaar zijn, rekening houdend met de vereiste middelen. Het komt erop aan betrokkenen te helpen de aard van de inbreuk te begrijpen en hen uit te leggen welke maatregelen zij kunnen nemen om zichzelf te beschermen.

Verwerkingsverantwoordelijken zijn het best geplaatst om te bepalen welk contactkanaal het meest geschikt is om een inbreuk aan personen mee te delen, met name als zij frequent met hun klanten communiceren. Het is echter duidelijk dat een verwerkingsverantwoordelijke op zijn hoede moet zijn voor het gebruik van een contactkanaal dat door de inbreuk is gecompromitteerd, aangezien dit kanaal ook kan worden gebruikt door aanvallers die zich voordoen als de verwerkingsverantwoordelijke.

Tegelijkertijd wordt in overweging 86 het volgende uitgelegd:

> "Dergelijke kennisgevingen aan betrokkenen dienen zo snel als redelijkerwijs mogelijk te worden gedaan, in nauwe samenwerking met de toezichthoudende autoriteit en met inachtneming van de door haarzelf of door andere relevante autoriteiten, zoals rechtshandhavingsautoriteiten, aangereikte richtsnoeren. Zo zouden betrokkenen bijvoorbeeld onverwijld in kennis moeten worden gesteld wanneer een onmiddellijk risico op schade moet worden beperkt, terwijl een langere kennisgevingstermijn gerechtvaardigd kan zijn wanneer er passende maatregelen moeten worden genomen tegen aanhoudende of soortgelijke inbreuken in verband met persoonsgegevens."

Verwerkingsverantwoordelijken zouden daarom wellicht contact willen opnemen en overleg willen plegen met de toezichthoudende autoriteit, niet alleen om advies in te winnen over het informeren van betrokkenen over een inbreuk overeenkomstig artikel 34, maar ook over de passende berichten die aan

personen moeten worden verzonden en over de meest geschikte manier om contact met hen op te nemen.

Hieraan gekoppeld is het advies in overweging 88 dat bij de kennisgeving van een inbreuk "rekening [dient] te worden gehouden met de gerechtvaardigde belangen van de rechtshandhavingsautoriteiten wanneer vroegtijdige bekendmaking het onderzoek naar de omstandigheden van een inbreuk in verband met persoonsgegevens nodeloos zou hinderen". Dit kan betekenen dat de verwerkingsverantwoordelijke in bepaalde omstandigheden, wanneer zulks gerechtvaardigd is, en op advies van de rechtshandhavingsautoriteiten de mededeling van de inbreuk aan de getroffen personen kan uitstellen tot het tijdstip waarop dergelijke onderzoeken er niet langer door in het gedrang zouden komen. De betrokkenen zouden echter na dit tijdstip nog steeds onverwijld op de hoogte moeten worden gebracht.

Als het voor de verwerkingsverantwoordelijke niet mogelijk is een inbreuk aan een persoon mee te delen omdat er onvoldoende gegevens zijn opgeslagen om contact met die persoon op te nemen, dient de verwerkingsverantwoordelijke de betrokkene zo snel als redelijkerwijs mogelijk is op de hoogte te stellen (bijv. wanneer een persoon zijn in artikel 15 beschreven recht van inzage in persoonsgegevens uitoefent en de verwerkingsverantwoordelijke de nodige aanvullende informatie verstrekt om contact met hem op te nemen).

D. Voorwaarden waaronder geen mededeling vereist is

In artikel 34, lid 3, worden drie voorwaarden genoemd. Indien aan die voorwaarden is voldaan, hoeft een inbreuk niet aan personen te worden gemeld. Deze voorwaarden zijn:

- De verwerkingsverantwoordelijke heeft passende technische en organisatorische maatregelen genomen om persoonsgegevens vóór de inbreuk te beschermen, met name maatregelen die de persoonsgegevens onbegrijpelijk maken voor onbevoegden. Dit kan bijvoorbeeld de bescherming van persoonsgegevens door middel van geavanceerde versleuteling of door tokenisatie omvatten.
- Onmiddellijk na een inbreuk heeft de verwerkingsverantwoordelijke maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van natuurlijke personen zich waarschijnlijk niet meer zal voordoen. Afhankelijk van de omstandigheden van het geval is het bijvoorbeeld mogelijk dat de verwerkingsverantwoordelijke de persoon die toegang tot de persoonsgegevens heeft gehad onmiddellijk heeft geïdentificeerd en dat de verwerkingsverantwoordelijke actie heeft ondernomen voordat die persoon iets met de persoonsgegevens kon doen. Er moet nog naar behoren rekening worden gehouden met de mogelijke gevolgen van een eventuele inbreuk op de vertrouwelijkheid, eveneens afhankelijk van de aard van de betrokken gegevens.
- Het zou onevenredige inspanningen vergen[37] om contact op te nemen met personen, misschien omdat hun contactgegevens verloren zijn gegaan als gevolg van de inbreuk of omdat deze gegevens niet bekend zijn. Bijvoorbeeld het magazijn van een bureau voor de statistiek is overstroomd en de documenten die persoonsgegevens bevatten zijn alleen op papier opgeslagen. De verwerkingsverantwoordelijke moet een openbare mededeling doen of een soortgelijke maatregel nemen, waarbij de personen even doeltreffend worden geïnformeerd. In het geval van onevenredige inspanningen kan ook worden gedacht aan technische regelingen om informatie over de inbreuk op verzoek beschikbaar te stellen, wat nuttig kan blijken voor personen die door een inbreuk zijn getroffen maar met wie de verwerkingsverantwoordelijke anders geen contact kan opnemen.

[37] Zie de WP29-richtsnoeren inzake transparantie, waarin het probleem van onevenredige inspanningen aan de orde komt, die beschikbaar zijn op http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

Overeenkomstig het verantwoordingsbeginsel moeten verwerkingsverantwoordelijken aan de toezichthoudende autoriteit kunnen aantonen dat zij aan een of meer van deze voorwaarden voldoen [38]. Er zij echter op gewezen dat hoewel het in eerste instantie mogelijk niet verplicht is een inbreuk te melden indien er geen risico voor de rechten en vrijheden van natuurlijke personen is, dit in de loop van de tijd kan veranderen en het risico opnieuw moet worden geëvalueerd.

Als een verwerkingsverantwoordelijke besluit een inbreuk niet aan de persoon mee te delen, wordt in artikel 34, lid 4, uitgelegd dat de toezichthoudende autoriteit de verwerkingsverantwoordelijke hiertoe kan verplichten indien zij van mening is dat de inbreuk waarschijnlijk een hoog risico voor personen met zich meebrengt. Anderzijds kan de toezichthoudende autoriteit oordelen dat aan de voorwaarden van artikel 34, lid 3, is voldaan, in welk geval de inbreuk niet aan personen hoeft te worden meegedeeld. Indien de toezichthoudende autoriteit van oordeel is dat het besluit om de inbreuk niet aan de betrokkenen mee te delen niet gegrond is, kan zij overwegen gebruik te maken van haar beschikbare bevoegdheden en sancties.

IV. **Beoordeling van het risico en hoog risico**

A. Risico als aanleiding voor meldingen/mededelingen

Hoewel de AVG de verplichting invoert om een inbreuk te melden, is dit niet in alle omstandigheden verplicht:

- Een inbreuk moet aan de bevoegde toezichthoudende autoriteit worden gemeld, tenzij het onwaarschijnlijk is dat ze een risico voor de rechten en vrijheden van natuurlijke personen inhoudt.
- Een inbreuk wordt alleen aan de persoon meegedeeld als het waarschijnlijk is dat ze een hoog risico voor de rechten en vrijheden inhoudt.

Dit betekent dat het van essentieel belang is dat de verwerkingsverantwoordelijke onmiddellijk nadat hij kennis heeft gekregen van een inbreuk niet alleen tracht het incident onder controle te krijgen, maar ook het risico inschat dat eruit kan voortvloeien. Daar zijn twee belangrijke redenen voor: in de eerste plaats zal kennis van de waarschijnlijkheid en de potentiële ernst van het effect op de persoon de verwerkingsverantwoordelijke helpen om doeltreffende maatregelen te nemen teneinde de inbreuk in te dammen en aan te pakken; in de tweede plaats zal het de verwerkingsverantwoordelijke helpen bepalen of een melding aan de toezichthoudende autoriteit en, indien nodig, een mededeling aan de betrokken personen vereist is.

Zoals hierboven uiteengezet, moet een inbreuk worden gemeld/meegedeeld tenzij het onwaarschijnlijk is dat ze een risico voor de rechten en vrijheden van natuurlijke personen inhoudt. De belangrijkste aanleiding op grond waarvan een inbreuk aan betrokkenen moet worden meegedeeld, is als het waarschijnlijk is dat de inbreuk een *hoog* risico voor de rechten en vrijheden van natuurlijke personen met zich meebrengt. Dit risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen wier gegevens het voorwerp van de inbreuk zijn. Voorbeelden van dergelijke schade zijn discriminatie, identiteitsdiefstal of -fraude, financieel verlies en reputatieschade. Wanneer de inbreuk betrekking heeft op persoonsgegevens waaruit ras of etnische afkomst, politieke opvatting, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt, of op persoonsgegevens die genetische gegevens of gegevens met betrekking tot de gezondheid

[38] Zie artikel 5, lid 2.

of het seksleven, of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen omvatten, moet dergelijke schade als waarschijnlijk worden beschouwd[39].

B. Factoren waarmee rekening moet worden gehouden bij de beoordeling van risico's

In de overwegingen 75 en 76 van de AVG wordt gesuggereerd dat in het algemeen bij de beoordeling van risico's rekening moet worden gehouden met zowel de waarschijnlijkheid als de ernst van het risico voor de rechten en vrijheden van betrokkenen. Voorts is in deze overwegingen bepaald dat risico's moeten worden geëvalueerd op basis van een objectieve beoordeling.

Opgemerkt dient te worden dat de focus bij de beoordeling van het risico voor de rechten en vrijheden van personen als gevolg van een inbreuk verschilt van de focus bij de beoordeling van het risico in het kader van een gegevensbeschermingseffectbeoordeling)[40]. Bij een gegevensbeschermingseffectbeoordeling wordt rekening gehouden met zowel de risico's van de gegevensverwerking die wordt uitgevoerd zoals gepland als de risico's van een inbreuk. Bij de beoordeling van een mogelijke inbreuk wordt in het kader van een gegevensbeschermingseffectbeoordeling in algemene termen gekeken naar de waarschijnlijkheid dat de inbreuk zich voordoet en naar de schade die de betrokkene daardoor zou kunnen lijden; met andere woorden, het gaat om de beoordeling van een hypothetische gebeurtenis. Bij een daadwerkelijke inbreuk heeft de gebeurtenis zich al voorgedaan en gaat de aandacht dus volledig uit naar het daaruit voortvloeiende risico van het effect van de inbreuk op personen.

Voorbeeld:

Een gegevensbeschermingseffectbeoordeling wijst erop dat het voorgestelde gebruik van bepaalde beveiligingssoftware voor de bescherming van persoonsgegevens een geschikte maatregel is om een beveiligingsniveau te waarborgen dat is afgestemd op het risico dat de verwerking anders voor personen zou inhouden. Indien later echter een kwetsbaarheid in de software aan het licht komt, zou dit de software minder geschikt maken om het risico voor de beschermde persoonsgegevens te beperken en zou het risico dus opnieuw moeten worden beoordeeld in het kader van een lopende gegevensbeschermingseffectbeoordeling.

Een kwetsbaarheid in de software wordt later uitgebuit en er doet zich een inbreuk voor. De verwerkingsverantwoordelijke dient de specifieke omstandigheden van de inbreuk, de betrokken gegevens, het potentiële niveau van het effect op personen en de waarschijnlijkheid dat dit risico zich zal voordoen, te beoordelen.

Bijgevolg dient de verwerkingsverantwoordelijke bij de beoordeling van het risico dat een inbreuk voor personen inhoudt rekening te houden met de specifieke omstandigheden van de inbreuk, met inbegrip van de ernst van het potentiële effect en de waarschijnlijkheid dat dit zich voordoet. De WP29 beveelt daarom aan om bij de beoordeling rekening te houden met de volgende criteria[41]:

[39] Zie de overwegingen 75 en 85.

[40] Zie de richtsnoeren van de WP29 voor gegevensbeschermingseffectbeoordelingen: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[41] Artikel 3, lid 2, van Verordening (EU) nr. 611/2013 bevat richtsnoeren met betrekking tot de factoren die bij de melding van inbreuken in de sector elektronische-communicatiediensten in aanmerking moeten worden genomen. Deze richtsnoeren kunnen nuttig zijn in de context van meldingen krachtens de AVG. Zie http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:nl:PDF

- De aard van de inbreuk

Het type inbreuk dat heeft plaatsgevonden, kan van invloed zijn op het risico voor personen. Zo kan een inbreuk op de vertrouwelijkheid waarbij aan onbevoegden medische informatie is verstrekt andere gevolgen voor een persoon hebben dan een inbreuk waarbij medische gegevens van een persoon zijn verloren gegaan en niet langer beschikbaar zijn.

- De aard, gevoeligheid en omvang van de persoonsgegevens

Bij het beoordelen van risico's zijn natuurlijk de aard en gevoeligheid van de persoonsgegevens die door de inbreuk zijn gecompromitteerd een belangrijke factor. Hoe gevoeliger de gegevens, hoe groter gewoonlijk het risico op schade voor de betrokkenen. Er moet echter ook rekening worden gehouden met andere persoonsgegevens die mogelijk al over de betrokkene beschikbaar zijn. Het is bijvoorbeeld onwaarschijnlijk dat de bekendmaking van de naam en het adres van een persoon in normale omstandigheden aanzienlijke schade zal veroorzaken. Worden echter de naam en het adres van een adoptieouder aan een biologische ouder bekendgemaakt, kunnen de gevolgen zeer ernstig zijn voor zowel de adoptieouder als het kind.

Inbreuken waarbij gezondheidsgegevens, identiteitsdocumenten of financiële gegevens (bijv. creditcardgegevens) betrokken zijn, kunnen elk op zich schade veroorzaken, maar als die gegevens worden gecombineerd, kunnen ze worden gebruikt voor identiteitsdiefstal. Een combinatie van persoonsgegevens is doorgaans gevoeliger dan een enkel persoonsgegeven.

Sommige soorten persoonsgegevens kunnen op het eerste gezicht vrij onschuldig lijken, maar wat die gegevens over de betrokken persoon kunnen onthullen, moet zorgvuldig worden overwogen. Een lijst van klanten die thuis regelmatig bestellingen ontvangen is misschien niet bijzonder gevoelig, maar dezelfde gegevens over klanten die hebben verzocht om de leveringen stop te zetten terwijl ze op vakantie zijn, zou nuttige informatie zijn voor criminelen.

Evenzo kan een kleine hoeveelheid zeer gevoelige persoonsgegevens grote gevolgen hebben voor een persoon en kan een grote verscheidenheid aan gegevens een nog grotere verscheidenheid aan informatie over die persoon onthullen. Ook kan een inbreuk waarbij toegang is verkregen tot grote hoeveelheden persoonsgegevens over veel betrokkenen gevolgen hebben voor een overeenkomstig groot aantal personen.

- Gemak waarmee personen kunnen worden geïdentificeerd

Een belangrijke factor om rekening mee te houden is hoe gemakkelijk het voor iemand die toegang heeft tot gecompromitteerde persoonsgegevens zal zijn om specifieke personen te identificeren, of om de gegevens te matchen met andere informatie om personen te identificeren. Afhankelijk van de omstandigheden kan het mogelijk zijn om direct op basis van de gecompromitteerde persoonsgegevens de identiteit van de betrokkene te achterhalen zonder dat daar speciaal onderzoek voor nodig is, of kan het uiterst moeilijk zijn om persoonsgegevens aan een bepaalde persoon te koppelen, maar kan dat onder bepaalde omstandigheden toch mogelijk zijn. Identificatie kan direct of indirect mogelijk zijn op basis van de gecompromitteerde gegevens, maar kan ook afhankelijk zijn van de specifieke context van de inbreuk en de publieke beschikbaarheid van gerelateerde persoonsgegevens. Dit kan relevanter zijn voor inbreuken op de vertrouwelijkheid en de beschikbaarheid.

Zoals hierboven vermeld, zullen persoonsgegevens die door een passend niveau van versleuteling worden beschermd onbegrijpelijk zijn voor onbevoegden die niet over de decodeersleutel beschikken. Daarnaast kan een goed uitgevoerde pseudonimisering (in artikel 4, lid 5, gedefinieerd als "het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische

maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld") ook de kans verkleinen dat personen in het geval van een inbreuk worden geïdentificeerd. Pseudonimiseringstechnieken alleen maken de gegevens echter niet onbegrijpelijk.

- Ernst van gevolgen voor personen.

Afhankelijk van de aard van de bij een inbreuk betrokken persoonsgegevens, bijvoorbeeld speciale gegevenscategorieën, kan de schade voor personen die daaruit zou kunnen voortvloeien bijzonder ernstig zijn, met name als de inbreuk zou kunnen leiden tot identiteitsdiefstal of -fraude, lichamelijk letsel, psychisch leed, vernedering of reputatieschade. Als de inbreuk betrekking heeft op persoonsgegevens van kwetsbare personen, kunnen zij een groter risico op schade lopen.

Of de verwerkingsverantwoordelijke zich er al dan niet van bewust is dat persoonsgegevens in handen zijn van personen van wie de intenties onbekend of mogelijk kwaadwillig zijn, kan van invloed zijn op het niveau van het potentiële risico. Er kan een inbreuk op de vertrouwelijkheid zijn, waarbij persoonsgegevens per vergissing aan een derde, zoals gedefinieerd in artikel 4, lid 10, of aan een andere ontvanger worden verstrekt. Dit kan bijvoorbeeld het geval zijn als persoonsgegevens per ongeluk naar de verkeerde afdeling van een organisatie of naar een veelgebruikte organisatie van leveranciers worden gestuurd. De verwerkingsverantwoordelijke kan de ontvanger verzoeken om de ontvangen gegevens terug te sturen of veilig te vernietigen. In beide gevallen kan de ontvanger als "betrouwbaar" worden beschouwd aangezien de verwerkingsverantwoordelijke een zakelijk relatie met hem onderhoudt en mogelijk op de hoogte is van de procedures, de voorgeschiedenis en andere relevante details van de ontvanger. Met andere woorden, de verwerkingsverantwoordelijke kan een mate van zekerheid hebben ten aanzien van de ontvanger, zodat hij redelijkerwijs kan verwachten dat die partij de per vergissing verzonden gegevens niet leest of er geen toegang toe heeft, en dat zij zich houdt aan zijn instructies om deze terug te sturen. Zelfs als de gegevens zijn ingekeken, kan de verwerkingsverantwoordelijke er mogelijk nog op vertrouwen dat de ontvanger er verder niets mee zal doen en dat hij de gegevens onmiddellijk naar de verwerkingsverantwoordelijke zal terugsturen en zijn medewerking zal verlenen aan het herstel van de gegevens. In dergelijke gevallen kan dit worden meegewogen in de risicobeoordeling die de verwerkingsverantwoordelijke na de inbreuk uitvoert – het feit dat de ontvanger wordt vertrouwd, kan de ernst van de gevolgen van de inbreuk tenietdoen, maar betekent niet dat er geen inbreuk heeft plaatsgevonden. Dit kan echter op zijn beurt betekenen dat de risico's voor personen niet langer waarschijnlijk zijn, waardoor de verwerkingsverantwoordelijke de inbreuk niet langer aan de toezichthoudende autoriteit moet melden of aan de getroffen personen moet meedelen. Nogmaals, dit verschilt van geval tot geval. Niettemin moet de verwerkingsverantwoordelijke informatie over de inbreuk nog steeds bijhouden in het kader van de algemene verplichting om gegevens over inbreuken te registreren en bij te houden (zie deel V hieronder).

Er moet ook rekening worden gehouden met het blijvende karakter van de gevolgen voor personen, waarbij de gevolgen als groter kunnen worden beschouwd indien het langetermijneffecten betreft.

- Bijzondere kenmerken van de persoon

Een inbreuk kan betrekking hebben op persoonsgegevens van kinderen of andere kwetsbare personen, die als gevolg daarvan een groter risico of gevaar lopen. Er kunnen andere factoren met betrekking tot de persoon zijn die van invloed kunnen zijn op de mate waarin de inbreuk voor hem gevolgen heeft.

- Bijzondere kenmerken van de verwerkingsverantwoordelijke

De aard en rol van de verwerkingsverantwoordelijke en zijn activiteiten kunnen van invloed zijn op het risico dat een inbreuk voor personen inhoudt. Zo zal een medische organisatie speciale categorieën van persoonsgegevens verwerken, wat betekent dat er een grotere bedreiging is voor personen als hun persoonsgegevens zijn geschonden dan bij een mailinglijst van een krant.

- Het aantal getroffen persoon

Een inbreuk kan slechts één persoon treffen of kan een paar personen, enkele duizenden personen of nog veel meer personen treffen. Over het algemeen kan een inbreuk grotere gevolgen hebben naarmate er meer personen bij betrokken zijn. Een inbreuk kan echter zelfs voor één persoon ernstige gevolgen hebben, afhankelijk van de aard van de persoonsgegevens en de context waarin deze zijn gecompromitteerd. Ook hier komt het erop aan te kijken naar de waarschijnlijkheid en ernst van de gevolgen voor de getroffenen.

- Algemene punten

Daarom dient de verwerkingsverantwoordelijke bij de beoordeling van het risico dat waarschijnlijk uit een inbreuk zal voortvloeien, rekening te houden met een combinatie van de ernst van de mogelijke gevolgen voor de rechten en vrijheden van natuurlijke personen en de waarschijnlijkheid dat deze zich voordoen. Het is duidelijk dat wanneer de gevolgen van een inbreuk ernstiger zijn, het risico groter is en dat wanneer de waarschijnlijkheid dat deze zich voordoen groter is, het risico ook groter is. In geval van twijfel dient de verwerkingsverantwoordelijke het zekere voor het onzekere te nemen en de inbreuk te melden. In bijlage B worden enkele nuttige voorbeelden gegeven van verschillende soorten inbreuken waarbij sprake is van een risico of een hoog risico voor personen.

Het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (ENISA) heeft aanbevelingen opgesteld voor een methode om de ernst van een inbreuk te beoordelen. Verwerkingsverantwoordelijken en verwerkers kunnen deze aanbevelingen nuttig vinden bij het opstellen van hun reactieplan voor het beheer van inbreuken[42].

V. **Verantwoordingsplicht en registratie**

A. Inbreuken documenteren

Ongeacht of een inbreuk aan de toezichthoudende autoriteit moet worden gemeld, moet de verwerkingsverantwoordelijke alle inbreuken documenteren, zoals in artikel 33, lid 5, wordt uitgelegd:

> "De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren."

Dit hangt samen met het in artikel 5, lid 2, vervatte verantwoordingsbeginsel van de AVG. Het doel van de registratie van zowel niet te melden als te melden inbreuken houdt ook verband met de verplichtingen van de verwerkingsverantwoordelijke op grond van artikel 24. De toezichthoudende autoriteit kan verzoeken om inzage in deze geregistreerde gegevens. Verwerkingsverantwoordelijken worden er daarom toe aangemoedigd een intern register van inbreuken op te zetten, ongeacht of voor die inbreuken een meldingsplicht geldt[43].

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity

[43] De verwerkingsverantwoordelijke kan ervoor kiezen inbreuken te documenteren als onderdeel van zijn registratie van verwerkingsactiviteiten die overeenkomstig artikel 30 wordt bijgehouden. Een afzonderlijk

Hoewel het aan de verwerkingsverantwoordelijke is om te bepalen welke methode en structuur bij het documenteren van een inbreuk moeten worden gebruikt, zijn er wat te registreren informatie betreft belangrijke elementen die in alle gevallen moeten worden opgenomen. Zoals vereist op grond van artikel 33, lid 5, dient de verwerkingsverantwoordelijke bijzonderheden met betrekking tot de inbreuk te registreren, waaronder de oorzaken, wat er zich heeft afgespeeld en de betrokken persoonsgegevens. De verwerkingsverantwoordelijke dient ook de gevolgen van de inbreuk te registreren, alsmede de corrigerende maatregelen die hij heeft genomen.

In de AVG is niet gespecificeerd hoelang deze documentatie moet worden bewaard. Indien deze geregistreerde gegevens persoonsgegevens bevatten, is het aan de verwerkingsverantwoordelijke om de passende bewaartermijn te bepalen in overeenstemming met de beginselen voor de verwerking van persoonsgegevens[44] en om te voldoen aan de rechtsgrond voor de verwerking[45]. Hij dient de documentatie overeenkomstig artikel 33, lid 5, te bewaren voor zover de toezichthoudende autoriteit de verwerkingsverantwoordelijke kan verzoeken om het bewijs te leveren dat hij dat artikel, of meer in het algemeen het verantwoordingsbeginsel, naleeft. Als de geregistreerde gegevens geen persoonsgegevens bevatten, is het in de AVG opgenomen beginsel van opslagbeperking uiteraard niet van toepassing.[46]

Naast deze details beveelt de WP29 aan dat de verwerkingsverantwoordelijke ook zijn motivering voor de besluiten die naar aanleiding van een inbreuk zijn genomen, documenteert. Met name wanneer inbreuk niet is gemeld, moet de motivering voor dat besluit worden gedocumenteerd. De motivering dient de redenen te omvatten waarom de verwerkingsverantwoordelijke van mening is dat de inbreuk waarschijnlijk geen risico voor de rechten en vrijheden van natuurlijke personen inhoudt[47]. Indien de verwerkingsverantwoordelijke van mening is dat aan een van de voorwaarden van artikel 34, lid 3, is voldaan, moet hij afdoend bewijs kunnen leveren dat dit het geval is.

Als de verwerkingsverantwoordelijke een inbreuk niet meldt aan de toezichthoudende autoriteit maar de melding uitstelt, moet hij dat uitstel kunnen motiveren; documentatie in verband daarmee zou kunnen helpen om aan te tonen dat het uitstel gerechtvaardigd en niet buitensporig is.

Indien de verwerkingsverantwoordelijke een inbreuk aan de getroffen personen meedeelt, dient hij transparant te zijn over de inbreuk en doeltreffend en tijdig te communiceren. Bijgevolg zou het de verwerkingsverantwoordelijke helpen om aan te tonen dat hij het verantwoordingsbeginsel naleeft en zich aan de regels houdt door het bewijs van die mededeling te bewaren.

Ter ondersteuning van de naleving van de artikelen 33 en 34 zou het voor zowel verwerkingsverantwoordelijken als verwerkers nuttig zijn over een gedocumenteerde meldingsprocedure te beschikken waarin wordt uiteengezet welke procedure moet worden gevolgd wanneer een inbreuk is geconstateerd, met inbegrip van de wijze waarop het incident moet worden ingeperkt, beheerd en hersteld, het risico moet worden beoordeeld en de inbreuk moet worden gemeld. Om aan te tonen dat de AVG wordt nageleefd, kan het in dit verband ook nuttig zijn om aan te tonen dat werknemers op de hoogte zijn gebracht van het bestaan van dergelijke procedures en mechanismen en dat zij weten hoe zij op inbreuken moeten reageren.

---

register is niet vereist, mits de informatie met betrekking tot de inbreuk duidelijk als zodanig herkenbaar is en op verzoek kan worden opgevraagd.

[44] Zie artikel 5.

[45] Zie artikel 6 en ook artikel 9.

[46] Zie artikel 5, lid 1, onder e).

[47] Zie overweging 85.

Merk op dat het niet naar behoren documenteren van een inbreuk ertoe kan leiden dat de toezichthoudende autoriteit haar bevoegdheden op grond van artikel 58 uitoefent en/of een administratieve boete oplegt in overeenstemming met artikel 83.

B. Rol van de functionaris voor gegevensbescherming

Een verwerkingsverantwoordelijke of verwerker kan een functionaris voor gegevensbescherming hebben[48], hetzij op grond van artikel 37, hetzij vrijwillig als goede praktijk. In artikel 39 van de AVG zijn een aantal verplichte taken van de functionaris voor gegevensbescherming vastgesteld, maar dit belet de verwerkingsverantwoordelijke niet om indien passend extra taken toe te wijzen.

De verplichte taken van de functionaris voor gegevensbescherming die van bijzonder belang zijn voor de melding van inbreuken, zijn onder meer: het verstrekken van advies en informatie over gegevensbescherming aan de verwerkingsverantwoordelijke of verwerker, het toezien op de naleving van de AVG en het verstrekken van advies met betrekking tot gegevensbeschermingseffectbeoordelingen. De functionaris voor gegevensbescherming werkt ook samen met de toezichthoudende autoriteit en fungeert als contactpunt voor de toezichthoudende autoriteit en voor de betrokkenen. Er zij ook op gewezen dat in artikel 33, lid 3, onder b), is bepaald dat de verwerkingsverantwoordelijke bij de melding van een inbreuk aan de toezichthoudende autoriteit de naam en contactgegevens van zijn functionaris voor gegevensbescherming of een ander contactpunt moet verstrekken.

Wat de documentatie van inbreuken betreft, kan het zijn dat de verwerkingsverantwoordelijke of verwerker het advies van zijn functionaris voor gegevensbescherming wenst in te winnen over de structuur, de opstelling en het beheer van deze documentatie. De functionaris voor gegevensbescherming zou ook kunnen worden belast met het bijhouden van dergelijke gegevens.

Deze factoren houden in dat de functionaris voor gegevensbescherming een sleutelrol moet spelen bij de preventie van of de voorbereiding op een inbreuk door advies te verstrekken en toe te zien op de naleving, zowel tijdens een inbreuk (d.w.z. bij het in kennis stellen van de toezichthoudende autoriteit) als tijdens elk daaropvolgend onderzoek door de toezichthoudende autoriteit. In dit licht beveelt de WP29 aan dat de functionaris voor gegevensbescherming onmiddellijk op de hoogte wordt gebracht van het bestaan van een inbreuk en wordt betrokken bij het gehele proces om de inbreuk te beheren en te melden.

VI. Kennisgevingsverplichtingen op grond van andere rechtsinstrumenten

Naast en los van de melding en mededeling van inbreuken in het kader van de AVG dienen verwerkingsverantwoordelijken zich ook bewust te zijn van elke verplichting om veiligheidsincidenten te melden op grond van andere aanverwante wetgeving die mogelijk op hen van toepassing is en of deze hen tegelijkertijd ook kan verplichten om de toezichthoudende autoriteit in kennis te stellen van een inbreuk in verband met persoonsgegevens. Deze verplichtingen kunnen van lidstaat tot lidstaat verschillen. Hieronder volgen enkele voorbeelden van kennisgevingsverplichtingen in andere rechtsinstrumenten en van de wijze waarop deze zich tot de AVG verhouden:

[48] Zie de WP-richtlijnen voor functionarissen voor gegevensbescherming: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- Verordening (EU) nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS-verordening)[49].

Krachtens artikel 19, lid 2, van de eIDAS-verordening moeten verleners van vertrouwensdiensten het toezichthoudende orgaan in kennis stellen van een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de verleende vertrouwensdienst of voor de persoonsgegevens die daarmee worden beheerd. Indien van toepassing – d.w.z. wanneer een dergelijke inbreuk of een dergelijk verlies ook een inbreuk in verband met persoonsgegevens is krachtens de AVG – moet de verlener van trustdiensten de inbreuk ook aan de toezichthoudende autoriteit melden.

- Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS-richtlijn)[50].

Op grond van de artikelen 14 en 16 van de NIS-richtlijn zijn aanbieders van essentiële diensten en digitaledienstverleners verplicht veiligheidsincidenten aan hun bevoegde autoriteit te melden. Zoals in overweging 63 van de NIS-richtlijn erkend[51], kan bij veiligheidsincidenten vaak sprake zijn van een compromittering van persoonsgegevens. Hoewel in de NIS-richtlijn is bepaald dat bevoegde autoriteiten en toezichthoudende autoriteiten in deze context moeten samenwerken en informatie moeten uitwisselen, blijft het zo dat wanneer dergelijke incidenten krachtens de AVG inbreuken in verband met persoonsgegevens zijn of worden, deze aanbieders en/of verleners verplicht zouden zijn de toezichthoudende autoriteit daarvan in kennis te stellen, los van de in de NIS-richtlijn opgenomen verplichtingen inzake de melding van incidenten.

Voorbeeld:

Een aanbieder van clouddiensten die een inbreuk meldt overeenkomstig de NIS-richtlijn, moet mogelijk ook een verwerkingsverantwoordelijke op de hoogte stellen als er ook sprake is van een inbreuk in verband met persoonsgegevens. Evenzo kan een verlener van vertrouwensdiensten die in het kader van de eIDAS-verordening een inbreuk meldt ook verplicht zijn de bevoegde gegevensbeschermingsautoriteit in kennis te stellen van de inbreuk.

- Richtlijn 2009/136/EG (de burgerrechtenrichtlijn) en Verordening (EU) nr. 611/2013 (de verordening betreffende het melden van inbreuken).

Aanbieders van openbare elektronische-communicatiediensten in de context van Richtlijn 2002/58/EG[52] moeten inbreuken melden aan de bevoegde nationale autoriteiten.

---

[49] Zie http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[50] Zie http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

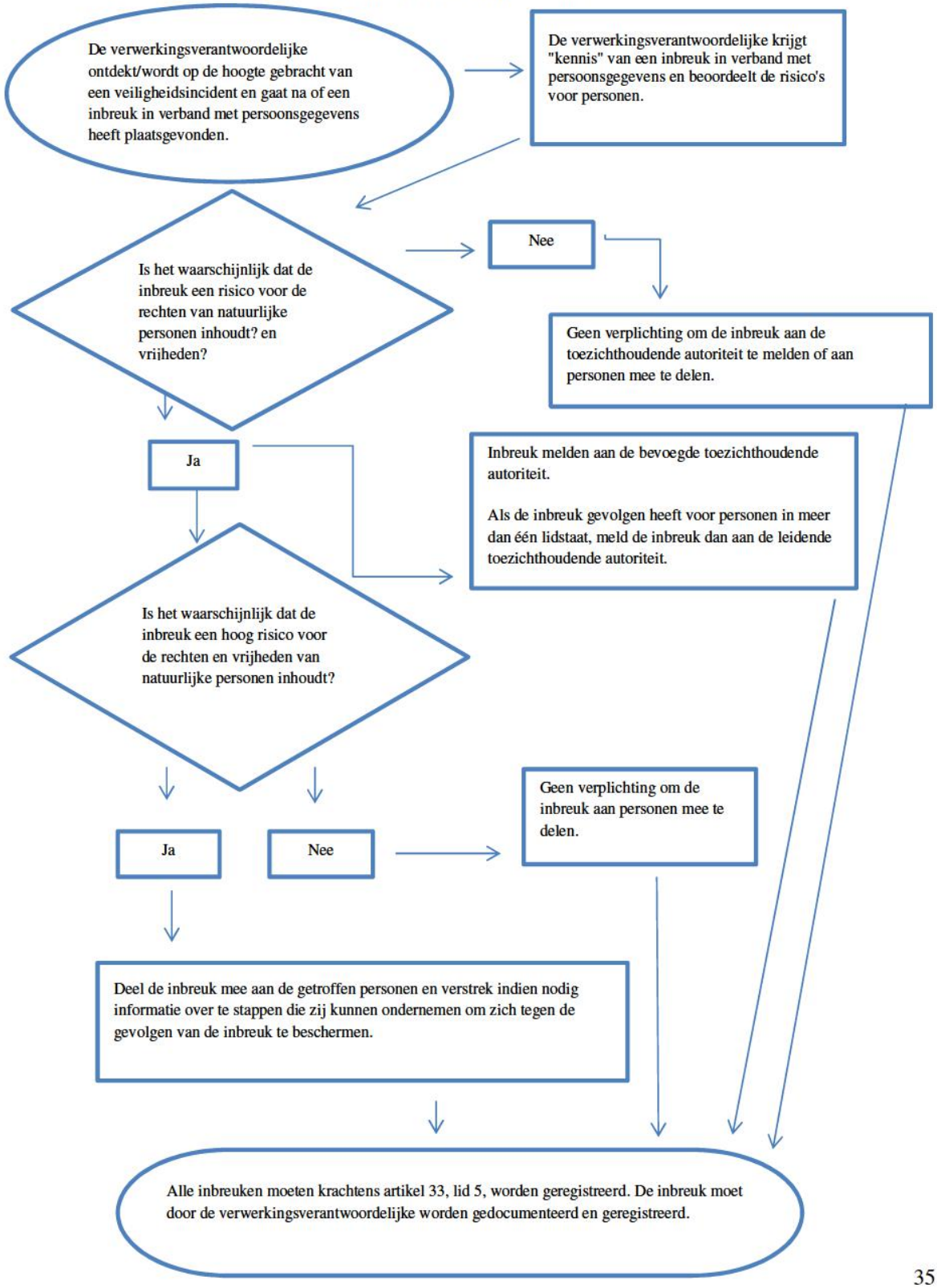
51 Overweging 63: *"In veel gevallen worden persoonsgegevens aangetast als gevolg van incidenten. Daarom moeten de bevoegde autoriteiten en de autoriteiten voor gegevensbescherming samenwerken en informatie over alle relevante zaken uitwisselen om inbreuken in verband met persoonsgegevens als gevolg van incidenten aan te pakken."*

[52] Op 10 januari 2017 heeft de Europese Commissie een verordening betreffende privacy en elektronische communicatie voorgesteld die Richtlijn 2009/136/EG zal vervangen en de kennisgevingsverplichtingen zal afschaffen. Zolang dit voorstel echter niet door het Europees Parlement is goedgekeurd, blijft de bestaande meldingsverplichting van kracht, zie https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

Verwerkingsverantwoordelijken moeten ook op de hoogte zijn van aanvullende wettelijke, medische of professionele kennisgevingsverplichtingen op grond van andere toepasselijke regelingen.

VII. Bijlage

A. Stroomschema met kennisgevingsverplichtingen



B. Voorbeelden van inbreuken in verband met persoonsgegevens en aan wie de inbreuken moeten worden gemeld/meegedeeld

De volgende niet-limitatieve voorbeelden helpen verwerkingsverantwoordelijken bepalen of zij in verschillende scenario's van inbreuken in verband met persoonsgegevens de inbreuk al dan niet moeten melden/meedelen. Deze voorbeelden kunnen ook helpen om een onderscheid te maken tussen risico en hoog risico voor de rechten en vrijheden van natuurlijke personen.

Voorbeeld:	**Melden aan de toezichthoudende autoriteit?**	**Meedelen aan de betrokkene?**	**Opmerkingen/aanbevelingen**
i. 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.
ii. Een verwerkingsverantwoordelijke exploiteert een onlinedienst. 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.	
iii. Een stroomstoring van enkele minuten in het callcenter van een verwerkingsverantwoordelijke heeft tot gevolg dat klanten de verwerkingsverantwoordelijke 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.
iv. 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.
v. 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	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 verwerkingsverantwoordelijke de inbreuk meedelen aan andere personen indien er een groot risico voor hen bestaat.

andere personen.			
vi. 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 digitaledienstverlener.
vii. 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 verwerkingsverantwoordelijke 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.

viii. 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 privacy van de patiënt.	Ja, deel deze inbreuk mee aan de getroffen personen.	
ix. 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.	
x. 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: 2023-10-06 14:03:41+00:00
Aan: Frank Rijkaart
CC: art.5.1-2e art.5.1-2e ; art.5.1-2e
Onderwerp: IAV advies Frank - FW: Datalek Youforce: advies melden aan AP
"

Zie onderstaande mail ter beantwoording.

Met vriendelijke groet,

art.5.1-2e

Bestuursassistent van gedeputeerde de heer F. Rijkaart

Gedeputeerde van: Landbouw en Visserij, Stikstof, Gebiedsgedeputeerde Veenweiden ZH-PLG, Groene Hart (NOVEX), Personeel & Organisatie

M art.5.1-2e

E art.5.1-2e)pzh.nl <mailt o art.5.1-2e)pzh.nl>

Werkdagen: ma/di/do/vr

Krachtig Zuid-Holland.

Van: Frank Rijkaart <f.rijkaart@pzh.nl>
Verzonden: vrijdag 6 oktober 2023 13:58
Aan: art.5.1-2e pzh.nl>
Onderwerp: FW: Datalek Youforce: advies melden aan AP

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto: art.5.1-2e pzh.nl> >
Verzonden: vrijdag 6 oktober 2023 13:57:55 (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Aan: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
CC: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; Frank Rijkaart <f.rijkaart@pzh.nl <mailto:f.rijkaart@pzh.nl> >; privacy <privacy@pzh.nl <mailto:privacy@pzh.nl> >
Onderwerp: Datalek Youforce: advies melden aan AP

Beste art.5.1-2e

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

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

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

Met vriendelijke groet,

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7art.5.1-2e art.5.1-2e%40pzh.nl%7Cb671e54abf6b4d2ac2a608dbc66448a5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638321906267647148%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=%2Fco05LqHr9Ama0qMi4aeKHZTlSkJxjTz5F8m%2FTcjwyM%3D&reserved=0>

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

Krachtig Zuid-Holland


provincie
Zuid-Holland

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Status: concept

Melding gegevens

Aangemeld door	:	art.5.1-2e (FG)
Registratienummer van het incident	:	M23 10 00723
Datum en tijdstip van de melding	:	5 oktober 2023, 15:50
Route van de melding	:	melding bestanden in te zien zonder de juiste rechten (digitale Loket op Binnenplein)

Advies

Opgesteld door	:	art.5.1-2e
Datum en tijdstip advies	:	6 oktober 2023 11:06
Advies besproken met	:	Besproken met art.5.1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Gedeeld met eenheid Privacy

Situatie

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

Beoordeling van de ernst van de situatie

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

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

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

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

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

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

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

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

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

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

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


provincie
Zuid-Holland


15:45
6
Frank Rijkaart
laatst gez. vandaag om 13:32
do 21 sep.
Berichten en gesprekken worden end-to-end versleuteld. Niemand buiten deze chat kan ze lezen of beluisteren, zelfs WhatsApp niet. Tik voor meer informatie.
Frank, zie de mail van art.5.1-2e Belangrijk signaal. Heeft mijn hoogste aandacht. Ik hou je op de hoogte van te zetten stappen.
Groet, art.5.1-2e
10:08
Was er al nieuws? Ben even benieuwd naar de stand van zaken Want uit het nadere onderzoek is wel gebleken dat dit een ernstig lek is. Morgen ben ik de gehele dag zo ongeveer onderweg op werkbezoeken. Tussen 0700 en 0830 zit ik in de auto. Vanaf 1530 ben ik weer in de auto op de weg terug maar indien nodig onderbreek ik mijn werkbezoek.
Duidelijk is dat actie niet uit kan blijven. Wat de mail van art.5.1-2e niet duidelijk maakt maar ik wel wil weten: is dit lek alleen toegankelijk


15:46
6
Frank Rijkaart
laatst gez. vandaag om 13:32
Was er al nieuws? Ben even benieuwd naar de stand van zaken Want uit het nadere onderzoek is wel gebleken dat dit een ernstig lek is. Morgen ben ik de gehele dag zo ongeveer onderweg op werkbezoeken. Tussen 0700 en 0830 zit ik in de auto. Vanaf 1530 ben ik weer in de auto op de weg terug maar indien nodig onderbreek ik mijn werkbezoek.
Duidelijk is dat actie niet uit kan blijven. Wat de mail van art.5.1-2e niet duidelijk maakt maar ik wel wil weten: is dit lek alleen toegankelijk voor mensen binnen de organisatie die geen toegang behoren te hebben tot deze delen van IDMS of is het ook voor externen toegankelijk (geweest)?
Is het probleem te isoleren/ makkelijk op te lossen door de delen alsnog af te sluiten? Zo nee? Dan vrees ik dat er niets anders op zit dan IDMS af te sluiten tot het probleem is opgelost en de data veilig is.


15:46
6
Frank Rijkaart
laatst gez. vandaag om 13:32
dag zo ongeveer onderweg op werkbezoeken. Tussen 0700 en 0830 zit ik in de auto. Vanaf 1530 ben ik weer in de auto op de weg terug maar indien nodig onderbreek ik mijn werkbezoek.
Duidelijk is dat actie niet uit kan blijven. Wat de mail van Niels niet duidelijk maakt maar ik wel wil weten: is dit lek alleen toegankelijk voor mensen binnen de organisatie die geen toegang behoren te hebben tot deze delen van IDMS of is het ook voor externen toegankelijk (geweest)?
Is het probleem te isoleren/ makkelijk op te lossen door de delen alsnog af te sluiten? Zo nee? Dan vrees ik dat er niets anders op zit dan IDMS af te sluiten tot het probleem is opgelost en de data veilig is.
Daarnaast dienen we tevens maatregelen te nemen om al onze systemen te reviewen en naar aanleiding daarvan waar nodig te verbeteren.
21:53

Werkinstructie Datalek

Definitie:
Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Hierdoor kunnen de betrokken personen schade leiden.

AVG kent de term datalek niet! Er is sprake van inbreuk in verband met persoonsgegevens

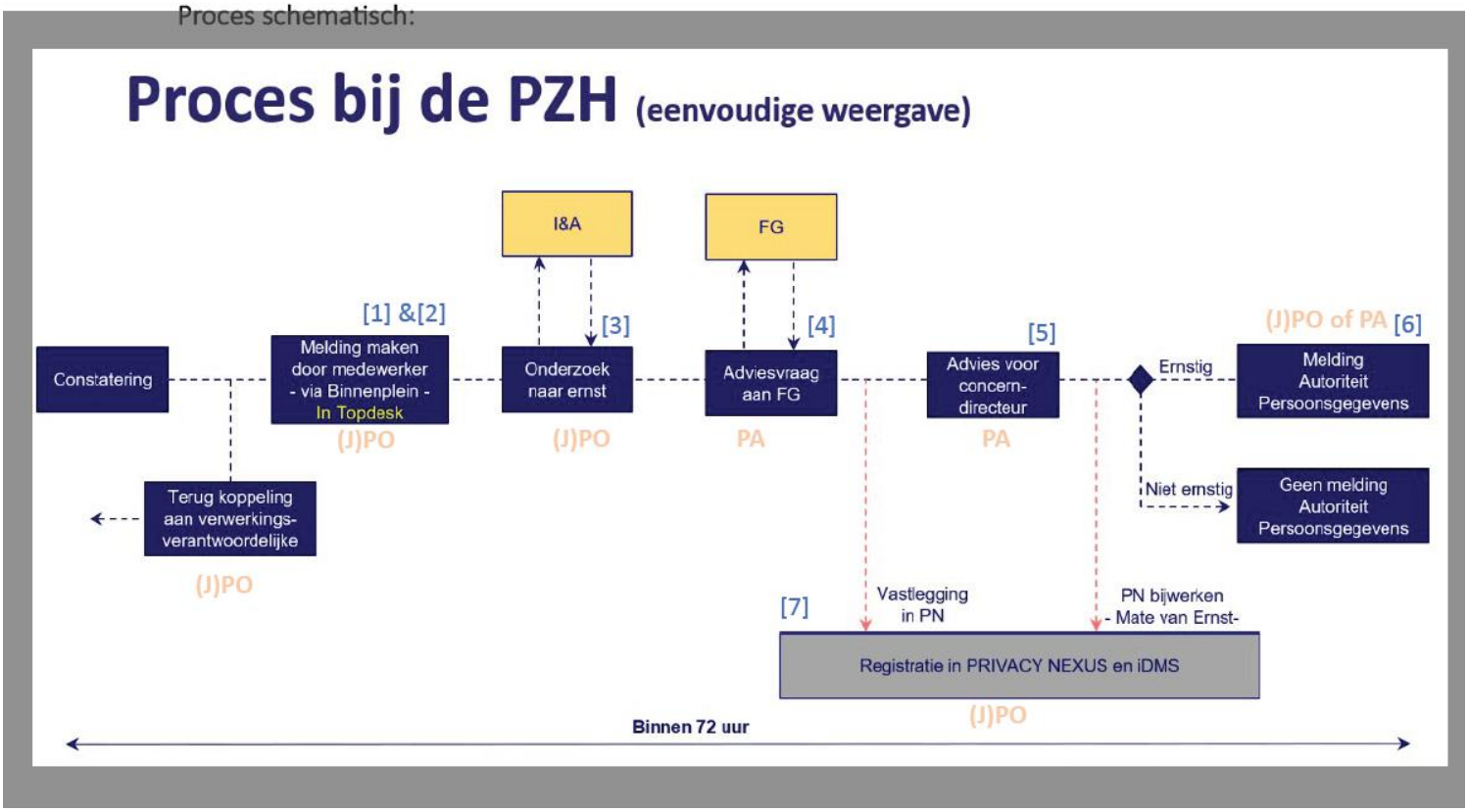
Artikel 33 zegt: Melding van een inbreuk in verband

- met persoonsgegevens aan de toezichthoudende autoriteit"
- Binnen 72 uur melden aan de AP
- De gene die het constateert informeert direct de verwerkingsverantwoordelijke
    - De aard van de inbreuk
    - Contactgegevens
    - De waarschijnlijke gevolgen van de inbreuk
    - De maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk aan te pakken

Stappen:

1. Via Binnenplein wordt een melding gedaan in
2. het TOPDESK meldingsformulier
3. Onderzoek naar ernst van het datalek.
4. Advies aanvraag bij FG. Deze bekijkt de ernst van de inbreuk op de Privacy en geeft een advies om deze wel of niet door te geven aan de Autoriteit Persoonsgegevens
5. Advies wordt kortgesloten met de Concerndirecteur
6. Indien ernstig, dan wordt er melding gedaan bij autoriteit Persoonsgegevens
7. T.b.v. de administratie en eventuele latere controles door AP, wordt alles in PN gezet.

Proces schematisch:



Rooster Datalekdienst: https://pzh.sharepoint.com/:x:/r/sites/teameenpri/Gedeelde%20documenten/General/Rooster%20Datalekken%202022%20en%202023%20-%20Eenheid%20Privacy.xlsx?d=we1f6e3c15254425199aa786e9e3a21dd&csf=1&web=1&e=TJcfao

* Zet je eigen week in je outlook agenda!

1 Melding

Meldingen worden gedaan in een speciaal formulier op Binnenplein. Indien dat niet is gebeurt dan de melden verzoeken om dit alsnog te doen.

Binnenplein pagina over datalekken: https://binnenplein.pzh.nl/loket/ict/datalek/

2 Melding Topdesk

Topdeskformulier over datalekken:
https://pvzh.topdesk.net/tas/public/ssp/content/serviceflow?unid=0523af60acfc4c509d4f4abf09f43e2a

Inloggen Topdesk
In Topdesk komen de meldingen binnen.
Direct naar Topdesk-formulieren: https://pvzh.topdesk.net/ => Inloggen als behandelaar

Onthoud het 'meldingsnummer' goed.
Ga naar tab-blad; bijlagen en sla 'oorspronkelijke aanvraag.pdf' op.
(bijvoorbeeld in de map Deze PC\Downloads)

3 Onderzoek van het datalek

iDMS-map
Maak een nieuwe map aan in de datalekken-map op iDMS (alleen binnen Citrix!!!!!!)
https://idms/otcs/llisapi.dll?func=ll&objId=646462858&objAction=browse&viewType=1

Maak een nieuwe map aan voor deze gebeurtenis (groen plusje , rechts boven

De mapnaam bevat eerst de datum van de gebeurtenis
Format: JJJJ-MM-DD -spatie- meldingsnummer -spatie- omschrijving
2023-02-29 M23 02 01568 - Phishing mail

Sla alle relevantie zaken over de melding op in deze map. (t.b.v. dossieropbouw voor WOO)

- Kopie oorspronkelijke Topdesk melding (uploaden uit Download-map)
- Contact met melders en betrokkenen
- Mailverkeer (ook reacties op je eigen mail)
- Geschreven adviezen (advies aan concerndirecteur)
- Voorlopige meldingen van AP (indien er een melding is gedaan bij de AP)
- etc, etc

4 Stel concept advies aanvraag op (P.O)

*** Kopieer een adviesrapport uit een vorige map en zet deze in deze map. Op deze manier heb je het format voor het adviesrapport. Bewerk data advies voor deze melding.

Houdt contact met Privacy Jurist en FG

5 Controle door Privacy jurist

Laat een P.J de melding controleren

6 Advies aanvragen FG

De privacy Jurist stemt het advies af met de FG

Daarna stuurt hij het afgestemde advies door aan de concerndirecteur en in c.c. de gedeputeerde.

Reactie van de concerndirecteur wordt opgenomen in de iDMS map

7 Registratie in Privacy Nexus:

Als alles klaar is en de melding is afgerond dan wordt de datalekmelding ook nog eens dubbel geregistreerd in Privacy Nexus.

Link: https://pzh.privacynexus.io/

Directe link: https://pzh.privacynexus.io/incident/browse

Maak een nieuwe datalekmelding aan: https://pzh.privacynexus.io/incident/create

Herhaal vele teksten uit het geschreven advies in de invoervelden.

Schrijf het incidentnummer ergens op. Die gebruik je bij de volgende stap in iDMS.

Bijwerken Excelbestand

Nog uitwerken

AUTORITEIT PERSOONSGEGEVENS

Meldloket

Ontvangstbevestiging

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

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

Tijdstip ontvangst
16-04-2021 09:49:15
Uniek nummer
art.5.1-2e

0. Over deze melding

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

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Naam van het bedrijf of de organisatie
Provincie Zuid-Holland

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

Wie meldt het datalek?

Naam
art.5.1-2e
Functie
Adviseur informatieveiligheid
E-mailadres
art.5.1-2e pzh.nl
Telefoonnummer
art.5.1-2e

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

De melder is contactpersoon
Ja

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?
Ja, namelijk:
Naam van de andere organisatie die betrokken was bij de inbreuk
Rijkswaterstaat
In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?
De provincie heeft een e-mail verstuurd aan RWS aangaande een situatie in de leefomgeving. In de e-mail staat ook informatie over het effect van die situatie op gezondheid en gemoedstoestand van betrokkene.

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend
13-04-2021
Startdatum van de periode waarbinnen de inbreuk was
12-04-2021
Einddatum van de periode waarbinnen de inbreuk was
13-04-2021
Duurt de inbreuk op dit moment nog voort?
Nee
Wanneer werd de inbreuk ontdekt?
13-04-2021

3. Gegevens over het datalek

3.1 Aard van de inbreuk

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

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?
Overig
Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest
Betrokkene (burger) heeft de provincie een e-mail gestuurd aangaande een situatie in de leefomgeving. In de e-mail staat ook informatie over het effect van die situatie op zijn gezondheid en gemoedstoestand. De provincie heeft vanuit haar werkrelatie met RWS de e-mail doorgezonden aan RWS met de bedoeling om dicht bij de bron tot een goed antwoord te komen en daarmee in het belang van betrokkene te handelen. Op grond van de AVG had deze e-mail, ondanks de goede bedoelingen, zonder expliciete toestemming van betrokkene niet doorgestuurd mogen worden.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

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

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt

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

4.3 Hoeveelheid persoonsgegevens

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

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

Werknemers
Nee
Klanten (huidig en potentieel)
Nee
Leerlingen of studenten
Nee
Patiënten
Nee
Minderjarigen
Nee
Personen uit kwetsbare groepen
Nee
Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
Burger
Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
1
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
1

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

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

Nee

7. Gevolgen van het datalek

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

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

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

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

Discriminatie
Nee
Identiteitsdiefstal of -fraude
Nee
Financiële verliezen
Nee
Reputatieschade
Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens
Nee
Ongeoorloofde ongedaanmaking van pseudonimisering
Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen
Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen
Nee
Andere gevolgen, namelijk:
Betrokkene heeft geen toestemming gegeven en maakt bezwaar tegen het doorsturen van de e-mail. De provincie heeft gehandeld vanuit de basis dat professioneel samengewerkt wordt met de organisatie RWS. De provincie heeft geen reden om aan te nemen dat RWS oneigenlijk gebruik zal maken van de ontvangen informatie.
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen
1. Verwaarloosbaar

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?
Ja
Wanneer heeft u het datalek gemeld aan de betrokkenen?
12-04-2021
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?
1
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?
e-mail

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
Betreffende provincieambtenaar is geïnformeerd over wat er op grond van de AVG mag worden doorgestuurd en onder welke voorwaarden.

8.3 Internationale aspecten

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

9. Overig

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

Print dit overzicht voor uw eigen administratie

-
-

Van: art.5.1-2e
Verzonden: 2023-09-28 14:41:04.979000+00:00
Aan: art.5.1-2e
CC:
Onderwerp: jaarverslag FG 2021
"

Met vriendelijke groet,

art.5.1-2e

People manager en AOG Informatietransitie, Bewustwording, Datagedreven werken (ai)

en Duurzaam Digitaal Informatiebeheer

Domein Informatisering & Automatisering

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

art.5.1-2e

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

Werkdagen: ma, di, do, vr

Krachtig Zuid-Holland

"


provincie
Zuid-Holland

Van: art.5.1-2e
Verzonden: 2022-11-28 11:04:13.890000+00:00
Aan: art.5.1-2e
CC:
Onderwerp: Fwd: DZH - 4b. 1 03062022 DEF Bijlage reactie op Jaarverslag 2021 van de functionaris voor gegevensbescherming.pdf
"
Reactie op jaarverslag FG vanuit is I&A, maar ook uit organisatie

Groeten art.5.1-2e

Van: art.5.1-2e art.5.1-2e gmail.com>
Verzonden: Monday, November 11:02:47 AM
Aan: art.5.1-2e < art.5.1-2e pzh.nl>
Onderwerp: DZH - 4b. 1 03062022 DEF Bijlage reactie op Jaarverslag 2021 van de functionaris voor gegevensbescherming.pdf

Groeten art.5.1-2e

Bijlage 'Reactie op bevindingen Jaarverslag 2021 van de Functionaris voor Gegevensbescherming'

Thema	Door FG gesignaleerd risico	Door FG gegeven advies	Reactie
Organisatie	Capaciteit en kennis privacy officers afdelingen. Pag. 11.	Eenheid Privacy: personele bezetting invullen; aandacht voor plaats eenheid binnen organisatie.	Inmiddels heeft de werving plaatsgevonden en zijn er mensen aangenomen voor de Eenheid Privacy. De Eenheid Privacy is op 23 mei 2022 gestart.
	Positie FG Pag. 11.	Onafhankelijkheid FG waarborgen; niet binnen een afdeling maar naast of boven de organisatie.	De FG werkt provincie breed en is daarom bewust bij de afdeling Bestuur gepositioneerd. De feitelijke aansturing vindt plaats door de concerndirecteur/loco-provinciesecretaris waarmee de FG als zodanig zich 'boven' de organisatie beweegt.
Thuiswerken	Gebruikers kunnen zelf applicatie (zonder invloed I&A) op laptops/telefoons installeren. Pag. 11.	Beleid maken wat wel/niet geïnstalleerd mag worden.	Onderdeel van de opgave digitale werkplek is beleid ten aanzien van de installatie van applicaties door gebruikers. In 2022 vindt uitgifte van nieuwe telefoons plaats. Hierbij wordt dit advies opgepakt.
	Organisatie maakt (te veel) gebruik van schaduw IT. Pag. 11.	Beleid maken om gebruik schaduw IT in te perken.	De afdeling Informatisering en Automatisering maakt gebruik van Cybersprint om onze digitale assets te detecteren om daarmee voor een deel shadow-IT te beperken. De effectiviteit hiervan wordt in 2022 bezien. Vanuit het ISO27001 implementatietraject zal naar samenwerking gezocht worden met de opgave digitale werkplek, ter realisatie van een passend beleid ten aanzien van schaduw-IT. Daarbij zal rekening worden gehouden met de vast te stellen visie op Bring Your Own Device (BYOD). Op hoofdlijnen zullen de uitgangspunten uitgewerkt worden in het te actualiseren informatiebeveiligingsbeleid, wat evenals onderdeel is van de ISO27001 implementatie.
Maatschappelijke ontwikkelingen	Zorgen over zakelijk gebruik Whatsapp binnen provincie door zowel bestuurders als medewerkers. Pag. 12.	FG zal in 2022 adviseren over gebruik Whatsapp en social media kanalen binnen de provincie.	Vanuit de afdeling communicatie zullen we hierin nauw optrekken met de FG.
	Maatschappelijke onrust over gebruik algoritmen bij de (provinciale) overheid. Pag. 12.	Binnen provincie wordt gesproken over het opstellen van een algoritmeregister. FG voert toezicht uit op zo'n algoritmeregister, in afwachting van wettelijke verplichting.	De afdeling Bestuur is de afgelopen 1,5 jaar betrokken geweest bij het landelijke consortium 'Publieke controle op algoritmes'. Vanuit daar is een standaard ontwikkeld voor het vastleggen van de algoritmes die een overheidsorganisatie gebruikt. Een eerste inventarisatie van algoritmes binnen Zuid-Holland is tevens gemaakt. Verkend wordt hoe eigenaarschap belegd kan worden en wat ervoor nodig is in 2022 een eerste set algoritmes volgens de standaard te publiceren.
Privacy beleid	Er is geen beleid op verwerking persoonsgegevens. AVG vereist beleid. Pag. 12.	Opstellen, formeel vaststellen en bekendmaken van beleid voor bescherming persoonsgegevens.	Er is beleid ten aanzien van gegevens van het personeel, maar de FG wijst erop dat er aanvullend behoefte is aan beleid ten aanzien van persoonsgegevens (inwoners, relaties etc.). Daar gaat de nieuwe Eenheid Privacy mee aan de slag.

Bijlage 'Reactie op bevindingen Jaarverslag 2021 van de Functionaris voor Gegevensbescherming'

Gegevens-minimalisatie en iDMS	PZH voldoet niet aan beginselen van gegevensminimalisatie, opslagbeperking en integriteit en vertrouwelijkheid, vooral niet bij document management systeem (iDMS) Pag. 12.	PZH blijft AVG schenden totdat er een nieuw en/of sterk verbeterd DMS is, met alle risico's op sancties door de AP.	In het jaarverslag wordt de schending van de AVG gekoppeld aan de kwaliteit van het iDMS. Er wordt niet ingegaan op de feitelijke tekortkomingen en de te nemen maatregelen om tot verbeteringen te komen. De stelling dat de aanschaf van een nieuw DMS, de risico's op sancties door de Autoriteit Persoonsgegevens verminderd of wegneemt, wordt niet onderbouwd. Onderzoek van Gartner om te komen tot een visie op het informatiebeheer heeft uitgewezen dat de geconstateerde tekortkomingen een relatie hebben met de organisatiecultuur en de wijze waarop medewerkers met informatie omgaan. Daarnaast is er een historie van gegevens die moeten worden opgeschoond. Het opschonen van deze gegevens valt binnen de scope van het project "Stukken Beter Bewaard" (SBB) spoor 1. Binnen dit project zal ook aandacht zijn voor bewustwording over de omgang met informatie door medewerkers. Steeds vaker vindt dossiervorming plaats buiten het iDMS. De dossiervorming voor bijvoorbeeld het proces Vergunningverlening Digitaal Stelsel Omgevingswet (DSO) zal gaan plaatsvinden in een andere 'oplossing' dan het iDMS. Tijdens het aanbestedingstraject zijn in het programma van eisen de criteria van recordmanagement (Duto-eisen), informatieveiligheid (Beschikbaarheid, integriteit, vertrouwelijkheid) en architectuur benoemd om te komen tot een gewenste inrichting. Vanwege de complexiteit van het onderwerp is de FG persoonlijk vanaf het beginstadium bij dit traject betrokken.
Werkdruk en positie FG	Door de toename van de hoeveelheid verwerkingen en risicoanalyses die de FG moet behandelen loopt de verwerkingstijd behoorlijk op en daarmee ook de 'wachttijd' voor de indieners. Dat vormt een groot risico op afbreuk aan motivatie om op een goede manier met PIA's om te gaan. Pag. 13.	--	De nieuwe Eenheid Privacy zal bijdragen aan de verlichting van de werkdruk bij de FG.
Regelgeving binnen de provincie	Een deel van de medewerkers werkt niet volgens de vereisten van de AVG. De risico's om de AVG niet na te leven, of de adviezen van de FG niet in te winnen of na te leven, laten zich raden. Pag. 13.	Voorkom het omzeilen van verplichtingen uit de AVG.	De verantwoordelijkheid om compliant te zijn met (privacy)regelgeving ligt primair bij de proceseigenaren. De nieuwe eenheid gaat zich ervoor inzetten om hen hierbij te ondersteunen (juridisch advies, opstellen/beoordelen verwerkersovereenkomsten, hulp bij uitvoeren Data Protection Impact Assessments (DPIA) etc.).

Bijlage 'Reactie op bevindingen Jaarverslag 2021 van de Functionaris voor Gegevensbescherming'

Datagedreven werken en big data	Datagedreven werken kan de efficiency en de kwaliteit van besluiten verhogen. De provincie moet daarbij echter wel ruimschoots aandacht hebben voor privacy. Aandacht voor bewust (ethische) afwegingen m.b.t. wenselijkheid van het op grootschalige schaal verwerken van persoonsgegevens. Pag. 14.	1.Uitvoeren verenigbaarheidstoets (is het doel waarvoor de gegevens worden verwerkt verenigbaar met het doel waarvoor ze oorspronkelijk zijn verzameld?) 2.Privacy Impact Assessment (PIA) uitvoeren 3.Ethische Impact Analyse (al dan niet i.c.m. PIA)	1.Dit is onderdeel van de PIA die door informatiebeveiliging wordt uitgevoerd bij nieuwe trajecten. Dit valt onder het informatiemanagementproces. 2. en 3. Wordt zoals benoemd uitgevoerd door informatiebeveiliging. Alle nieuwe trajecten doorlopen het informatiemanagementproces, via dit proces is ook informatiebeveiliging altijd betrokken en wordt waar nodig een PIA uitgevoerd. In de komende periode wordt bezien hoe we ethische afwegingen bewuster een plek kunnen geven.
Bewustwording	De provincie verzamelt op grote schaal persoonsgegevens, weliswaar op minder grote schaal dan bijvoorbeeld gemeenten, maar daarin schuilt juist weer een risico. Te vaak werd niet voldoende of helemaal geen gevolg gegeven aan adviezen van de FG. Pag. 15.	De provincie moet nog de nodige stappen zetten om het bewustzijn van privacyregelgeving onder bestuurders, management en medewerkers te vergroten.	De interne bewustwordingscampagne Up-to-Data over datagovernance loopt sinds begin 2019 en behandelt de onderwerpen informatiebeheer, datakwaliteit, informatieveiligheid, integriteit en privacy door alle medewerkers te informeren, verrassen en af en toe shockeren. Een belangrijk onderdeel van de campagne is het bewustzijn van alle medewerkers te vergroten over de wijze waarop zij met informatie omgaan. Door EAA is onderzocht hoe medewerkers van de Provincie Zuid-Holland omgaan met hun informatie. Conclusie: Bewustzijn bij de omgang met informatie is aanwezig. De bekendheid met de Campagne Up-to-Data is wisselend: sommige activiteiten uit de campagne zijn redelijk goed bekend bij de respondenten en anderen zijn minder opgevallen. Recente initiatieven zijn het meest bekend. Bewustzijn van provinciale medewerkers met betrekking tot privacy, informatiekwaliteit/-integriteit, informatieveiligheid, informatiebeheer en archivering is aanwezig, maar moet wel verbeterd worden. Met de aanbevelingen uit het rapport in het bijzonder met betrekking tot privacy gaat de nieuwe Eenheid Privacy aan de slag. Het gaat dan bijvoorbeeld om trainingen, webinars en opleidingen.
Wet politiegegevens	Uit de interne audit komen enkele zaken naar voren die niet in orde zijn en dus actie vereisen. Een van die zaken is de verwerking in iDMS. Een andere is dat de FG onvoldoende toezicht houdt. Pag. 16	De FG is het eens met bevindingen uit de interne rapportage.	Afdeling Dienst Beheer Infrastructuur (DBI) werkt samen met de FG aan het oppakken van de aanbevelingen. Mede als gevolg van de beperkingen van iDMS wordt, samen met de afdeling Informatisering & Automatisering, een aansluiting op een BOA registratiesysteem gerealiseerd. Daarnaast vindt overleg plaats met de FG over de gevolgen voor de BOA taken van DBI waarbij de aanbevelingen centraal staan.

Van: art.5.1-2e
Verzonden: 2022-11-28 11:27:11.688000+00:00
Aan: art.5.1-2e
CC:
Onderwerp: Fwd: DZH - 4b. 0 Jaarverslag FG 2021.pdf
"
Nu met dan

Groeten art.5.1-2e

Van: art.5.1-2e <art.5.1-2egmail.com>
Verzonden: Monday, November 28, 2022 11:03:07 AM
Aan: art.5.1-2e <art.5.1-2epzh.nl>
Onderwerp: DZH - 4b. 0 Jaarverslag FG 2021.pdf

Groeten art.5.1-2e

provincie
Zuid-Holland

JAARVERSLAG 2021

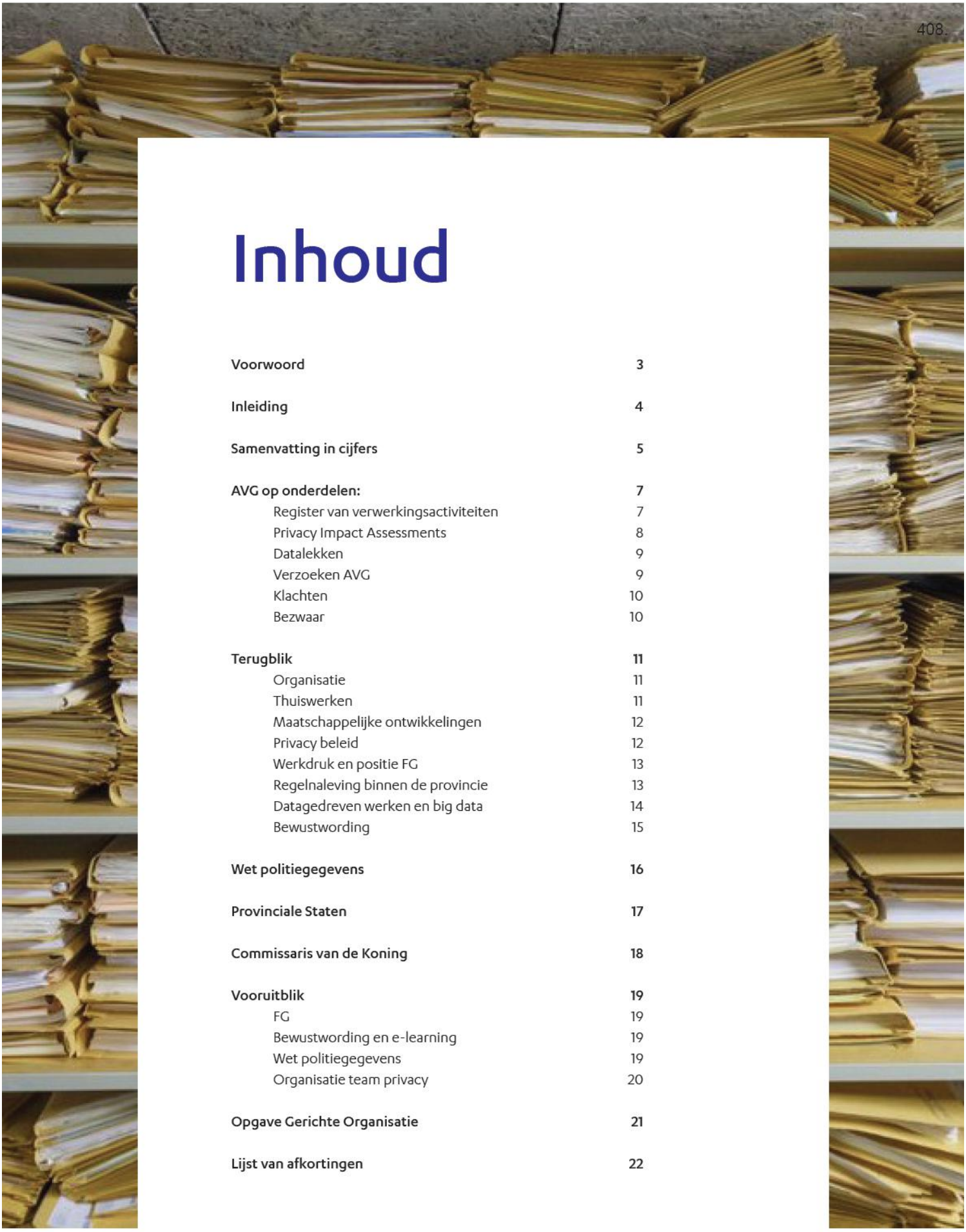
Van de Functionaris voor Gegevensbescherming

art.5.1-2e

Functionaris voor Gegevensbescherming
Provincie Zuid-Holland

februari 2022

Elke dag beter. Zuid-Holland.



Inhoud

Voorwoord

De overheid kan haar taken niet uitvoeren zonder persoonsgegevens te verwerken.
Dat geldt zeker ook voor provincies. Provincies verwerken vaak meer persoonsgegevens dan de meeste ambtenaren zich bewust zijn. Niet alleen persoonlijke informatie over de eigen inwoners, maar ook over andere burgers, medewerkers en relaties. De Algemene Verordening Gegevensbescherming (AVG) biedt waarborgen voor het beschermen van deze gegevens.
Dit is belangrijk omdat de gevolgen van onjuist en onzorgvuldig gebruik van persoonsgegevens grote gevolgen kunnen hebben voor mensen. Ook draagt het aantoonbaar voldoen aan de AVG in belangrijke mate bij aan een betrouwbare overheid.

De Functionaris Gegevensbescherming (FG) van de provincie Zuid-Holland (hierna: de provincie) informeert en adviseert de organisatie over de uitvoering van de AVG. De FG heeft echter vooral een toezichthoudende rol. Dit houdt in dat de FG erop toe ziet dat de provincie voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens.

De FG rapporteert rechtstreeks aan het college van Gedeputeerde Staten, als het gaat om de verwerkingen van persoonsgegevens die onder verantwoordelijkheid van het college vallen.
De FG brengt het college dus op de hoogte over de stand van zaken van privacy.
Deze rapportage bevat de bevindingen over het jaar 2021.

De FG is tevens verantwoordelijk voor het toezicht op de twee andere bestuursorganen binnen de provincie: Provinciale Staten en de Commissaris van de Koning. Deze rapportage doet ook hierover verslag.

De provincie heeft ook een FG op grond van de Wet politiegegevens, deze ziet toe op de verwerking van persoonsgegevens door de buitengewoon opsporingsambtenaren (BOA's) van de provincie bij hun handhavingstaken. In deze rapportage gaat een hoofdstuk in op de verwerkingsactiviteiten van BOA's.

Inleiding

De uitvoering van de AVG heeft een blijvende grote invloed op bijna alle processen van de provincie. In 2021 heeft de organisatie de vanaf 2018 neergelegde basis verder uitgebouwd. De AVG is echter een omvangrijke en gecompliceerde wet, die om structurele inzet blijft vragen van bestuur, management en medewerkers.

De praktijk laat zien dat er de afgelopen jaren flink is aangepakt, maar ook dat er nog veel ruimte voor verbetering is. Het vraagt om een gedegen planning en een goed ingerichte continue verbeteringscyclus. Daarnaast is het cruciaal dat er voldoende capaciteit beschikbaar is om alle AVG-verplichtingen ook daadwerkelijk te kunnen uitvoeren.

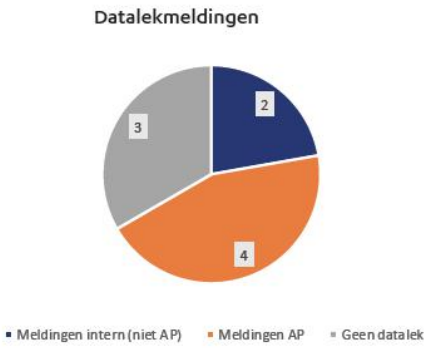
Dat laatste blijkt in de praktijk lastig, waardoor processen in de tijd uitlopen. Dit gaat bijvoorbeeld om het up-to-date houden van het verwerkingsregister van persoonsgegevens, tijdig melden en registeren van datalekken, maar ook om het op tijd uitvoeren (en afronden) van PIA's. Zeker in deze tijd waarin we vooral thuis werken, is het werken aan een hoger niveau van bewustzijn voor bescherming van persoonsgegevens ook een uitdaging.

Deze rapportage geeft de stand van zaken van de naleving van de AVG. Het rapport begint met een cijfermatige samenvatting en toelichting daarop, waaruit blijkt hoe de organisatie er voor staat op gebied van de AVG. Het daarop volgende hoofdstuk gaat in op een aantal knelpunten binnen de provincie in 2021. De rapportage sluit af met een korte vooruitblik op 2022.

Samenvatting in cijfers

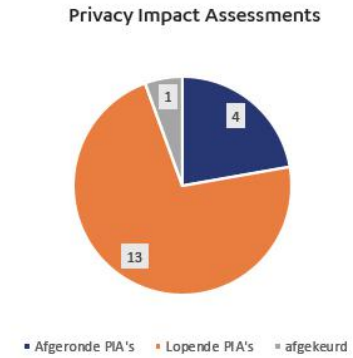
Verwerkingsregister

complete verwerkingen	72
incomplete verwerkingen	122



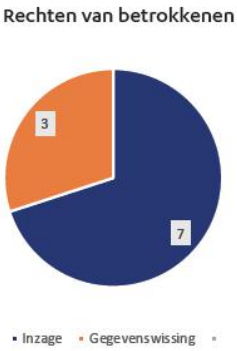
Datalekmeldingen

Meldingen intern (niet AP)	2
Meldingen AP	4
Geen datalek	3



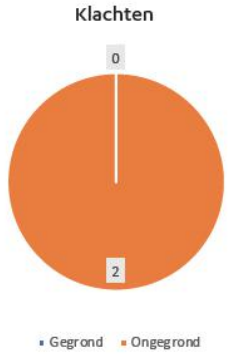
PIA's

Afgeronde PIA's	4
Lopende PIA's	13
afgekeurd	1



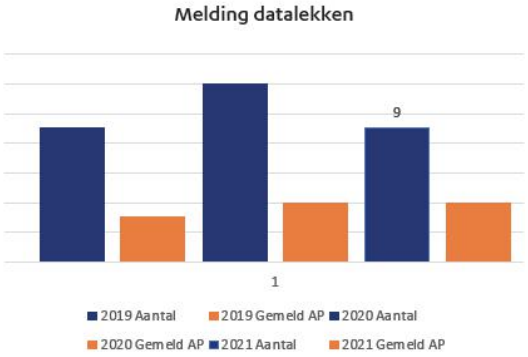
Rechten van betrokkenen

Inzage	7
Gegevenswissing	3



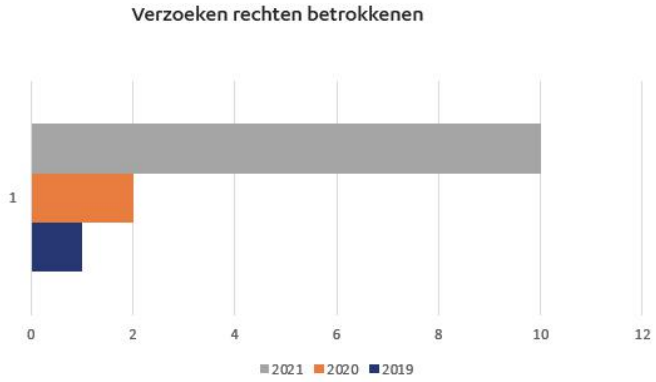
Klachten

Gegrond	0
Ongegrond	2



Ontwikkeling melding datalekken

2019	Aantal	9
	Gemeld AP	3
2020	Aantal	12
	Gemeld AP	4
2021	Aantal	9
	Gemeld AP	4



Ontwikkeling verzoeken rechten van betrokkenen

2019	1
2020	2
2021	10

AVG op onderdelen:

Register van verwerkingsactiviteiten

Een van de instrumenten die de AVG aanreikt om als organisatie te kunnen aantonen op welke wijze zij omgaat met persoonsgegevens (in overeenstemming met de vereisten van de AVG) is het register van verwerkingsactiviteiten, kortweg het verwerkingsregister. Dit verwerkingsregister is een belangrijke basis voor andere thema's die vanuit de AVG moeten worden opgepakt. Denk daarbij onder andere aan de uitoefening van de rechten van betrokkenen.

Voordat de AVG op 25 mei 2018 in werking trad, had de provincie een verwerkingsregister in de vorm van een Excel-bestand waarin verwerkingen waren opgenomen. Dit bestand was echter niet compleet, want zowel kwalitatief als kwantitatief was het geen goede afspiegeling van alle processen waarin de provincie persoonsgegevens verwerkt. Daarnaast bleek dat het up-to-date houden in deze vorm niet mogelijk was. De provincie schafte daarom eind 2020 een nieuwe tool aan en startte begin 2021 een project waarbij alle afdelingen zelf hun verwerkingen in kaart brengen en in het nieuwe verwerkingsregister plaatsen, ondersteund door externe expertise. Het verwerkingsregister is onderdeel van een nieuwe tool met een ingebouwde alarmerings-systematiek, die afdelingen jaarlijks attendeert op het controleren van hun gegevens.

De meeste afdelingen hebben eind 2021 een groot deel van hun verwerkingen in het nieuwe register gezet. Begin 2022 plaatsen vier afdelingen hun verwerkingen nog in het register. Naar verwachting komt het totaal aantal verwerkingen dan rond de 240 uit. Dit aantal is in lijn met andere provincies.

Eind 2021 waren in totaal 183 verwerkingen opgenomen in het register. Elke opgenomen verwerking krijgt nog enkele controles, 42 verwerkingen zijn volledig goedgekeurd. Al die afdelingen verdienen een compliment voor hun inzet voor het vullen van het register en de mate waarin zij de formulieren compleet invulden.

De invoering van het nieuwe systeem en de betrokkenheid van de afdelingen vergroten het bewustzijn dat dit niet een eenmalige gebeurtenis is, maar een continu proces. Nieuwe verwerkingen en systemen moeten altijd een plaats krijgen in het register, dit moet een vast onderdeel worden van alle bedrijfsprocessen waarbij de provincie persoonsgegevens verwerkt.

In het kader van transparantie en 'accountability', kan het college van Gedeputeerde Staten (GS), overwegen om het register in beperkte vorm openbaar te maken op de corporate website van de provincie.

Privacy Impact Assessments

“Onder de Algemene verordening gegevensbescherming (AVG), de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) kunnen organisaties verplicht zijn een data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico’s van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico’s te verkleinen” (Autoriteit Persoonsgegevens).

De provincie gebruikt nog de oude benaming Privacy Impact Assessment (PIA) voor een data protection impact assessment (in goed Nederlands een gegevensbeschermingseffectbeoordeling). De wetgever heeft een ondergrens aangegeven voor verwerkingen waarbij een PIA verplicht is. Om een betrouwbare overheid te zijn, zouden overheidsorganisaties (dus ook de provincie) niet strikt die ondergrens moeten aanhouden, maar daar wat ruimer op in steken. Naast het imago heeft dit nog andere voordelen. Zo kan de provincie voor transparantie beter inzicht geven in de verwerking en wordt de organisatie zich bewuster van de processen waarin persoonsgegevens in het spel zijn en kan zij ook scherper kijken naar een van de uitgangspunten van de AVG, namelijk privacy-by-design.

In 2021 werden bij de provincie in totaal 18 PIA’s uitgevoerd. De FG rondde vier daarvan met een positief advies af. Eén PIA kreeg een negatief advies, waarna het contract met de leverancier is opgezegd. De overige PIA’s zijn of nog in behandeling, of zijn stilgelegd. De FG heeft hierop meestal geen zicht. Niet iedere afdeling meldt een statusverandering bij het opstellen van een PIA. Het is gewenst dat de verantwoordelijken voor de PIA dit in de nabije toekomst oppakken.

Volgens de AVG moet de provincie een PIA uitvoeren vóórdat de verwerking start. Dit is bij de provincie niet altijd het geval, hier is dus nog veel ruimte voor verbetering. Daarnaast heeft de Autoriteit Persoonsgegevens (AP) aangegeven dat verwerkingen die al bestonden voor het in werking treden van de AVG binnen drie jaar een PIA moeten krijgen. Hier ligt voor de provincie nog een opgave. GS hebben bepaald dat voor iedere verwerking waarvoor de provincie een PIA uitvoert een dwingend advies van de FG is vereist. Zonder positief advies van de FG mag de provincie de verwerking niet uitvoeren. Ook in het afgelopen jaar bleek de organisatie hier wel weer eens moeite mee te hebben.

De Autoriteit Persoonsgegevens adviseert, vooral de overheid, om een samenvatting van iedere uitgevoerde PIA te publiceren. Dit maakt het ook hier mogelijk om aan meer vertrouwen in de gegevensverwerking door de overheid te werken. De provincie heeft hierin nog geen standpunt ingenomen.

Datalekken

Eén van de maatregelen om aan de verantwoordingsplicht te voldoen is het verplichte vastleggen van alle inbreuken op persoonsgegevens, ofwel het bijhouden van een datalekregister. Het doel van dit verplichte vastleggen is te stimuleren dat organisaties leren van eerdere inbreuken en maatregelen nemen om de kans op nieuwe inbreuken te verminderen. Dit biedt daarnaast handvatten om binnen de organisatie het gesprek aan te gaan over AVG-bewustzijn. Ook kan de AP als toezichthoudende autoriteit via de vastgelegde gegevens controleren of organisaties de meldplicht voor datalekken naleven.

In 2021 zijn er bij de provincie negen datalekken geregistreerd. Daarnaast waren er drie meldingen die na onderzoek geen datalek bleken te zijn. Van de negen geregistreerde datalekken zijn er vier gemeld bij de Autoriteit Persoonsgegevens. Acht onderzoeken zijn in 2021 afgerond, één onderzoek loopt nog door in 2022. Zes van de datalekken hebben geleid tot het onbedoeld openbaar maken van persoonsgegevens, als gevolg van een technische onvolkomenheid of als gevolg van menselijk handelen.

Het totaal van negen datalekken betekent een lichte afname van het aantal ten opzichte van eerdere jaren. Dit gaat in tegen de trend die de AP constateert. Opvallend is dat het aantal datalekken voor een organisatie als de provincie erg laag is. Mogelijk worden datalekken niet herkend, of niet (intern) gemeld. De provincie zou zich daarom de komende jaren moeten in zetten om het bewustzijn van de medewerkers over datalekken te verhogen en eventuele hindernissen voor het melden daarvan wegnemen.

Verzoeken AVG

De AVG kent aan betrokkenen een aantal rechten toe. Dit zijn vooral recht op inzage, rectificatie en wissen van persoonsgegevens. Volgens de termijn van de AVG heeft de verwerkingsverantwoordelijke (de provincie) één maand voor de afhandeling van een verzoek en in complexe gevallen verlenging van 2 maanden. De provincie heeft alle verzoeken van het afgelopen jaar binnen de gestelde termijn afgehandeld.

Dergelijke verzoeken afhandelen betekent wel een grote aanslag op vooral de personele- en IT-middelen van de organisatie. Bovendien wordt de aanpak van de behandeling van meldingen in vele gevallen ad-hoc bepaald. Een meer gestandaardiseerd proces voor het doorzoeken van de systemen zou beter zijn. Als het verwerkingsregister volledig op orde is, draagt dit ook bij aan een snellere en vooral betere afhandeling van verzoeken. Bovendien is het eigenaarschap van de gegevens en de systemen dan ook geen vraagstuk meer, terwijl het dat nu regelmatig wel is. Wie verantwoordelijk is voor de verschillende processen staat namelijk in het verwerkingsregister opgenomen.

Op meerdere terreinen van het informatiebeheer bij de provincie ontbreekt nog veel (vastgesteld) beleid. Dat komt de betrouwbaarheid van de organisatie, ook naar de betrokkenen toe, niet ten goede. Daardoor kan de provincie bepaalde keuzes voor een verzoek niet uitleggen aan betrokkenen omdat zij niet kan verwijzen of terugvallen op vastgestelde beleidsregels.
In 2021 zijn er 10 verzoeken geweest op grond van de AVG. Zeven verzoeken hadden betrekking op artikel 15 AVG, 'Recht van inzage van de betrokkene'. Drie verzoeken hadden betrekking op artikel 17 AVG, 'Recht op gegevenswissing'.

Klachten

Er zijn in 2021 twee klachten binnengekomen over het handelen van de provincie in het licht van de AVG. Eén klacht had betrekking op mogelijke zorgen over een datalek dat de provincie veroorzaakt zou hebben waarbij de persoonsgegevens van de klager waren betrokken.
De andere klacht ging over dat de provincie niet naleeft wat zij zegt over persoonsgegevens in haar eigen privacyverklaring. Beide klachten bleken ongegrond.

Bezwaar

Er zijn in 2021 geen bezwaarschriften ingediend inzake de AVG.

Terugblik

Organisatie

Toen de AVG inging, stelde de provincie een functionaris voor gegevensbescherming aan. Eind 2018 zijn er op verschillende afdelingen privacy officers benoemd die als een soort ambassadeurs de afdelingen moesten ondersteunen bij het naleven van de AVG. Omdat dit een rol was die de privacy officers naast hun reguliere werkzaamheden deden, bleek dit voor hen een te grote belasting te zijn. Daarnaast bleek het lastig om de kennis van zoveel medewerkers op een toereikend niveau te krijgen.

In 2021 bleek dat om aan de verplichtingen vanuit de AVG te kunnen voldoen, dit meer inzet vergt vanuit de organisatie. De functionaris voor gegevensbescherming heeft hier aandacht voor gevraagd. De provincie besloot daarom een Eenheid Privacy in te richten, die bestaat uit een aantal centrale privacy officers, een privacy jurist en een ondersteuner. Zij kunnen zich volledig richten op het optimaliseren van de bescherming bij het verwerken van persoonsgegevens binnen de provincie. De bedoeling is om in 2022 de personele bezetting van deze Eenheid Privacy in te vullen. Aandachtspunt is de plaats van de eenheid binnen de organisatie.

Om de onafhankelijkheid van de FG te waarborgen zou de positie van de FG niet binnen een afdeling, maar naast of boven de organisatie moeten zijn. De FG legt immers verantwoording af aan de drie bestuursorganen en niet aan de lijn.

Thuiswerken

In 2021 werd duidelijk dat de maatregelen door de corona pandemie een blijvende impact hebben op de provincie. Volgens de werkgemeenschap van de toekomst krijgt thuiswerken een blijvende plek. Dit heeft ook gevolgen voor hoe de provincie met persoonsgegevens omgaat en dit brengt ook weer andere risico's mee. De provincie bleek niet altijd in staat om soepel en adequaat de nodige maatregelen te treffen, ondanks inspanningen van medewerkers en de FG om bepaalde risico's te mijden. Een voorbeeld: medewerkers die persoonsgegevens op papier moeten vastleggen voor een bepaalde periode, kregen geen papiervernietigers omdat procedures binnen de provincie dit niet toelieten. Deze medewerkers moesten vervolgens zelf en uit eigen middelen de papiervernietigers aanschaffen.

De FG maakt zich zorgen over de laptops en telefoons van de provincie waar gebruikers zelf applicaties op kunnen installeren zonder dat de afdeling I&A invloed heeft op de veiligheid. Er is ook hier geen vastgesteld beleid over wat wel en niet geïnstalleerd mag worden en dat brengt de nodige (en mogelijk grote) risico's met zich mee.

Ditzelfde geldt overigens ook voor de organisatie zelf. De provincie maakt (teveel) gebruik van schaduw-IT zonder dat de afdeling I&A of de FG hier zicht op hebben. Daarmee loopt de provincie risico's voor de bescherming van persoonsgegevens. Het verwerkingsregister biedt hier kansen op meer inzicht als de afdelingen al hun verwerkingen en systemen in het register plaatsen. De provincie zou beleid moeten maken om het gebruik van schaduw-IT in te perken.

Maatschappelijke ontwikkelingen

Al jarenlang domineren vijf grote IT-bedrijven de digitale (online) wereld: Meta (het moederbedrijf van o.a. Facebook, Whatsapp en Instagram), Alphabet (moederbedrijf van o.a. Google, YouTube en Android), Amazon, Apple en Microsoft. Veel van deze bedrijven slaan (een deel van de) gegevens van gebruikers op in de Verenigde Staten, maar dit gebeurt niet altijd volgens de vereisten van de AVG. Daar worden in Europees verband dan ook al enkele jaren verschillende rechtszaken over gevoerd. In 2020 kwam daar een uitspraak van het Hof van Justitie van Europa bij, het zogenoemde Schrems II-arrest. Dit arrest maakt nogmaals duidelijk dat een bedrijf in de Verenigde Staten persoonsgegevens bij hoge uitzondering binnen de kaders van de AVG kan verwerken. Vervolgens is de klacht over het gebruik van Google Analytics bij alle nationale Europese toezichthouders neergelegd. Enkele nationale toezichthouders verbieden het gebruik van deze applicatie al en ook de AP heeft gewaarschuwd dat het gebruik in Nederland mogelijk in strijd is met de AVG. Er zijn ook ernstige zorgen over het gebruik van Whatsapp, dat ook binnen de provincie zowel door bestuurders als door medewerkers steeds vaker zakelijk gebruikt wordt. In 2022 zal de FG adviseren over het gebruik van Whatsapp en social media kanalen binnen de provincie.

In de afgelopen jaren ontstond ook veel maatschappelijke onrust over het gebruik van algoritmen bij de overheid. Onduidelijkheid over het gebruik van algoritmen en de invloed daarvan op burgers schaadt het vertrouwen van die burger in de overheid. Naast de Rijksoverheid gebruiken gemeenten en provincies ook algoritmen. De provincie moet dan ook zo snel mogelijk duidelijk in kaart brengen welke algoritmen zij gebruikt, daar een register van aanleggen, volgens het register van verwerkingsactiviteiten, waarin duidelijk het doel, de grondslag en de methodiek staan. Binnen de provincie spreken ze nu over het opstellen van zo'n register.
Het ligt voor de hand dat de FG van de provincie het toezicht uitvoert op zo'n algoritmeregister in afwachting van een wettelijke verplichting.

Privacy beleid

In het jaarverslag over 2019 stond al dat de provincie geen beleid heeft op de verwerking van persoonsgegevens. De AVG eist wel zo'n beleid en door het gebrek daaraan kan de AP een boete opleggen. Daarnaast draagt een vastgesteld privacybeleid er ook aan bij dat burgers vertrouwen hebben in de verwerking van hun gegevens door de overheid. Bovendien is het een belangrijk middel om besluiten te onderbouwen bij verzoeken op grond van de AVG.

Bovenstaande vraagt dringend om een formeel vastgesteld en bekend gemaakt beleid voor de bescherming van persoonsgegevens. En niet alleen om algemeen beleid, maar om beleid op meerdere terreinen van informatieverwerking en -beveiliging. Hoewel de opdracht voor een beleidsverkenning onderweg is, neemt dit de zorg van een lang en stroperig proces nog niet weg.

Gegevensminimalisatie en iDMS

De AVG kent meerdere uitgangspunten voor de verwerking van persoonsgegevens. Drie daarvan zijn het beginsel van gegevensminimalisatie, het beginsel van opslagbeperking en het beginsel van integriteit en vertrouwelijkheid.

Gegevensminimalisatie betekent dat de provincie niet meer gegevens mag verwerken dan strikt noodzakelijk is voor het vastgestelde doel. Opslagbeperking wil zeggen dat de provincie gegevens niet langer mag bewaren of verder verwerken dan noodzakelijk is voor het vastgestelde doel.
Het beginsel van integriteit en vertrouwelijkheid omvat onder meer het uitgangspunt dat niet meer mensen de gegevens mogen verwerken dan strikt noodzakelijk is voor hun functie, dit houdt ook in dat zij alleen die gegevens mogen inzien die strikt noodzakelijk zijn om hun functie uit te oefenen.

De provincie voldoet niet altijd aan deze beginselen, vooral niet bij haar document management systeem (iDMS). De FG wees hier al op in het jaarverslag over 2019. Ondanks dat de organisatie het systeem verbeterde, blijft duidelijk dat het systeem niet is ingericht op een adequate naleving van de AVG. Daarnaast weten medewerkers vaak niet goed hoe ze persoonsgegevens in het iDMS moeten verwerken, waardoor gevoelige en soms ook bijzondere persoonsgegevens in strijd met de AVG worden verwerkt. In 2021 kwam de afdeling I&A met een nieuwe visie op het informatiebeheer binnen de provincie, waarin ook het document management systeem een plaats heeft. De provincie blijft de AVG schenden totdat er een nieuw en/of sterk verbeterd DMS is, met alle risico's op sancties door de AP.

Werkdruk en positie FG

In 2021 is er hard gewerkt om het verwerkingsregister te vullen op basis van de processen waarbij de provincie persoonsgegevens verwerkt. Dat leidt natuurlijk ook tot meer PIA's, en dat is een goede ontwikkeling. Door de hoeveelheid verwerkingen en risicoanalyses die de FG moet controleren en hopelijk goedkeuren, loopt de verwerkingstijd behoorlijk op en daarmee ook de 'wachttijd' voor de indieners. Dat vormt een groot risico op afbreuk aan motivatie om op een goede manier met PIA's om te gaan. Dit zou zonde zijn want er is de laatste twee jaar veel effort in de organisatie gestoken om dit goed te doen.

Regelnaleving binnen de provincie

Ook in 2021 bleek dat een deel van de medewerkers niet volgens de vereisten van de AVG werkt, waardoor de FG niet tijdig geïnformeerd wordt. De FG ziet nog te vaak dat verplichtingen uit de AVG worden omzeild. Aangevoerde excuses zijn "een rem op de ontwikkelingen", "lastig", of "dat geldt niet voor ons". De risico's om de AVG niet na te leven, of de adviezen van de FG niet in te winnen of na te leven, laten zich raden. Er zijn sprekende en recente voorbeelden uit de pers zoals bijvoorbeeld bij de toeslagenaffaire, SyRi en de controle van burgers via social media.

Datagedreven werken en big data

In 2021 hoorde de FG over datagedreven werken, zoals datagedreven HR en de verwerking van big data voor beleidsvorming en -besluiten. Datagedreven werken kan de efficiency en de kwaliteit van besluiten verhogen. De provincie moet daarbij echter wel ruimschoots aandacht hebben voor privacy. En dat leidt nog wel eens tot knelpunten, ook omdat de kennis vaak ontbreekt over wat wel en niet mag volgens de privacyregels. De toeslagenaffaire bij de Belastingdienst, het Systeem Risico Indicatie (SyRI) en monitoring op social media zijn voorbeelden van hoe het mis kan gaan bij de verwerking van big data.

Op zich staat de AVG niet in de weg bij de verwerking van grote hoeveelheden persoonsgegevens, als dit binnen de kaders van de wet gebeurt. Belangrijke voorwaarde is het doel waarvoor de gegevens worden verwerkt. Is dit verenigbaar met het doel waarvoor ze oorspronkelijk zijn verzameld? Om deze vraag te beantwoorden moet een verenigbaarheidstoets worden uitgevoerd. Verder is het ook de vraag op welke grondslag de organisatie zich baseert om de gegevens te verwerken? En tenslotte: de provincie kan zich niet beroepen op de uitzonderingsgrond dat zij de gegevens verwerkt voor statistische doeleinden, want hoewel dit in het afgelopen jaar wel is geprobeerd, biedt dit lang niet altijd een uitweg.

Om grote hoeveelheden persoonsgegevens te verwerken, zal de provincie ieder keer weer een PIA moeten uitvoeren, waarbij de FG deze telkens toetst aan de vereisten uit de AVG. Het is duidelijk dat de provincie nog worstelt met de bescherming van privacy bij het verwerken van grote hoeveelheden persoonsgegevens. Dat privacybeleid ontbreekt, draagt hier ook aan bij.

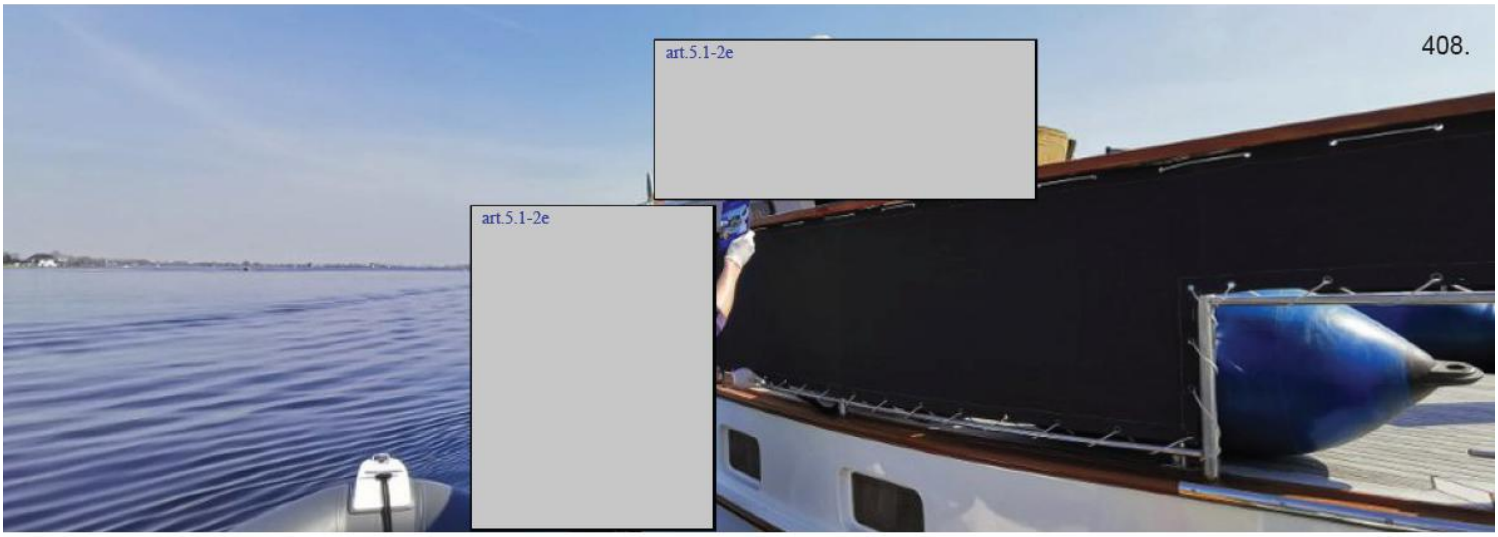
Belangrijk is ook om bewust een afweging te maken van de wenselijkheid om sowieso op grootschalige wijze persoonsgegevens te verwerken. Hoewel dit sterk raakt aan de ethische aspecten en daarmee weliswaar niet direct valt binnen de werkingssfeer van de FG, zou het wel goed zou zijn wanneer dit binnen de provincie ingebed zou zijn. Dit zou bijvoorbeeld kunnen via een ethische impact analyse, vergelijkbaar en wellicht ook te combineren met de Privacy Impact Assessment.

Bewustwording

De overheid is de grootste verwerker van persoonsgegevens in Nederland. Ook de provincie verzamelt op grote schaal persoonsgegevens. Weliswaar op minder grote schaal dan bijvoorbeeld gemeenten, maar daarin schuilt ook juist weer een risico. Gemeenten zijn zich mogelijk meer bewust dat zij werken met (gevoelige) persoonsgegevens dan de provincie. Gemeenten herkennen daardoor vaak beter persoonsgegevens en verwerken deze dan in lijn met de AVG. Dat bewustzijn blijkt in de praktijk bij de provincie minder groot. Enkele citaten zijn hier voorbeelden van:

- "wij verwerken bijna geen persoonsgegevens"
- "die hele AVG is flauwekul, daar heb ik geen zin in"
- "ik ben ambtenaar met een geheimhoudingsplicht, dus ik mag altijd alle persoonsgegevens gebruiken"
- "de AVG is zijn doel ver voorbij aan het schieten"

Deze citaten maken duidelijk dat de provincie nog de nodige stappen moet zetten om het bewustzijn van privacyregelgeving onder bestuurders, management en medewerkers te vergroten. In 2021 werd te vaak niet voldoende of helemaal geen gevolg gegeven aan adviezen van de FG. De mate waarin mensen adviezen van de FG opvolgen, lijkt soms af te hangen van de mate waarin het advies de ontvanger uitkomt voor diens doel. Op deze manier omgaan met adviezen van de FG raakt niet alleen de naleving van de AVG, maar evenzeer de integriteit van de organisatie.



Wet politiegegevens

De provincie heeft voor toezicht en handhaving op haar waterwegen een aantal buitengewoon opsporingsambtenaren (BOA's) in dienst. Bij de uitoefening van hun toezichthoudende taken hebben de BOA's te maken met de AVG. Voor hun handhavingstaken hebben zij echter te maken met de Wet politiegegevens (Wpg). De Wpg schrijft voor dat de verwerkingsverantwoordelijke bij het verwerken van persoonsgegevens (de provincie), een FG moet aanwijzen. De provincie heeft één FG aangewezen die zowel toezichthouder is op grond van de AVG als op grond van de Wpg.

De Wpg schrijft, in tegenstelling tot de AVG, voor dat de provincie jaarlijks een interne audit moet uitvoeren op de verwerking van persoonsgegevens en een vierjaarlijkse externe privacy audit. Een registerauditor van de Eenheid Audit en Advies van de provincie voerde in 2021 voor het eerst een interne audit uit. De bevindingen daaruit leverden input voor de daarna uitgevoerde externe audit waarvan de rapportage in 2022 verschijnt.

Uit de interne audit komen enkele zaken naar voren die niet in orde zijn en dus actie vereisen. Een van die zaken is de verwerking in iDMS. Een andere is dat de FG onvoldoende toezicht houdt. De FG is het eens met bevindingen uit de interne rapportage.

Provinciale Staten

Provinciale Staten zijn verantwoordelijk voor de verwerking van persoonsgegevens binnen de Griffie. Evenals de afdelingen binnen de provincie heeft de Griffie dit jaar veel tijd en energie gestoken in het op orde krijgen van het register van verwerkingsactiviteiten. Daarin zijn tot op heden negen verwerkingen opgenomen. Alle processen zijn getoetst en akkoord bevonden.
De Griffie startte in 2021 een PIA voor de vervanging van het oude Staten Informatie Systeem (SIS) en rondt deze begin 2022 af.

Commissaris van de Koning

In de taken van de CdK onderscheiden we Rijkstaken en provinciale taken. De FG van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties houdt toezicht op de Rijkstaken. De FG van de provincie houdt toezicht op de verwerking van persoonsgegevens van de provinciale taken van de CdK.

Over 2021 zijn geen bijzonderheden te melden.

Vooruitblik

FG

De FG vraagt aandacht voor nu al bekende uitdagingen in 2022. Op zijn planning staan, naast de reguliere toezichthoudende activiteiten, in elk geval:

- Voor ondermijning een audit voor de processen waarbij persoonsgegevens een rol spelen;
- Een advies schrijven over de doorgifte van persoonsgegevens naar derde landen, in het bijzonder de Verenigde Staten en de opslag van persoonsgegevens door bedrijven met een Amerikaanse moedermaatschappij;
- De Eenheid Audit en Advies een volwassenheidsonderzoek laten uitvoeren;
- Een advies schrijven voor het gebruik van social media, chat apps en videoconferencing;
- Aandacht vragen voor de implementatie van het beginsel Privacy by Design;
- Een audit naar de processen in de applicatie PINK.

Bewustwording en e-learning

Het niveau van bewustwording is te laag. Nu is werken aan bewustwording en bewustzijn een continue proces waarbij de provincie verschillende middelen kan inzetten. De AVG legt werken aan bewustwording ook aan de verwerkingsverantwoordelijke op. Om iedere medewerker ook echt te bereiken, kan de provincie een e-learning programma inzetten. Om zeker te zijn van deelname van iedere medewerker, zou dit een jaarlijkse verplichting moeten zijn voor iedere medewerker, afgesloten met een toets.

Met de komst van een Eenheid Privacy kan de provincie ook meer en structureel inzetten op voorlichting en bewustwording van afdelingen en teams. Uiteraard spelen de privacy officers van de afdelingen hierbij een belangrijke rol.

Wet politiegegevens

Begin 2022 verschijnt de rapportage van de privacy audit die een externe auditor uitvoerde in 2021. Het is al duidelijk dat daaruit een aantal belangrijke bevindingen naar voren komen die de provincie voortvarend moet oppakken. Enerzijds is dat de implementatie van een separate applicatie voor de Boa's, waarin zij op een verantwoorde wijze persoonsgegevens en politiegegevens kunnen verwerken. Daarnaast zal de FG werk moeten maken van toezicht houden.

Organisatie team privacy

De provincie heeft een grote en belangrijke stap voorwaarts gezet om in 2022 de bescherming van persoonsgegevens stevig in te bedden in de organisatie door het oprichten van een Eenheid Privacy van 6 fte. Deze centrale eenheid zal de afdelingen ondersteunen om aan de verplichtingen te voldoen op het gebied wet- en regelgeving rondom privacy en gegevensbescherming. Dit doen zij onder meer door hulp te bieden bij Privacy Impact Assessments en door bewustwording te vergroten bij alle medewerkers. Daarnaast onderhouden zij het register van verwerkingsactiviteiten en zorgen voor de afhandeling van datalekken. De eenheid geeft vorm aan en houdt het privacybeleid up-to-date en levert rapportages aan de FG.

Een punt van aandacht is de plaats van de eenheid in de organisatie. Een plaats naast de afdelingen verdient de voorkeur, bijvoorbeeld bij een afdeling die zich bezighoudt met concern control. De positie van de FG verdient ook een heroverweging. Nog te vaak ziet de organisatie de FG als een verlengstuk van de afdeling Bestuur. De FG legt verantwoording af aan de drie bestuursorganen, waardoor een plaats naast of boven de afdelingen logisch lijkt.
Los hiervan moet er in 2022 op de afdelingen ruimte en aandacht zijn voor privacy, bijvoorbeeld door structureel tijd te creëren voor de privacy officers van de afdelingen zodat zij hun rol ook goed kunnen invullen.

Opgave Gerichte Organisatie

De provincie zit in een transitie naar een ander organisatiemodel. Het huidige model is tamelijk hiërarchisch ingericht met afdelingen en bureaus of teams. De organisatie werkt toe naar een flexibeler model om vanuit opgaves te gaan werken. De provincie moet bij de overgang naar opgavegericht werken goed nadenken over hoe zij de AVG hierin borgt.

Lijst van afkortingen

AI	Artificiële Intelligentie
AP	Autoriteit Persoonsgegevens
DPIA	Data Protection Impact Assessment
FG	Functionaris voor Gegevensbescherming
GEB	Gegevensbeschermingseffectbeoordeling
GS	College van Gedeputeerde Staten
PIA	Privacy Impact Assessment, zie ook DPIA en GEB
PS	Provinciale Staten


VIGILATE DEO

Zuid-Holland applicatie | ICT-plein

Datalek

Procedure datalek

Vermoed je een datalek binnen de provincie Zuid-Holland? Meld dit dan zo snel mogelijk via het loket (zie link aan de rechterkant).

Wat is een datalek?

We spreken van een datalek als persoonsgegevens (http://binnenplein.pzh.nl/groepen/privacybescherming/veelgestelde-vragen/) zijn blootgesteld aan verlies of onrechtmatige verwerking. Bijvoorbeeld als persoonsgegevens in handen vallen van derden, die geen toegang tot die gegevens zouden mogen hebben. Het onbedoeld vernietigen of onbruikbaar maken van persoonsgegevens is eveneens een datalek.

Een datalek? En hoe nu verder?

Wanneer er een melding is gedaan wordt die behandeld door de eenheid Privacy. Een van de Privacy Officers van die eenheid neemt na de melding contact met je op voor meer details. Om je gerust te stellen: een datalek kan iedereen overkomen en het is niet strafbaar! Datalekken komen in iedere organisatie voor en één van de doelen van het melden van een datalek is dat we er als organisatie van kunnen leren. De provincie als organisatie kan overigens wel een boete opgelegd krijgen, als wij datalekken niet of niet op tijd melden.

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

Binnen 72 uur moet de provincie een datalek melden aan de Autoriteit Persoonsgegevens. Hierbij moet er sprake zijn van een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Of als het datalek aanleiding kan zijn voor ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Daarom is het belangrijk om een datalek meteen te melden via Het Loket, zodat de provincie nog tijd heeft om te onderzoeken hoe groot het datalek is en hoe groot de mogelijke gevolgen zijn van het datalek. Bedenk ook dat als je een datalek op een vrijdagmiddag meldt, je daarna dan wel bereikbaar moet blijven voor de collega's van de eenheid Privacy, omdat datalekken zo snel mogelijk onderzocht moeten worden.

Denk na over de omgang met persoonsgegevens

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

Dus: constateer je een datalek? Meld het!

Voorbeelden van mogelijke datalekken zijn:

- Het versturen van gevoelige persoonsgegevens naar een onjuist e-mailadres, ofwel naar iemand waar het niet voor bedoeld was.
- Het versturen van documenten met o.a. persoonsgegevens naar een organisatie die de persoonsgegevens niet nodig heeft voor de uitvoering van haar taak.
- Het versturen van een brief met daarop persoonsgegevens, naar de verkeerde persoon.
- Het zonder noodzaak op internet publiceren van documenten met persoonsgegevens.

- Diefstal van gegevensdragers (bijvoorbeeld documenten, USB stick) met persoonsgegevens.
- Als je vaststelt dat je toegang hebt tot persoonsgegevens waar je geen toegang toe zou moeten hebben.
- Inbraak in een computer met onversleutelde persoonsgegevens.
- Een telefoon/laptop/tablet (privé of zakelijk) met persoonsgegevens, die verloren of gestolen is en onvoldoende beveiligd.
- Anonieme enquêteresultaten die toch herleidbaar blijken te zijn tot respondenten.
- Afgedrukte documenten met persoonsgegevens die onbeheerd bij een kopieerapparaat liggen.

Heb je nog vragen?

Bekijk de veel gestelde vragen in de AVG groep (http://binnenplein.pzh.nl/groepen/privacybescherming/veelgestelde-vragen/) op het Binnenplein. Staat jouw vraag hier niet tussen? Plaats dan een bericht in deze groep of stuur een mail naar privacy@pzh.nl (mailto:privacy@pzh.nl).

Melden van een datalek (https://pvzh.topdesk.net/tas/public/ssp/content/serviceflow?unid=0523af60acfc4c509d4f4abf09f43e2a)

A 97999 Bestuur - melding vermissing ICT middel Security

art.5.1-2e

Wijzigingsaanvraag (W23 03 00293)

Naam	art.5.1-2e	Noodwijziging	Nee
Gebouw	PZH	Impact	Cat.0 - Uitvoerder
Soort	Bestuur Datalek	Prioriteit	Hoog
Korte omschrijving (Wijziging)	Diefstal of vermissing ICT middel		
Categorie	Bestuur - Eenheid Privacy		
Subcategorie	Datalek		

Details

Korte omschrijving (Activiteit)	Bestuur - melding vermissing ICT middel Security
Categorie	Bestuur - Eenheid Privacy
Subcategorie	Datalek

Afhandeling

Behandelaar	Bestuur - Eenheid Privacy
Behandelaarsgroep	Bestuur - Eenheid Privacy
Gestart	Nee
Afgerond	Nee
Overgeslagen	Nee
Bestede tijd	00:00
Kosten	0,00

Planning

Gepland voor fase	Wijzigingsaanvraag
Planning	Automatisch aanpassen
Geplande startdatum	24 maart 2023 10:22
Geplande einddatum	27 maart 2023 10:22

Actie

24 maart 2023 10:22

Acties Eenheid Privacy - vermissing ICT middel
- Beoordeel of er sprake is van verlies van persoonsgegevens en volg de afhandeling van het protocol datalekken.
- Sluit de actie af in Topdesk.

Bestede tijd

Oorspronkelijk plan	00:00
Huidig plan	00:00
Gerealiseerd	00:00
Nog te verwachten (+)	00:00

Kosten

Oorspronkelijke planning	0,00
Huidig plan	0,00
Gerealiseerd	0,00
Nog te verwachten (+)	0,00

art.5.1-2e

A 97999 Bestuur - melding vermissing ICT middel Security

Opslaan | Nieuwe activiteit | Meer

ALGEMEEN | OVERZICHT ACTIVITEITEN | PLANNER | WIJZIGING | BEHEER | P&O | BIJLAGEN (2) | TIJDREGISTRATIE

Overzicht

Tonen ○ Alle ◉ Groep

Sorteren ◉ Nieuwste notities bovenaan ○ Oudste notities bovenaan

Omschrijvingen

Acties

A 98000 **24-03-2023 10:5** art.5.1-2e
- Melding aangemaakt, doorgezet naar team privacy: M23 03 02998
- Wipe op afstand uitgevoerd.
- Wachtwoordreset uitgevoerd.
- CMDB aangepast
- Gebruiker heeft diefstalformulier ingevuld: W23 03 00293
- Vervangende laptop uitgegeven: M23 03 03025

A 98000 **24-03-2023 10:22 :**
Acties Servicedesk (indien mogelijk) bij vermissing of diefstal:
- Wijzig in overleg met de gebruiker het wachtwoord.
- Verwijder het computeraccount uit de AD.
- Indien mogelijk: Doe een "remote wipe" van het apparaat.
- Als het om een mobiele telefoon gaat: verwijder het 06-nummer uit het AD "pager" field van de gebruiker.
- Blokkeer het toestel (IMEI).
- Blokkeer het GSM-nummer.
- Sluit de actie af in Topdesk.
- Maak als het om een tablet of pzh-laptop gaat een call aan voor netwerk en telecom met het verzoek om a.d.h.v. het desbetreffende ci-nr het device in ICE te blokkeren (blacklist).

LET OP!
- Als alle acties zijn afgerond (zie in de wijziging het tabblad planner) sluit dan de wijziging door bij de Status
- 'Afgerond' te selecteren.

A 97999 **24-03-2023 10:22 :**
Acties Eenheid Privacy - vermissing ICT middel

AUTORITEIT
PERSOONSGEGEVENS

Vragenlijst meldformulier datalekken

In dit document vindt u de vragen uit het online meldformulier datalekken van de Autoriteit Persoonsgegevens (AP). Dit document helpt u om vóór het invullen van het online formulier de vragen alvast in te zien. Zo kunt u de benodigde informatie alvast verzamelen. Daarnaast kan de vragenlijst uw organisatie helpen om een stappenplan op te stellen waarmee u een (toekomstig) datalek zo tijdig en volledig mogelijk kunt melden.

Versie 1.0, juli 2022

Disclaimer

U kunt geen rechten ontlenen aan dit document. De AP kan dit document tussentijds wijzigen. De laatste versie vindt u op de website van de AP.

Let op: u kunt dit document niet gebruiken om een datalekmelding per post of e-mail aan de AP te sturen. De AP accepteert alleen datalekmeldingen via het online meldformulier datalekken.

Welke informatie heeft u (mogelijk) nodig bij het melden van een datalek?

Deze informatie heeft u altijd nodig:

- contactgegevens van de persoon die de AP kan benaderen bij vragen;
- contactgegevens van uw functionaris gegevensbescherming (indien van toepassing);
- correspondentie over de ontdekking van het datalek;
- verwerkingsregister (artikel 30 AVG);
- datalekkenregister (artikel 33, lid 5 AVG);
- de getroffen maatregelen om het datalek te beëindigen;
- de getroffen maatregelen om het datalek in de toekomst te voorkomen;
- de maatregelen die u al voor het datalek had getroffen;
- data protection impact assessment (DPIA) (indien van toepassing).

Indien sprake is geweest van een hacking- of malware-incident of ander incident waarbij (extern) onderzoek heeft plaatsgevonden:

- het onderzoeksrapport naar aanleiding van de inbreuk.

Als u gebruikmaakt van een derde partij om persoonsgegevens te verwerken:

- verwerkersovereenkomst;
- andere overeenkomsten, zoals een samenwerkingsovereenkomst.

AUTORITEIT
PERSOONSGEGEVENS

Als u de betrokkenen (de getroffen personen) moet informeren:

- correspondentie aan de betrokkenen.

Onderzoek bij hacking, malware (bijv. ransomware) en/of phishing

Meldt u een datalek aan de AP als gevolg van hacking, malware (bijv. ransomware) en/of phishing? Dan verwacht de AP dat u zo snel mogelijk onderzoek doet of laat doen naar de omvang van het incident. Het is immers mogelijk dat kwaadwillende hackers op minder zichtbare delen van uw netwerk en/of systemen malware en andere wijzigingen hebben toegepast, waarmee ze bijvoorbeeld op een later moment weer toegang kunnen krijgen tot uw netwerk. Bovendien kunt u zonder het uitvoeren van onderzoek geen uitsluitsel krijgen over de vraag of persoonsgegevens door derden zijn ingezien, gekopieerd/gestolen of veranderd. De AP verwacht dat u in ieder geval het volgende bij uw onderzoek betrekt:

- Is er toegang geweest tot de persoonsgegevens, bijvoorbeeld tot e-mails in een mailbox of de inhoud van een database?
- Zijn deze persoonsgegevens gekopieerd, ingezien of anderszins verzonden naar de hackers?
- Zijn er loggegevens beschikbaar en zo ja, kunt u met die loggegevens uitsluiten dat persoonsgegevens zijn gekopieerd of ingezien?

Documentatieplicht - datalekkenregister

Het melden van een datalek bij de AP is slechts een onderdeel van de meldplicht datalekken. Daarnaast moet u een register bijhouden waarin u alle datalekken registreert die binnen uw organisatie plaatsvinden. Dus ook de datalekken die u niet aan de AP heeft gemeld omdat dat niet nodig was. Neem in het register in ieder geval de volgende informatie op:

- de feiten over het datalek, zoals de oorzaak, wat er precies is gebeurd en om welke persoonsgegevens het gaat;
- de gevolgen van het datalek;
- de maatregelen die u heeft getroffen om het lek te dichten en om herhaling te voorkomen.

Het is aan te raden om ook aan te geven waarom u een datalek wel of niet heeft gemeld aan de AP en de betrokkenen. Maar dit is niet verplicht.

AUTORITEIT
PERSOONSGEGEVENS

Vragenlijst meldformulier datalekken

AUTORITEIT
PERSOONSGEGEVENS

1. Introductie

Een nieuwe melding doen van een inbreuk

1.1 Wat voor soort melding wilt u doen?

- Ik wil één inbreuk melden (reguliere melding) [= door naar 1.2]
- Ik wil meerdere gelijksoortige inbreuken, als gevolg van een grootschalige postverzending, tegelijk melden (bulkmelding) [= door naar 1.1.2]

1.1.1. Heeft uw organisatie uitdrukkelijke schriftelijke toestemming ontvangen van de AP om inbreuken in bulk te melden?

- Ja [=door naar 1.1.2]
- Nee [EINDE FORMULIER]

Op dit moment loopt er een pilot waarbij alleen pensioenfondsen, verzekeraars en banken inbreuken in bulk mogen melden. Het is op dit moment niet mogelijk om toestemming te krijgen om bulkmeldingen in te dienen. Zodra dit wel kan, staat dit op de website van de AP.

1.1.2 Geef het aantal inbreuken aan dat u bij de AP in bulk wilt melden:

[open veld]

Geef onder vraag 5.3 “Beschrijving van het incident” duidelijk aan dat het gaat om een bulkmelding, en geef aan om hoeveel poststukken het gaat. Controleer verder of u aan alle door de AP gestelde voorwaarden voor het doen van een bulkmelding heeft voldaan, voordat u de melding verstuurt.

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?

- Algemene verordening gegevensbescherming (AVG)
- Telecommunicatiewet (Tw)
- Wet justitiële en strafvorderlijke gegevens (Wjsg)
- Wet politiegegevens (Wpg)

De meldplicht datalekken is in vier wetten opgenomen. In de meeste gevallen zult u een melding doen onder de AVG. Alleen wanneer u een telecommunicatieaanbieder bent of u op grond van de Wjsg of de Wpg persoonsgegevens verwerkt, kan dat anders zijn.

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

- Ja, namelijk: Meerdere opties zijn mogelijk.
  - ☐ Autoriteit Financiële Markten (AFM)
  - ☐ Agentschap Telecom (AT)
  - ☐ De Nederlandsche Bank (DNB)

AUTORITEIT
PERSOONSGEGEVENS

- ☐ Inspectie Gezondheidszorg en Jeugd (IGJ)
- ☐ Inspectie Leefomgeving en Transport (ILT)
- ☐ Inspectie voor het Onderwijs
- ☐ Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
- ☐ Onderzoeksraad voor Veiligheid (OVV)
- ☐ Andere toezichthouder, namelijk [open veld]

o Nee

AUTORITEIT
PERSOONSGEGEVENS

2. Internationale aspecten

2.1 Grensoverschrijdende inbreuk

2.1.1 Heeft de inbreuk gevolgen voor personen in meerdere landen?

- Ja [= door naar 2.1.2]
- Nee [= door naar 3]

Wanneer u persoonsgegevens verwerkt in meer dan één land of wanneer de verwerking schadelijke gevolgen kan hebben voor personen in meer dan één land, is het mogelijk dat u de inbreuk bij meer dan één toezichthouder moet melden. Twijfelt u of u de inbreuk bij de AP of bij een toezichthouder uit een ander Europees land moet melden? Dan kunt u gebruik maken van het "Stroomschema identificatie leidende toezichthouder". Zie daarnaast de Q&A voor meer informatie.

2.1.2 Bevindt de hoofdvestiging of de enige vestiging van uw organisatie zich in Nederland?

- Ja [= door naar 2.1.3]
- Nee [= door naar 2.1.3]

De AP is de leidende toezichthouder wanneer de hoofdvestiging of de enige vestiging van uw organisatie zich in Nederland bevindt.

2.1.3 Als er sprake is van een grensoverschrijdende gegevensverwerking, om welke landen gaat het dan?

[lijst met EU landen + mogelijkheid andere landen op te geven + optie om aantal betrokkenen op te geven]

2.2 Bevoegde toezichthouders in andere EU-lidstaten

2.2.1 Heeft uw organisatie de inbreuk gemeld bij andere privacytoezichthouders?

- Nee [= door naar 2.2.2]
- Ja [= door naar 2.2.1.1]

2.2.1.1 Geef aan in welk(e) land(en) u de inbreuk aan de privacytoezichthouder heeft gemeld. Meerdere opties zijn mogelijk.

[lijst met EU landen + mogelijkheid andere landen op te geven + optie om aantal betrokkenen op te geven]

2.2.2 Gaat uw organisatie de inbreuk nog melden bij andere privacytoezichthouders?

- Nee [= door naar 3]
- Ja [= door naar 2.2.2.1]

2.2.2.1 Geef aan in welk(e) land(en) u de inbreuk aan de privacytoezichthouder gaat melden. Meerdere opties zijn mogelijk.

AUTORITEIT
PERSOONSGEGEVENS

[lijst met EU landen + mogelijkheid andere landen op te geven + optie om aantal betrokkenen op te geven]

AUTORITEIT
PERSOONSGEGEVENS

3. De verwerkings-verantwoordelijke

3.1 Contactgegevens

3.1.1. Over welke organisatie of welk bedrijf gaat het?

Registratienummer van de FG	[open veld] [optioneel]
KvK-nummer	[open veld] [optioneel]
Naam van het bedrijf of de organisatie	[open veld]
Adres	[open veld]
Postcode	[open veld]
Plaats	[open veld]

3.1.2 In welke sector is de organisatie of het bedrijf actief?

[Lijst met sectoren]

Weet u niet zeker binnen welke sector u actief bent, controleer dan binnen welke SBI u bij de Kamer van Koophandel geregistreerd staat of selecteer de sector die het dichtst bij uw economische activiteiten in de buurt komt.

3.2 Gegevens melder en contactpersoon

3.2.1 Wie meldt de inbreuk?

Naam	[open veld]
Functie	[open veld]
E-mailadres	[open veld]
Telefoonnummer	[open veld]
Tweede telefoonnummer	[open veld] [Optioneel]

Dit dient een direct telefoonnummer te zijn en geen algemeen telefoonnummer

3.2.2 Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?

- ○ Ja [= door naar 3.3]
- ○ Nee [velden invullen en daarna door naar 3.3]

Naam contactpersoon	[open veld]
Functie contactpersoon	[open veld]
E-mailadres contactpersoon	[open veld]
Telefoonnummer contactpersoon	[open veld]
Tweede telefoonnummer	[open veld] [Optioneel]

De contactpersoon dient daags na de melding goed bereikbaar te zijn tijdens kantooruren om eventuele vragen van de AP over de inbreuk te

AUTORITEIT
PERSOONSGEGEVENS

kunnen beantwoorden.

3.3 Andere organisaties

3.3.1 Waren er andere organisaties betrokken bij de inbreuk?

- Ja [= door naar 3.3.2]
- Nee [= door naar 4]

Een organisatie is betrokken bij de inbreuk als deze een rol heeft gehad bij het ontstaan van de inbreuk.

3.3.2 Geef aan welke andere organisaties betrokken waren bij de inbreuk?

Naam	Op welke wijze betrokken	Toelichting (optioneel)
Organisatie A	bijvoorbeeld verwerker	
Organisatie B		
+ Voeg nog een organisatie toe		

AUTORITEIT
PERSOONSGEGEVENS

4. Tijdlijn

4.1. Duurt de inbreuk op dit moment nog voort?
- Ja [=door naar 4.1.1]
- Nee [=door naar 4.1.1 + 4.1.2]
- Onbekend [=door naar 4.1.1]

4.1.1 (Mogelijke) startdatum van de inbreuk
[datumveld]
4.1.2 (Mogelijke) einddatum van de inbreuk
[datumveld]

4.2 Wanneer is het incident ontdekt?
[datumveld]

4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt
[open veld]

4.4 Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk ("datalek") en dus kennis heeft gekregen van de inbreuk?
- Ja [=door naar 5, tenzij later dan 72 uur na de ontdekkingsdatum dan door naar 4.5]
- Nee [=door naar 4.4.1]

Met het krijgen van kennis van een inbreuk wordt bedoeld dat u op basis van objectieve factoren heeft kunnen aannemen dat het aannemelijk is dat een datalek zich heeft voorgedaan. Dit hoeft niet het moment te zijn waarop u het datalek heeft ontdekt. **Let op**: Dit kan niet het moment zijn waarop het incident bij de FG werd gemeld. De FG is niet verantwoordelijk voor de verplichtingen die de meldplicht datalekken met zich mee brengt. Dit betekent dat de AP dit niet als gerechtvaardigde reden beschouwd waarom de melding te laat is ingediend.

4.4.1 Wanneer heeft u kennis gekregen van de inbreuk?
[datumveld]

Als de inbreuk later dan 72 uur na kennisname wordt gemeld moet de volgende vraag beantwoord worden:
4.5 Beschrijf hieronder waarom u de inbreuk later dan 72 uur na ontdekking meldt:
[open veld]

AUTORITEIT
PERSOONSGEGEVENS

5. Gegevens over de inbreuk

5.1 Aard van de inbreuk Meerdere opties zijn mogelijk.

Bij een incident kan sprake zijn van één of meerdere type inbreuken die gaan over de vertrouwelijkheid, de beschikbaarheid en de integriteit van de persoonsgegevens. Een voorbeeld hiervan is wanneer u geconfronteerd wordt met ransomware (gijzelsoftware). Om een bestand te versleutelen / gijzelen dient de malafide software de bestanden eerst te openen om deze vervolgens te kunnen versleutelen. Hierdoor is zowel sprake van een inbreuk op de vertrouwelijkheid / ingezien door onbevoegden als sprake van een inbreuk op de beschikbaarheid. Kijk voor meer informatie in onze Q&A.

☐ P

ersoonsgegevens (mogelijk) ingezien door onbevoegden

Onder "ingezien" wordt ook bedoeld dat er sprake is (geweest) van ongeoorloofde of onbedoelde verstrekking van of toegang tot persoonsgegevens

☐ Persoonsgegevens ongeoorloofd of onopzettelijk gewijzigd
☐ Persoonsgegevens permanent niet beschikbaar (verloren/verwijderd)
☐ Persoonsgegevens tijdelijk niet beschikbaar

Het moet gaan om onopzettelijk of ongeoorloofd verlies van toegang tot persoonsgegevens of een onopzettelijke of ongeoorloofde vernietiging van persoonsgegevens. Hiervan kan ook sprake zijn als u (tijdelijk) geen gebruik kunt maken van de persoonsgegevens die noodzakelijk zijn voor de verwerkingsdoeleinden.

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest? Slechts één optie is mogelijk.

☐ E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)

5.2.1.Heeft de verkeerde ontvanger bevestigd de e-mail te hebben verwijderd?

- Ja [= door naar 5.3]
- Nee [= door naar 5.3]
- De verkeerde ontvanger heeft niet gereageerd [= door naar 5.3]

☐ E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in de cc, in plaats van bcc [= door naar 5.3]
☐ Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)

5.2.2. Heeft de verkeerde ontvanger bevestigd dat de persoonsgegevens vernietigd zijn, of zijn de persoonsgegevens teruggestuurd?

- Ja [= door naar 5.3]
- Nee [= door naar 5.3]
- De verkeerde ontvanger heeft niet gereageerd [= door naar 5.3]

☐ Brief of postpakket met persoonsgegevens geopend retour ontvangen [= door naar 5.3]
☐ Brief of postpakket met persoonsgegevens kwijtgeraakt [= door naar 5.3]

AUTORITEIT
PERSOONSGEGEVENS

☐ Autorisatie(s) van medewerker(s) verkeerd ingesteld. [= door naar 5.3]

Dit incident heeft betrekking op de situatie waarbij de toegang- of leesrechten van een gebruiker niet of abusievelijk zijn aangepast, waardoor een gebruiker meer mogelijkheden in het systeem heeft dan zou moeten. Bijvoorbeeld: een autorisatierol is bij functiewijziging niet goed doorgevoerd.

☐ Netwerkmappen of -locaties met persoonsgegevens zijn te breed toegankelijk ingesteld binnen de organisatie. [= door naar 5.3]

Dit heeft betrekking op het systeem, waarbij een gedeelde map, locatie of applicatie verkeerd is ingesteld en daardoor voor onbevoegde personen is in te zien. Bijvoorbeeld: Een map met personeelsgegevens was toegankelijk voor elke medewerker.

☐ Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen [= door naar 5.3]
☐ Persoonsgegevens per ongeluk gepubliceerd [= door naar 5.3]
☐ Hacking, malware (bijv. ransomware) en/of phishing Meerdere opties zijn mogelijk

De AP adviseert u tevens aangifte te doen bij de Politie wegens onder andere computervredebreuk en/of computersabotage. Door aangifte te doen kan de politie in overleg met het Openbaar Ministerie (OM) besluiten om een onderzoek te starten en helpt u het OM bij het in kaart brengen van criminaliteit. Hiermee kan de politie strafbare feiten opsporen en meer slachtoffers voorkomen. Kijk voor meer informatie op www.nomoreransom.org.

☐ Phishing [= door naar 5.2.3]

Phishing is een verzamelnaam voor digitale activiteiten die tot doel hebben informatie van mensen te ontfutselen. Met deze informatie kunnen criminelen toegang krijgen tot (bedrijfs-)netwerken en fraude plegen, bijvoorbeeld bankfraude of identiteitsfraude.

☐ Ransomware [= door naar 5.2.3]

Ransomware is kwaadaardige software die een computer of bestanden gijzelt. In de meeste gevallen wordt daarna betaling geëist.

☐ Ander type hacking en/of malware [= door naar 5.2.3]

AUTORITEIT
PERSOONSGEGEVENS

Hieronder kunnen alle activiteiten vallen waarbij onrechtmatig toegang is verschaft tot persoonsgegevens of waarbij persoonsgegevens op een andere wijze onrechtmatig zijn aangetast.

5.2.3. Heeft u (digitaal forensisch) onderzoek uitgevoerd of laten uitvoeren naar de aard en de omvang van de inbreuk? [= door naar 5.3]

- Ransomware kan het hele systeem en alle gekoppelde bestanden raken. U kunt bij ransomware zonder (digitaal forensisch) onderzoek uit te voeren er niet van uit gaan dat de inbreuk beperkt is gebleven tot het zichtbaar besmette bestand of systeem.
- Een geslaagde phishing-actie, waarbij e-mailadres en wachtwoord zijn bemachtigd, kan ertoe leiden dat hackers toegang krijgen tot mailboxen, netwerken en systemen. In het geval van mailboxen is het mogelijk dat ook de e-mails in een mailbox zijn getroffen. Bij phishing kunnen dus niet alleen de contactpersonen in het adresboek van het e-mailaccount getroffen zijn, maar ook de personen van wie er e-mails in mailbox zijn opgeslagen.

- ○ Ja, het onderzoek loopt

Zodra het onderzoek is afgerond, moet u een vervolgmelding doen bij de AP.
De AP verwacht dat u in ieder geval het volgende bij uw onderzoek betrekt:

- Is er toegang geweest tot de persoonsgegevens, bijvoorbeeld tot e-mails in een mailbox of de inhoud van een database?
- Zijn deze persoonsgegevens gekopieerd, ingezien of anderszins verzonden naar de hackers?
- Zijn er loggegevens beschikbaar en, zo ja, kan u aan de hand van die loggegevens uitsluiten dat persoonsgegevens zijn gekopieerd of ingezien?

- ○ Ja, het onderzoek is afgerond [= door naar 5.2.3.1]

5.2.3.1. Upload hier de rapportage van het onderzoek naar de inbreuk
[UPLOAD-knop] [optioneel]

- ○ Nee, het onderzoek is nog niet gestart

De AP verwacht dat u zo snel mogelijk onderzoek (laat) doen naar de aard en de omvang van de inbreuk. U moet binnen 4 weken een vervolgmelding doen met de stand van zaken. De AP verwacht dat u in ieder geval het volgende bij uw onderzoek betrekt:

- Is er toegang geweest tot de persoonsgegevens, bijvoorbeeld tot e-mails in een mailbox of de inhoud van

AUTORITEIT
PERSOONSGEGEVENS

een database?
- Zijn deze persoonsgegevens gekopieerd, ingezien of anderszins verzonden naar de hackers?
- Zijn er loggegevens beschikbaar en, zo ja, kan u aan de hand van die loggegevens uitsluiten dat persoonsgegevens zijn gekopieerd of ingezien?

o Nee, er wordt geen onderzoek verricht

Zonder onderzoek zal de onzekerheid over de omvang van de besmetting echter blijven bestaan. Dit betekent dat u niet redelijkerwijs kunt uitsluiten dat persoonsgegevens door een derde zijn ingezien, gekopieerd, gestolen of veranderd. De AP verwacht dat u zo snel mogelijk onderzoek (laat) doen naar de aard en de omvang van de inbreuk. De AP verwacht dat u in ieder geval het volgende bij uw onderzoek betrekt:
- Is er toegang geweest tot de persoonsgegevens, bijvoorbeeld tot e-mails in een mailbox of de inhoud van een database?
- Zijn deze persoonsgegevens gekopieerd, ingezien of anderszins verzonden naar de hackers?
- Zijn er loggegevens beschikbaar en, zo ja, kan u aan de hand van die loggegevens uitsluiten dat persoonsgegevens zijn gekopieerd of ingezien?

5.2.3.2 Licht toe waarom u geen onderzoek verricht.

[open veld]

☐ Persoonsgegevens van verkeerde klant getoond in klantportaal
☐ Persoonsgegevens toegevoegd aan het verkeerde dossier
☐ Persoonsgegevens bij oud papier gezet
☐ Persoonsgegevens door storing (tijdelijk) niet beschikbaar
☐ Overig, namelijk: [open veld]

5.3 Beschrijving van het incident
Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

[open veld]

5.4 Indien beschikbaar: upload hier relevante ondersteunende documentatie bij uw melding.

Let op dat u geen persoonsgegevens opneemt in de bestanden als dat niet noodzakelijk is.
[UPLOAD-knop] [optioneel]

AUTORITEIT
PERSOONSGEGEVENS

AUTORITEIT
PERSOONSGEGEVENS

6. Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen Meerdere opties zijn mogelijk

☐ Naam
☐ Geslacht
☐ Geboortedatum en/of leeftijd
☐ Burgerservicenummer (BSN)
☐ Contactgegevens
- ☐ Adres en woonplaats
- ☐ E-mailadres
- ☐ Telefoonnummer

☐ Toegangs- of identificatiegegevens

Bijvoorbeeld gebruikersnamen en wachtwoorden

☐ Financiële gegevens
- ☐ Bankrekeningnummer / IBAN
- ☐ Creditcardgegevens
- ☐ Gegevens over (problematische) schulden
- ☐ Gegevens over uitkering en/of schulden
- ☐ Andere financiële gegevens, namelijk:[open veld]

☐ (Kopieën van) paspoorten of andere legitimatiebewijzen
☐ Locatiegegevens

Geen NAW-gegevens. Hiermee worden gegevens bedoeld om de locatie van een persoon te bepalen of te kunnen volgen, bijv. GPS-gegevens, zendmastgegevens.

☐ Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

Ook indirect kan sprake zijn van een strafrechtelijk persoonsgegeven, bijvoorbeeld afgeleid uit het ontwerp of logo van een envelop afkomstig van de reclassering of het Openbaar Ministerie.

☐ Anders, namelijk: [open veld]
☐ Onbekend

Indien onbekend is geselecteerd:
U moet binnen 4 weken een vervolgmelding indienen, waarin u aangeeft welke persoonsgegevens bij het datalek betrokken zijn.

AUTORITEIT
PERSOONSGEGEVENS

6.2 Bijzondere categorieën van persoonsgegevens

Een bijzonder persoonsgegeven kan ook indirect blijken uit feiten en omstandigheden van de situatie. Denk bijvoorbeeld aan de envelop die gebruikt is of het bijzondere kenmerk van uw organisatie, bijvoorbeeld een kerk, vakbond, LHBTQ-vereniging, een GGZ-instelling of specialistische zorg (bijv. oncologie).

- ☐ Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt
- ☐ Persoonsgegevens waaruit iemands politieke opvattingen blijken
- ☐ Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken
- ☐ Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt
- ☐ Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
- ☐ Gegevens over iemands gezondheid
- ☐ Genetische gegevens
- ☐ Biometrische gegevens (bijvoorbeeld: vingerafdruk of irisscan)

Dit zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking van fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon. Op grond hiervan is eenduidige identificatie van die persoon mogelijk. Of wordt zijn/haar identiteit bevestigd.

6.3 Hoeveelheid persoonsgegevens

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

[open veld]

Met een gegevensrecord (artikel 33, lid 3, sub a AVG) wordt bedoeld: de registratie van informatie over een gebeurtenis of over een persoon. Het begrip laat zich het beste uitleggen aan de hand voorbeelden:

1) Elke regel in een database vormt één gegevensrecord. Dit kan een database zijn met alle geplaatste orders, maar kan ook een database zijn met alle klantgegevens (CRM). 100 klanten in een CRM systeem vormen 100 records. Als elke klant 5 orders heeft geplaatst bij dat bedrijf staan er 500 gegevensrecords als order opgenomen in de orderdatabase;
2) Elke regel in een logboek vormt één gegevensrecord. In een medisch dossier wordt bijvoorbeeld bijgehouden wie wanneer inzage heeft gehad en handelingen heeft verricht in het dossier. Als iemand een dossier heeft geopend en één ding heeft aangepast, dan kunnen er minstens drie regels aangemaakt zijn (openen dossier (1), wijzigen informatie (2), sluiten dossier (3));
3) Een brief vormt één gegevensrecord. De dagtekening, gegevens van de geadresseerde en afzender staan als informatie opgenomen in de

AUTORITEIT
PERSOONSGEGEVENS

brief;
4) Een e-mail vormt één gegevensrecord. De verzenddatum en –tijdstip, de geadresseerde en de verzender staan in de mail;
5) Een paspoort vormt één gegevensrecord. Op een paspoort staat informatie opgenomen over een persoon, zoals naam, geboortedatum, nationaliteit, BSN, documentnummer van het paspoort en de stempels van de douane van de landen waar iemand is geweest;
6) Een (papieren) dossier van een persoon vormt ook een record, omdat daar informatie is opgeslagen over een persoon.

Het is mogelijk dat er meerdere soorten gegevensrecords zijn getroffen bij een inbreuk, omdat bijvoorbeeld het gehele netwerk is getroffen, waardoor zowel CRM als HR gegevens zijn getroffen. In de volgende vraag kunt u een toelichting geven op de getroffen gegevensrecords. Als het aantal gegevensrecords te groot is of als u niet weet hoeveel persoonsgegevensregisters zijn getroffen, voer dan “1” in en licht het aantal toe bij de volgende vraag. Zie voor meer informatie de Q&A.

Geef een toelichting op bovengenoemd aantal:
[open veld]

Hier kunt u een nadere toelichting geven op het aantal en soort getroffen gegevensrecords . Aan de hand van uw toelichting kan de AP een beter of genuanceerder beeld krijgen van het incident. U kunt bijvoorbeeld aangeven of er één of meerdere databases zijn getroffen of dat de inbreuk is beperkt tot een brief of een dossier.

AUTORITEIT
PERSOONSGEGEVENS

7. Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk? Meerdere opties zijn mogelijk.

- ☐ Werknemers
- ☐ Klanten (huidig en potentieel)
- ☐ Leerlingen of studenten
- ☐ Patiënten
- ☐ Minderjarigen
- ☐ Personen uit andere kwetsbare groepen
- ☐ Anders, namelijk: [open veld]

Met "betrokkene" wordt hier bedoeld de persoon van wie de persoonsgegevens zijn getroffen door de inbreuk.

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.
[open veld]

7.3 Is het exacte aantal betrokkenen bekend?

- ○ Ja
  7.3.1 Het exacte aantal is:
  [open veld]

- ○ Nee
  7.3.2 Het minimum aantal betrokkenen is:
  [open veld]
  7.3.3 Het maximum aantal betrokkenen is:
  [open veld]

AUTORITEIT
PERSOONSGEGEVENS

8. Maatregelen vooraf

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

☐ Ja, namelijk: versleuteld (encryptie)

8.1.1 Welke versleutelingstechniek heeft u toegepast (indien bekend)?
[open veld+ optioneel]

Probeer waar mogelijk ook details te geven, zoals het aantal bits van de gebruikte sleutel en de standaard (bijvoorbeeld AES-256). Let op: indien een laptop of andere drager beveiligd is met een wachtwoord betekent dat niet altijd dat de gegevens op de drager zijn versleuteld en onder "versleuteld" wordt niet bedoeld: versleuteld door een ransomware aanval.

☐ Ja, namelijk gehasht

8.1.2 Welke hashingtechniek heeft u toegepast (indien bekend)?
[open veld+ optioneel]

Denk bijvoorbeeld aan MD5, SHA-256, bcrypt, of een andere cryptografische hashfunctie. Geef hierbij ook aan of er gebruik gemaakt is van een salt.

☐ Ja, namelijk: op een andere manier onbegrijpelijk of ontoegankelijk gemaakt

8.1.3 Op welke manier waren de gegevens onbegrijpelijk of ontoegankelijk gemaakt (indien bekend)?
[open veld+ optioneel]

Denk hierbij aan standaard versleutelde soft- of hardware of andere beveiligingsmethoden

☐ Nee [= direct door naar 9]

8.2 Als de persoonsgegevens onbegrijpelijk of ontoegankelijk gemaakt waren, om welk deel gaat dat dan?

- ○ Alle gegevens waren vooraf onbegrijpelijk of ontoegankelijk gemaakt
- ○ Een deel van de gegevens was onbegrijpelijk of ontoegankelijk gemaakt, namelijk: [open veld]

AUTORITEIT
PERSOONSGEGEVENS

9. Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens. Meerdere opties zijn mogelijk.

- ☐ Onbevoegden hebben kennis kunnen nemen van de gegevens
- ☐ De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt
- ☐ Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt
- ☐ Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties
- ☐ Een essentiële dienst kan tijdelijk niet meer worden verleend aan degenen van wie gegevens zijn gelekt
- ☐ Een essentiële dienst kan permanent niet meer worden verleend aan degenen van wie gegevens zijn gelekt
- ☐ Anders, namelijk: [open veld]

Hiermee wordt bedoeld welk effect de inbreuk mogelijk heeft op uw organisatie en de verwerking van persoonsgegevens binnen uw organisatie.

9.2 (Mogelijke) gevolgen voor de betrokkene(n) Meerdere opties zijn mogelijk.

- ☐ Discriminatie of uitsluiting
- ☐ Identiteitsdiefstal of -fraude
- ☐ Financieel verlies
- ☐ Reputatieschade
- ☐ Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens
- ☐ Ongeoorloofde ongedaanmaking van pseudonimisering
- ☐ Betrokkenen kunnen bijvoorbeeld (de verwerking van) hun persoonsgegevens niet inzien of op verzoek laten verwijderen (Uitoefening van rechten)
- ☐ Betrokkenen verliezen het overzicht van welke organisaties hun persoonsgegevens verwerken en worden verhinderd controle uit te oefenen
- ☐ Anders, namelijk: [open veld]

9.3 Inschatting risico
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)

- ○ Verwaarloosbaar
- ○ Beperkt
- ○ Aanzienlijk
- ○ Zeer groot

Licht uw keuze toe:
[open veld]

AUTORITEIT
PERSOONSGEGEVENS

Er zijn in ieder geval 7 factoren waar u rekening mee dient te houden:

1. Welk incident heeft plaatsgevonden?
2. Hoeveel persoonsgegevens en welke soort persoonsgegevens zijn getroffen én hoe gevoelig zijn de persoonsgegevens in de context waarin de persoonsgegevens worden verwerkt?
3. Hoe makkelijk zijn de gegevens te koppelen aan een natuurlijk persoon?
4. Hoe ernstig kunnen de hierboven aangegeven eventuele gevolgen zijn?
5. Behoort de betrokkene tot een kwetsbare groep?
6. Heeft u uw organisatie een bijzondere positie (zoals een ziekenhuis, een bank, een (bijzondere) school)
7. Wat is de grootte van de groep betrokkenen?

Daarnaast kunt u specifieke feiten en omstandigheden meenemen waardoor het risico voor de betrokkenen verhoogd of verlaag worden. Raadpleeg Richtsnoeren voor de melding van datalekken vanaf 27 pagina voor meer informatie.

AUTORITEIT
PERSOONSGEGEVENS

10. Vervolgacties

10.1 Informeren van de betrokkene(n)

10.1.1. Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?

- Ja [= door naar 10.1.3]
- Nee [= door naar 10.1.2]

10.1.2 Gaat u de inbreuk nog melden aan de betrokkene(n)?

- Ja [= door naar 10.1.4]
- Nee [direct door naar 10.2]
- Nog niet bekend [direct door naar 10.2]

Let op, u moet er vanuit gaan dat u de inbreuk moet melden aan de betrokkene(n) als het gaat om de volgende persoonsgegevens:

- bijzondere persoonsgegevens
- strafrechtelijke persoonsgegevens
- kopieën van identiteitsbewijzen en/of paspoorten
- combinatie van BSN, naam en geboortedatum
- persoonsgegevens van mensen een kwetsbare groep
- veel persoonsgegevens of persoonsgegevens van veel betrokkenen

En/of de inbreuk kan leiden tot:

- discriminatie
- identiteitsdiefstal of –fraude
- financiële verliezen
- reputatieschade
- doorbreking van beroepsgeheim

Zie ook: de Guidelines meldplicht datalekken.

Let op bij phishing
Indien u een phishing incident meldt ten aanzien van een e-mailaccount is het mogelijk dat u twee groepen betrokkenen moet informeren, namelijk degenen wiens contactgegevens in het adresboek in de e-mailbox stonden en de degenen wiens (bijzondere of gevoelige) persoonsgegevens in e-mails in de e-mailbox waren opgeslagen, bijvoorbeeld in een bijlage.

10.1.3 Aan hoeveel personen heeft u de inbreuk gemeld?
[invoerveld]

10.1.4 Aan hoeveel personen wilt u de inbreuk gaan melden?
[invoerveld]

Let op: komt het door u opgegeven aantal betrokkenen dat u gaat informeren niet overeen met het aantal dat u bij vraag 7 heeft opgegeven? Dan vragen wij u dit nader toe te lichten.

Let op bij phishing
Indien u een phishing incident meldt ten aanzien van een e-mailaccount is

AUTORITEIT
PERSOONSGEGEVENS

het mogelijk dat u twee groepen betrokkenen moet informeren, namelijk degenen wiens contactgegevens in de e-mailbox stonden en de degenen wiens (bijzondere of gevoelige) persoonsgegevens in e-mails in de e-mailbox waren opgenomen, bijvoorbeeld in een bijlage.

10.1.5 Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)? [= door naar 10.1.7]
[datumveld]

10.1.6 Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)? [= door naar 10.1.7]
[datumveld]

10.1.7 Licht toe aan welke (groep) betrokkenen u de inbreuk heeft gemeld. [= door naar 10.1.8]
[invoerveld]

10.1.8 Wat is de inhoud van de melding aan de betrokkene(n)? [= door naar 10.1.9]
[open veld]

U bent verplicht aan te geven:
- Wat er is gebeurd;
- Wat de gevolgen zijn;
- Welke maatregelen u heeft getroffen, en;
- De naam en contactgegevens van de Functionaris gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen.

Optioneel: Upload hier een kopie van de tekst van deze kennisgeving
[UPLOAD-knop]

10.1.9 Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren? Meerdere opties zijn mogelijk.
- ☐ Telefonisch
- ☐ Per brief
- ☐ Per e-mail
- ☐ Via een mededeling op de website
- ☐ Via social media
- ☐ Via een advertentie in de krant
- ☐ Anders, namelijk: [open veld]

Indien alleen “Via een mededeling op de website” is aangekruist:
Een mededeling die beperkt blijft tot een algemene mededeling op uw website is over het algemeen geen effectief middel om een inbreuk aan een persoon mee te delen. De AP raadt u aan een middel te kiezen waarbij de

AUTORITEIT
PERSOONSGEGEVENS

kans dat de informatie naar behoren aan alle getroffen personen wordt meegedeeld, zo groot mogelijk is. Dat kan betekenen dat u verschillende communicatiemethoden gebruikt in plaats van één enkel contactkanaal. Bijvoorbeeld via een aanvullend persbericht, uw bedrijfsblog, en via de officiële social media accounts van uw organisatie.

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

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

☐ Het zou een onevenredige inspanning vergen om iedere betrokkene op individuele basis te informeren

10.2.1.1 Licht toe waarom het een onevenredige inspanning zou vergen om de betrokkenen op individuele basis te informeren.
[open veld]

☐ De maatregelen die ik heb getroffen voordat de inbreuk plaatsvond bieden voldoende bescherming om de melding aan de betrokkene(n) achterwege te kunnen laten

10.2.1.2. Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?
[open veld]

☐ Ik heb na de inbreuk maatregelen genomen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkene(n)

10.2.1.2. Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?
[open veld]

☐ Mijn organisatie is een financiële onderneming als bedoeld in de Wet op het financieel toezicht (uitzondering artikel 42 UAVG).

☐ Er is sprake van een zwaarwegend belang om de getroffen personen niet te informeren. Namelijk:
[open veld]

AUTORITEIT
PERSOONSGEGEVENS

De getroffen personen hoeven niet te worden geïnformeerd, indien dat noodzakelijk en evenredig is ter bescherming van:
- de nationale veiligheid;
- landsverdediging;
- de openbare veiligheid;
- de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
- andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
- de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
- de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
- een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g;
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of de inning van civielrechtelijke vorderingen.

☐ Andere reden(en), namelijk:
[open veld]

10.3. Maatregelen om de inbreuk aan te pakken

10.3.1 Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?

- Nee, want:
  [open veld]
- Nog niet bekend [U bent verplicht een vervolgmelding te doen waarin u aangeeft welke maatregelen u heeft getroffen om de inbreuk te beëindigen.]
- Ja, namelijk:
  [open veld]

Bijvoorbeeld verzocht om vernietiging van de verkeerd bezorgde brief of e-mail te verwijderen, het controleren van de logging om een inbreuk uit te sluiten, het dichtzetten van het beveiligingslek, het aanpassen van de autorisatiestructuur / rechtenstructuur.

10.3.2 Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?

- Nee, want:
  [open veld]

AUTORITEIT
PERSOONSGEGEVENS

- Nog niet bekend [U bent verplicht een vervolgmelding te doen waarin u aangeeft welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.]
- Ja, namelijk:
  [open veld]

Bijvoorbeeld het geven van bewustwordingstraining, het aanpassen van werkprocessen, het toepassen van versleuteling op mobiele gegevensdragers, zoals laptops en USB-sticks, of het implementeren van twee- of multifactor authenticatie (MFA) op mailaccounts of applicaties.

AUTORITEIT
PERSOONSGEGEVENS

11. Verzenden

Is dit een voorlopige of een definitieve melding?

- ○ Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig
- ○ Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

Bent u nog bezig met onderzoek om de aard en omvang van de inbreuk vast te stellen? Dan vraagt de AP u om hier "nee" in te vullen en binnen 4 weken een vervolgmelding te doen waarin u de AP op de hoogte brengt van de voortgang of uitkomst van het onderzoek.

Datum vervolgmelding later dan 4 weken:
Geef aan wanneer u (uiterlijk) een vervolgmelding doet.
[datumveld]

De AP vraagt u binnen 4 weken na de eerste melding een vervolgmelding te doen waarin u een update geeft over de stand van zaken. Mocht u langer dan 4 weken nodig hebben, dan moet u dit motiveren.

Heeft de AP binnen 4 weken geen vervolgmelding ontvangen? Dan kan de AP contact met u opnemen. Doet u geen definitieve melding, dan kan u niet (volledig) aan uw meldplicht op grond van artikel 33 AVG hebben voldaan. De AP kan dan een nader onderzoek instellen.

- ☐ Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen.
- ☐ Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie

Privacyverklaring

- ☐ Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

EINDE FORMULIER

Ontvangstbevestiging

Uw verzoek tot het aanpassen van een melding is succesvol verstuurd. Als uw verzoek niet meteen kan worden verwerkt, bijvoorbeeld omdat het meldingsnummer dat u heeft opgegeven niet bekend is bij de Autoriteit Persoonsgegevens, dan ontvangt u daarover zo spoedig mogelijk bericht.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	17-11-2020 12:45:19

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een ingediende melding aanpassen
Wat is het meldingsnummer van de oorspronkelijke melding?	art.5.1-2e
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

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

In welke sector is de organisatie of het bedrijf actief?	Openbaar bestuur - Provincie

Wie meldt het datalek?

Naam	art.5.1-2e
Functie	Tactisch Specialist Informatieveiligheid
E-mailadres	art.5.1-2e)p zh.nl
Telefoonnummer	art.5.1-2e

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

De melder is contactpersoon	Ja

1.2 Betrokkenheid andere organisatie

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

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

Hostingpartij

2. Tijdlijn

Einddatum van de periode waarbinnen de inbreuk was	23-10-2020
Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	23-10-2020

3. Gegevens over het datalek

3.1 Aard van de inbreuk

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

3.2 Aard van het incident

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

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

De website www.relevant.nl bevat geen (gevoelige) bedrijfsinformatie. De bots hebben echter wel onbevoegd toegang verkregen tot het adressenboek behorend bij de website waarbij mogelijk een kopie

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

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

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke	Nee

overtuigingen blijken	
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

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

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

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

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

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

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

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

7. Gevolgen van het datalek

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

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

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

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

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Nee
Financiële verliezen	Nee
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

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

Wat is de inhoud van de melding aan de betrokkenen?

informatie over de situatie, te nemen maatregelen, wat zij zelf kunnen doen.

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

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
De Wie-is-wie is direct offline gezet en het registratieportaal voor de website is gesloten. - Het besloten gedeelte van Relevant (projectruimtes) is uit voorzorg offline gehaald, in afwachting van verder onderzoek. - Het openbare gedeelte van de website blijft online, omdat er op dit moment geen aanwijzingen zijn voor onwenselijke inmenging van derden. - De nepaccounts zijn verwijderd uit de gebruikerslijst (toegang is ontzegd). - Communicatie richting betrokkenen. - Verdere kwetsbaarheden op de website www.relevant.nl worden onderzocht middels een pentest. Uitkomt van de pentest stelt ons in staat om inzicht te verkrijgen in de aanwezige risico's, waarna het mogelijk is om tot verdere maatregelen te komen. - Afsluiten verwerkersovereenkomst - Publiceren privacyverklaring - Beoordeling grondslag

8.3 Internationale aspecten

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

9. Overig

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

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	art.5.1-2e
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Eenheid Audit en Advies
Kostenplaatscode	227

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	In de Recruitment Software; Ubeeo, krijg ik van een kandidaat te zien dat deze interesse heeft in meerdere functies bij meerdere organisatieonderdelen. Ik kan zien dat een kandidaat niet alleen interesse heeft voor een functie bij mijn eigen eenheid maar ook voor een functie bij een andere eenheid. De interesse van de sollicitant bij de andere eenheid had ik niet mogen zien. Dat is gênant.
Wat voor soort incident heeft er plaats gevonden?	Iemand kan bestanden inzien zonder de juiste rechten
Wanneer vond de inbreuk plaats? Indien bekend	4 augustus 2022 12:36
Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☐

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☑
Telefoonnummers	☑

E-mailadressen of andere adressen voor digitale communicatie	☑
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☐
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	Een collega bij de provincie bij afdeling P&O
Schatting van het aantal personen betrokken bij het datalek: minimaal	4
Schatting van het aantal personen betrokken bij het datalek: maximaal	4

Van: art.5.1-2e
Verzonden: 2023-10-03 22:56:43+00:00
Aan: art.5.1-2e art.5.1-2e
CC:
Onderwerp: verstuurde versie
"
Dag art.5.1-2e en art.5.1-2e

Dank voor jullie bijdragen aan het advies.

Bijgaand het advies zoals hij er uiteindelijk uit is gegaan naar art.5.1-2e

Met vriendelijke groet,

art.5.1-2e art.5.1-2e

Functionaris voor Gegevensbescherming

Gerechtelijk Deskundige

M art.5.1-2e

E art.5.1-2e pzh.nl

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art.5.1-2e art.5.1-2e 40pzh.nl
%7Cb649cfa95113434abffc08dbc4533fe3%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638319634047846995%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=ZiospSKDjqm1qBVWY0QGBDXG5tXqotH1qS3s3bFr7QE
%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Krachtig Zuid-Holland.
"

provincie Zuid-Holland

Memo

Contact
art.5.1-2e
T art.5.1-2e
art.5.1-2e@pzh.nl

Datum
3 oktober 2023

Aan
Concerndirecteur PZH art.5.1-2e

Kopie aan

Onderwerp
Advies melding datalek aan AP en aan betrokkenen

Geachte heer van art.5.1-2e

Vraagstelling

Dit memo geeft een advies aan de concerndirecteur ten aanzien van het melden van verschillende geconstateerde inbreuken aan de Autoriteit Persoonsgegevens (AP). De vraag die voorligt is of deze datalekken separaat gemeld moeten worden aan de AP of dat dit in één 'container'-melding kan worden gevangen. Daarnaast speelt de vraag of en wanneer betrokkenen moeten worden geïnformeerd.

Dit advies is met name juridisch ingestoken. Een bestuurlijke afweging moet gemaakt worden door het DT.

Wat is er aan de hand?

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

Tijdens het onderzoek naar het gemelde datalek (7/9) zijn meerdere inbreuken geconstateerd, zowel met handmatige acties door de FG en de Eenheid Privacy als bij geautomatiseerde zoekslagen door de functioneel beheerders van iDMS in samenwerking met het BI-team van I&A. Eén datalek, met drie zoektermen, is aan de Autoriteit Persoonsgegevens (AP) gemeld op 8 september 2023.

De FG heeft de concerndirecteur per brief van 21 september jl. geïnformeerd over de resultaten van een onderzoek dat hij heeft laten doen naar de toegankelijkheid van persoonsgegevens en bijzondere persoonsgegevens voor medewerkers die deze gegevens niet nodig hebben voor de uitoefening van hun functie. Uit dit onderzoek

bleek dat er naar alle waarschijnlijkheid een groot aantal documenten toegankelijk is voor onbevoegde medewerkers.

Constatering FG
Gelet op het onderstaande juridische kader (ook gelezen in samenhang met hetgeen in het laatste overleg in de stuurgroep is besproken) constateert de FG dat er geen valide grondslag is en geen gegronde redenen zijn om de opgemerkte overtredingen van de AVG niet komende donderdag in één keer te melden aan de AP. We moeten inbreuken melden en de oorzaak van de inbreuken is van dezelfde aard, alleen de (toevallige) zoektermen zijn anders.

Voor wat betreft het informeren van betrokkenen adviseert de FG nader in overleg te gaan met de AP. Overweging 86 AVG[1] geeft de provincie enige ruimte om betrokkenen eventueel op een later tijdstip te informeren. Contactpersoon voor de AP is bij wet geregeld, zijnde de FG van PZH.

Uiteraard ben ik bereid om u mondeling of schriftelijk nader te informeren.

art.5.1-2e
Functionaris voor Gegevensbescherming
Provincie Zuid-Holland

[1] (86) De verwerkingsverantwoordelijke moet de betrokkene zonder onredelijke vertraging in kennis stellen van de inbreuk in verband met persoonsgegevens wanneer die inbreuk in verband met persoonsgegevens grote risico's voor de rechten en vrijheden van de natuurlijke persoon met zich kan brengen, zodat hij de nodige voorzorgsmaatregelen kan treffen.
De kennisgeving dient zowel de aard van de inbreuk in verband met persoonsgegevens te vermelden als aanbevelingen over hoe de natuurlijke persoon in kwestie mogelijke negatieve gevolgen kan beperken.
Dergelijke kennisgevingen aan betrokkenen dienen zo snel als redelijkerwijs mogelijk te worden gedaan, in nauwe samenwerking met de toezichthoudende autoriteit en met inachtneming van de door haarzelf of door andere relevante autoriteiten, zoals rechtshandhavingsautoriteiten, aangereikte richtsnoeren.

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

Bijlage: Juridische kaders

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

<u>Definitie datalek:</u>
Artikel 4 AVG: Definities
12) „inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

De hierboven beschreven inbreuken zien met name op de ongeoorloofde verstrekking of ongeoorloofde toegang tot (in de oorspronkelijke wettekst unauthorised disclosure of, or access to) persoonsgegevens.

Melden aan betrokkenen
Artikel 34 AVG: Mededeling van een inbreuk in verband met de persoonsgegevens aan de betrokkene
lid 1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkenen de inbreuk in verband met persoonsgegevens onverwijld mee.
a. inbreuk in verband met persoonsgegevens: de AVG kent de term datalek niet, de juiste juridische terminologie hiervoor is inbreuk in verband met persoonsgegevens;
b. hoog risico: in het datalek van 7 september zijn een groot aantal identiteitsbewijzen naar boven gekomen, waaronder paspoorten, maar ook creditcardgegevens. Identiteitsbewijzen worden gezien als een hoog risico, gelet op de mogelijkheden om hiermee identiteitsfraude te plegen;
c. onverwijld: de melding moet onverwijld, althans zonder onnodige vertraging, worden gedaan, dat wil zeggen: zo snel als redelijk mogelijk. Zo zouden betrokkenen

bijvoorbeeld onverwijld in kennis moeten worden gesteld wanneer een onmiddellijk risico op schade moet worden beperkt, terwijl een langere kennisgevingstermijn gerechtvaardigd kan zijn wanneer passende maatregelen moeten worden genomen tegen aanhoudende of soortgelijke inbreuken in verband met persoonsgegevens).... Dergelijke kennisgevingen aan betrokkenen dienen zo snel als redelijkerwijs mogelijk te worden gedaan, in nauwe samenwerking met de toezichthoudende autoriteit...(overweging 86 AVG)

provincie Zuid-Holland

Van: art.5.1-2e
Verzonden: 2023-07-07 13:58:00.778000+00:00
Aan: art.5.1-2e
CC: art.5.1-2e
Onderwerp: Datalek bij aannemer van DBI
"
Hallo art.5.1-2e

CC. art.5.1-2e

Afgelopen week kregen wij van de IV-groep, een ingenieursbureau dat voor DBI heeft gewerkt, een melding van een datalek.

Het betrof een onvoldoende beveiligde server die benaderbaar was via internet.

Dit euvel is door een externe beveiligingsonderzoeker (ethische hacker) geconstateerd.

Er is op dit moment geen aanwijzing of er daadwerkelijk door onbevoegden, anders dan de ethisch hacker, toegang is geweest tot de server.

Wel is bekend dat op de server van de IV-groep een groot aantal persoonsgegevens stond.

Het betreffen waarschijnlijk de NAW-gegevens van ongeveer 700 aanwonenden aan de provinciale weg N468 bij Schipluiden.

Deze lijst was (het project is inmiddels beÃ«indigd) nodig om de bewoners te kunnen aanschrijven tijdens de werkzaamheden aan/op de weg.

De provincie Zuid-Holland is als initiatiefnemer van de werkzaamheden verantwoordelijk voor het verwerken en dus ook het beschermen van de persoonsgegevens.

Dit datalek wordt inmiddels verder onderzocht.

Er staan nog veel vragen open.

Wel is i.v.m. met de wettelijke verplichting, om een datalek met een verhoogd risico binnen 72 uur te melden bij de Autoriteit persoonsgegevens (AP), een voorlopige melding gedaan bij de AP.

Deze voorlopige melding geeft de provincie meer tijd om het datalek beter te onderzoek en eventuele vervolgacties te ondernemen.

Op dit moment wordt dit datalek dermate serieus ingeschat dat de 700 aanwonenden dienen te worden geÃ¯nformeerd.

Binnen een maand willen we dit datalek verder afronden en zal een definitief rapport worden opgemaakt, dat met jou en de nieuwe gedeputeerde zal worden gedeeld.

Deze mail was een vooraankondiging.

Vriendelijke groet,

art.5.1-2e

TeamcoÃ¶rdinator/Privacy Officer

Eenheid Privacy

T art.5.1-2e Mail art.5.1-2e pzh.nl
<mailto: art.5.1-2e pzh.nl>

"


provincie
Zuid-Holland

art.5.1-2e

15 september 2022 09:04

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

- Dinsdag 13 september heb ik een mail verstuurd naar de leden van de Erfgoedtafel Oude Hollandse Waterlinie. De geadresseerden (ongeveer 60) heb ik per ongeluk niet in de BCC, maar in de CC gezet. Dit betekent dat de geadresseerden elkaars e-mailadressen hebben kunnen zien. De inhoud van de mail betrof een uitnodiging voor een bijeenkomst en was qua inhoud dus niet gevoelig. De partijen die de mail hebben gehad kennen elkaar allemaal en ze treffen elkaar regelmatig bij bijeenkomsten van de Erfgoedtafel. In die zin was er wat mij betreft dus ook geen sprake van gevoelige informatie. Ik heb direct de IC_helpdesk geraadpleegd en die hebben samen met mij de mail ingetrokken, maar dit is voor zover ik hebben kunnen nagaan niet overal gelukt.

Binnen ons erfgoedbeleid richten wij ons op zeven erfgoedlijnen. Voorbeelden hiervan zijn de Atlantikwall, de Landgoederenzone en de Oude Hollandse Waterlinie. Rondom elk van deze erfgoedlijnen is een netwerk geformeerd met belanghebbenden zoals gemeenten, musea, historische verenigingen en ondernemers. Elke erfgoedlijn heeft een provinciale projectleider die o.a. de erfgoedtafels voorbereid, partijen uitnodigt en hij/zij is in feite aanspreekpunt namens de provincie. Vanuit die rol heb ik de betreffende mail verstuurd en normaalgesproken zet ik de geadresseerden dus in de BCC. Dat ging nu mis.

Wat voor soort incident heeft er plaats gevonden?
- Anders

Anders? Graag toelichten
- Meerdere mailadressen niet in BCC maar CC geplaatst. Nu kan iedereen elkaars mailadres zien.

Wanneer vond de inbreuk plaats? Indien bekend
- 13 september 2022 11:51

Wanneer vond de inbreuk plaats? Indien niet bekend
-

Lezen (vertrouwelijkheid)
- Ja

Kopiëren
- Nee

Veranderen (integriteit)
- Nee

Verwijderen of vernietigen (beschikbaarheid)
- Nee

Diefstal
- Nee

(Nog) niet bekend
- Nee

Naam-, adres- en woonplaatsgegevens
- Nee

Telefoonnummers
- Nee

E-mailadressen of andere adressen voor digitale communicatie
- Ja

Toegangs- of identificatiegegevens

- Nee

Financiële gegevens
- Nee

Burgerservicenummer (BSN) of andere persoonsidentificatienummers
- Nee

Kopieën van identificatie- en legitimatiebewijzen
- Nee

Geslacht, geboortedatum en/of leeftijd
- Nee

Bijzondere persoonsgegevens
- Nee

Andere gevoelige persoonsgegevens
- Nee

Anders, namelijk
- Nee

Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)
- Leden van de Erfgoedtafel Oude Hollandse Waterlinie

Schatting van het aantal personen betrokken bij het datalek: minimaal
- 66

Schatting van het aantal personen betrokken bij het datalek: maximaal
- 66

Ontvangstbevestiging

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

Tijdstip ontvangst	18-09-2019 15:07:58
Uniek nummer	art.5.1-2e

0. Over deze melding

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

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Naam van het bedrijf of de organisatie	Provincie Zuid-Holland

intern geëigende weg om te melden is gevolgd.

3. Gegevens over het datalek

3.1 Aard van de inbreuk

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

3.2 Aard van het incident

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

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Een provinciale medewerker heeft gemeld dat hij in het digitale Loket 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.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Ja

("gegevensregisters") zijn getroffen
door de inbreuk

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

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

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Het betreft (voormalige) statenleden en fractiemedewerkers.

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	42
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	42

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

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

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

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

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Ja
Financiële verliezen	Ja
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee
Andere gevolgen, namelijk:	

Toelichting: De betreffende persoonsgegevens kunnen leiden tot identiteitsdiefstal . In dit geval wordt het risico kleiner ingeschat, aangezien de gegevens niet zichtbaar zijn geweest voor externen, maar alleen voor provinciale medewerkers. Vandaar dat hierna 'Beperkt' is ingevuld.

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Ja

meer andere EU-landen, of gaat u dat nog doen?	
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?	Nee

9. Overig

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

AUTORITEIT PERSOONSGEGEVENS

Meldloket

Ontvangstbevestiging

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

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

  Tijdstip ontvangst
  03-04-2019 10:51:11
  Uniek nummer
  art.5.1-2e

---

0. Over deze melding

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

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

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

Wie meldt het datalek?

Naam
art.5.1-2e
Functie
Adviseur informatieveiligheid
E-mailadres
art.5.1-2e pzh.nl
Telefoonnummer
art.5.1-2e
onnummer
art.5.1-2e

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

De melder is contactpersoon
Ja

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?
Nee

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend
09-04-2008
Startdatum van de periode waarbinnen de inbreuk was
09-04-2008
Einddatum van de periode waarbinnen de inbreuk was
01-04-2019
Duurt de inbreuk op dit moment nog voort?
Nee
Wanneer werd de inbreuk ontdekt?
01-04-2019

3. Gegevens over het datalek

3.1 Aard van de inbreuk

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

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?
Overig
Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest
Betreft een e-mail van betrokkene aan de provincie die in 2008 als ingezonden stuk in het Staten Informatie Systeem is gepubliceerd en daarmee publiek toegankelijk is geworden. De e-mail bevat e-mailadres, naam, adres en telefoonnummer van betrokkene.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

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

Nee

4.2 Bijzondere categorieën van persoonsgegevens

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

4.3 Hoeveelheid persoonsgegevens

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

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

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

Nee
Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
Betrokkene heeft in 2008 een e-mail als ingezonden stuk aan de provincie gestuurd.
Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
1
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
1

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

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

7. Gevolgen van het datalek

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

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

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

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

Discriminatie
Nee
Identiteitsdiefstal of -fraude
Nee
Financiële verliezen
Nee
Reputatieschade
Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens
Nee
Ongeoorloofde ongedaanmaking van pseudonimisering
Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen
Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen
Nee
Andere gevolgen, namelijk:
Op basis van contactgegevens, zou betrokkene benaderd kunnen worden. Het is ons niet bekend of dit daadwerkelijk is gebeurd. Betrokkene heeft aangegeven inmiddels een ander e-mailadres te hebben. Betrokkene ervaart de situatie als een forse inbreuk op zijn privéleven.
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen
1. Verwaarloosbaar

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?
Ja
Wanneer heeft u het datalek gemeld aan de betrokkenen?
01-04-2019
Wat is de inhoud van de melding aan de betrokkenen?
Betrokkene heeft zelf op 01-04-2019 contact opgenomen met de FG van de provincie . Daarna is er contact geweest over de afhandeling.
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?
1

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?
telefoon

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
De betrokkene is op 2 april 2019 geïnformeerd dat de e-mail uit het Staten Informatie Systeem is verwijderd. De functionaris gegevensbescherming heeft betrokkene geinformeerd dat melding bij de Autoriteit Persoonsgegevens gedaan wordt.

8.3 Internationale aspecten

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

9. Overig

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

---

Ontvangstbevestiging

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

Tijdstip ontvangst	21-06-2019 13:02:20
Uniek nummer	art.5.1-2e

0. Over deze melding

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

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Naam van het bedrijf of de organisatie	Provincie Zuid-Holland

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

Wie meldt het datalek?

Naam	art.5.1-2e
Functie	Adviseur informatieveiligheid
E-mailadres	art.5.1-2e @pzh.nl
Telefoonnummer	art.5.1-2e
Tweede telefoonnummer	art.5.1-2e

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

De melder is contactpersoon	Nee
Naam contactpersoon	art.5.1-2e
Functie contactpersoon	Functionaris gegevensbescherming
E-mailadres contactpersoon	art.5.1-2e @pzh.nl
Telefoonnummer contactpersoon	art.5.1-2e

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Nee

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	10-05-2019
Startdatum van de periode waarbinnen de inbreuk was	14-12-2018
Einddatum van de periode waarbinnen de inbreuk was	13-05-2019
Duurt de inbreuk op dit moment nog voort?	Nee

Wanneer werd de inbreuk ontdekt?	10-05-2019
Als u de inbreuk later meldt dan 72 uur na de ontdekking, wat is daarvan dan de reden?	Na de eerste constatering is onderzoek gestart, zijn audit logs geanalyseerd en zijn gesprekken tussen leidinggevenden en medewerkers ingepland. Dit heeft enige tijd in beslag genomen.

3. Gegevens over het datalek

3.1 Aard van de inbreuk

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

3.2 Aard van het incident

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

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

In een beperkt toegankelijk e-dossier in het documentaire informatiesysteem bevond zich een document dat niet afgeschermd was. Door de rechtenbeperking op het betreffende e-dossier verschijnt het dossier alleen bij geautoriseerde medewerkers. Alleen door via de zoekfunctionaliteit in het systeem gericht op trefwoorden te zoeken, kon het document met de ruimere toegangsrechten toch door anderen worden gevonden. Daardoor hebben twee provinciale ambtenaren de mogelijkheid

gehad om kennis te nemen van een document waarin zich persoonsgegevens bevinden.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Nee
Burgerservicenummer (BSN)	Nee
Contactgegevens	Ja
Toegangs- of identificatiegegevens	Nee
Financiële gegevens	Nee
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee
Onbekend / anders, namelijk:	Informatie over het functioneren van ambtenaren in het dossier.

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
	Nee

Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	15

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

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

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Ambtenaren van de Provincie Zuid-Holland

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	15

15

Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

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

Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?
Door de rechtenbeperking op het betreffende e-dossier verschijnt het dossier alleen bij geautoriseerde medewerkers. Alleen door via de zoekfunctionaliteit in het systeem gericht op trefwoorden te zoeken, kon het document met de ruimere toegangsrechten toch door anderen worden gevonden.

7. Gevolgen van het datalek

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

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Nee
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee

Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

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

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Nee
Financiële verliezen	Nee
Reputatieschade	Ja
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee

Andere gevolgen, namelijk:

Het document bevat onder meer informatie over het optreden van collega's in een dossier. Of daadwerkelijk kennis is genomen van deze informatie in

het document is niet uit te sluiten. De kans dat dit is gebeurd én leidt tot schade bij betrokkenen, wordt als beperkt ingeschat.

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Nee
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	0
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	0
Waarom ziet u af van het melden van het datalek aan de betrokkenen?	Ik heb na het datalek maatregelen getroffen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkenen

Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?

De toegangsrechten zijn direct gecorrigeerd. Slechts twee ambtenaren hebben kennis kunnen nemen van het document waarin onder meer informatie staat over het optreden van collega's in een dossier. Ze zijn hier op aangesproken door hun leidinggevenden.

Welke andere redenen heeft u om de betrokkenen niet te informeren?

Of daadwerkelijk kennis is genomen van deze informatie in het document is niet uit te sluiten. Het document is niet verder met anderen binnen of buiten de organisatie gedeeld. De kans dat het bekend zijn van de persoonsgegevens leidt tot schade bij betrokkenen, wordt als beperkt ingeschat.

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
De toegangsrechten op het dossier zijn direct na constateren van het beveiligingsincident gecorrigeerd. De medewerkers hebben een gesprek gehad met hun bureauhoofd. Periodieke controles worden ingericht op correcte rechtenstructuur. In de bewustwordingscampagne wordt op dit moment specifieke aandacht geschonken aan de AVG en omgang met persoonsgegevens.

8.3 Internationale aspecten

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

9. Overig

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

"Van: art.5.1-2e
Verzonden: 2020-05-29 13:13:13+00:00
"Aan: art.5.1-2e
"CC: Zoete - van der Hout, WH, de; art.5.1-2e art.5.1-2e
Onderwerp: Melding bij Autoriteit Persoonsgegevens gereed
"
Hallo art.5.1-2e

Ik heb zojuist de melding aan de Autoriteit Persoonsgegevens gedaan:

Tijdstip ontvangst 29-05-2020 13:06:26

Uniek nummer art.5.1-2e

De verdere afhandeling vindt plaats hieronder zoals door art.5.1-2egeschetst.

Mocht je nog vragen hebben, dan hoor ik dat uiteraard graag.

Met vriendelijke groet,

art.5.1-2e

Van: art.5.1-2e <art.5.1-2e pzh.nl>
Verzonden: vrijdag 29 mei 2020 10:59
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>
Onderwerp: RE: Advies aan concerndirecteur in het kader van de meldplicht datalekken
Gevoeligheid: Vertrouwelijk

Dag art.5.1-2e

Terechte vragen!

Gelukkig is daar al op voorgesorteerd.

Er is een groepje medewerkers, onder leiding van art.5.1-2e met GSO n DBI, hier al sinds de ontdekking mee bezig geweest. Zij hebben oo art.5.1-2e geïnformeerd met het verzoek de betreffende gedeputeerde op de hoogte te houden.

De advocaat van betrokkene wordt ook regelmatig geïnformeerd door de advocaat van Pels Rijcken die namens de provincie op dit dossier zit.

Het voorstel aan Hennie vanuit die groep is om binnenkort een excuusbrief naar de betrokkene te sturen.

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 29 mei 2020 10:50
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> >; art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; Gaarden, TNF, van der art.5.1-2e pzh.nl <mailt o art.5.1-2e pzh.nl> >
Onderwerp: RE: Advies aan concerndirecteur in het kader van de meldplicht datalekken
Gevoeligheid: Vertrouwelijk

Helder, ik volg het advies.

Ik vind dit wel een dingetje… Twee aanvullende zaken:

* Normaliter zou de getroffene geïnformeerd moeten worden, maar die weet er al van begrijp ik omdat de advocaat in het verweer is gekomen. Ik mag toch aannemen dat er goed met de advocaat wordt gecommuniceerd, maar mogelijk moet dat (ook) vanuit de inhoudelijke medewerkers ipv alleen vanuit datalek-perspectief. Mag ik daar een reactie op.
* Vanuit de inhoud lijkt me dat dit moet worden opgeschaald. Is het betreffende management op de hoogte van deze misser? Dan kan mogelijk ook de bestuurder geïnformeerd worden. Ik hoor graag terug hierover.

Hartelijke groet, art.5.1-2e

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Verzonden: vrijdag 29 mei 2020 10:28
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 <m nl> >; art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e art.5.1-2e pzh.nl <mailt o art.5.1-2e pzh.nl> >
Onderwerp: Advies aan concerndirect an de meldplicht datalekken
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste art.5.1-2e

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

Het advies is afgestemd met onze FG en met Tessa van der Gaarden. art.5.1-2e is bij de afhandeling betrokken als privacy officer van DBI.

Zoals gebruikelijk is het datalek geregistreerd in onze provinciale administratie.

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

Ik hoor graag of je hiermee instemt.

Met vriendelijke groet,

art.5.1-2e

Van: art.5.1-2e

Verzonden: donderdag 28 mei 2020 17:15
Aan: art.5.1-2e <art.5.1-2epzh.nl <mailto :art.5.1-2epzh.nl> >
CC: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl <mailto:wh.de.zoete@pzh.nl>
>; art.5.1-2e <art.5.1-2epzh.nl <mailto :art.5.1-2epzh.nl> >
Onderwerp: Datalek in behandeling

Hallo art.5.1-2e

Het Privacyteam heeft een datalek in behandeling.

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

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

Hier wordt actie op ondernomen.

Het adviesrapport volgt morgenochtend.

Met vriendelijke groet,

art.5.1-2e

Adviseur informatieveiligheid

Afdeling Informatisering & Automatisering

T art.5.1-2e | M art.5.1-2e

art.5.1-2epzh.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

Van: loket@pzh.nl
Verzonden: 2023-03-17 13:17:07+00:00
Aan: art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e privacy
CC:
Onderwerp: Melding mogelijk datalek A 97859
"

Beste collega,

Er is een melding gedaan van een mogelijk datalek:

Zie voor meer informatie:
Activiteitnummer: A 97859
Wijzigingsnummer: W23 03 00217

Hier kan je de activiteit <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fpvzh.topdesk.net%2Ftas%2Fsecure%2Fcontained%2Fchangeactivity%3Funid%3Da7bc42af0fbd4b4ea7cbb898fa5b2797&data=05%7C01% art.5.1-2e art.5.1-2e 40pzh.nl%7C89c7287f3b4d4fb9f84408db26e18723%7C6d99bc288f284a73a50 8e1eb3040%7C0%7C0%7C638146522292363179%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=b8bwC1NVAUn%2BfBNiOSPdqxWok20BXFKUDqVm9dipJwg%3D&reserved=0> bekijken.

Met vriendelijke groet,

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

Het Loket telefoon 070 4417777 pvzh.topdesk.net
<https://eur03.safelinks.protection.o ook.com/?url=https%3A%2F%2Fpvzh.topdesk.net%2F&data=05%7C01% art.5.1-2e art.5.1-2e 40pzh.nl%7C89c7287f3b4d4fb9f84408db26e18723%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638146522292363179%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=yPru%2BNLaFiWRDg9v02b7B3AY2e6nGZvp%2FWhZRomXz8Y%3D&reserved=0> "

Van: art.5.1-2e
Verzonden: 2023-07-28 14:23:18.347000+00:00
Aan: art.5.1-2e art.5.1-2e
CC: Frank Rijkaart; art.5.1-2e
Onderwerp: Datalek bij Servicedesk.
"
Hallo art.5.1-2e en bij afwezighei d art.5.1-2e

cc. Gedeputeerde Rijkaart. Ter info.

cc. Functionaris voor gegevensbescherming, art.5.1-2e

Een nieuwe medewerker van de PZH constateerde dat zijn telefoonnummer en andere privé persoonsgegevens in een openbare iDMS-map stond van de Servicedesk.

Het betrof zijn eigen Keuzeformulier ICT-middelen die hij had ingevuld bij zijn indiensttreding.

In het formulier stond zijn privé NAW-gegevens, privé telefoonnummer, privé mailadres en handtekening.

Dit is onder de AVG een datalek.

Bij onderzoek door de Eenheid Privacy is daarnaast ook het volgende gebleken:

* Het formulier staat in een voor alle medewerkers toegankelijke IDMS-map.
* Bijna 400 formulieren staan opgenomen in deze iDMS-map, over een periode van meerdere jaren.
* De iDMS-map staat vol met privé persoonsgegevens van vele medewerkers van de PZH, Statenleden, Gedeputeerden en politici.
* Veel formulieren bevatten handtekeningen. Die vallen, onder de categorie bijzondere persoonsgegevens.
* Deze formulieren zijn na uitgifte van ICT-middelen in deze hoedanigheid niet meer nodig en dienen te worden gewist, hetgeen niet is gebeurd.
* In de formulieren is richting de aanvrager niet aangegeven hoelang de Servicedesk deze gegevens bewaart. De ontvanger van de ICT-middelen weet nu niet waar hij aan toe is.
* De verwerking is niet opgenomen in het verwerkingsregister van de PZH. Dit dient alsnog te gebeuren.

Vanwege de ernst van het datalek is hiervan een melding gedaan bij de Autoriteit Persoonsgegevens.

De eerste beperkende maatregel, het beperken van de toegang van de iDMS-map, is al genomen.

Overige herstel- en verbeteracties, waaronder het informeren van de betrokkene worden de komende tijd uitgevoerd.

Ik hoop je voldoende te hebben geïnformeerd.

Vriendelijke groet,

art.5.1-2e

Teamcoördinator/Privacy Officer

Eenheid Privacy

T art.5.1-2e Mail art.5.1-2e pzh.nl
<mailto: art.5.1-2e pzh.nl>

"

Advies aan de concerndirecteur in het kader van de meldplicht datalekken

Melding gegevens

Aangemeld door	:	art.5.1-2e Opdrachtgeverseenheid)
Registratienummer van het incident	:	M23 07 02766
Datum en tijdstip van de melding	:	26-07-2023, 16.45
Route van de melding	:	TopDesk - melding Datalek

Advies

Opgesteld door	:	art.5.1-2e (Eenheid Privacy)
Datum en tijdstip advies	:	27 juli 2023 om 12.00 uur
Advies besproken met	:	art.5.1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Gedeeld met eenheid Privacy

Situatie

Een nieuwe medewerker van de PZH constateerde dat zijn telefoonnummer in een openbare map van de Servicedesk in het iDMS stond. Het betrof zijn eigen invulling van het Keuzeformulier ICT-middelen. Deze had hij ingevuld bij zijn indiensttreding. In het formulier stond zijn privé telefoonnummer en privé emailadres.

Bij onderzoek door de Eenheid Privacy is daarnaast ook het volgende gebleken:

Het formulier staat in een voor alle medewerkers toegankelijke IDMS-map van de Servicedesk waarin bijna 400 formulieren staan opgenomen over een periode van meerdere jaren.

De IDMS-map staat vol met privé persoonsgegevens van vele medewerkers van de PZH, van Statenleden, van gedeputeerden en van politici buiten het politieke circuit van de provincie Zuid-Holland.

Veel formulieren bevatten handtekeningen. De handtekeningen in de formulieren vallen als biometrische gegevens onder bijzondere persoonsgegevens waarvoor extra zorgvuldigheid vereist is i.v.m. de mogelijkheid om te kunnen frauderen.

Deze formulieren zijn na uitgifte van ICT-middelen in deze hoedanigheid niet meer nodig en dienen gewist te worden. De benodigde gegevens die wel langer bewaard dienen te worden kunnen uit de formulieren worden overgenomen in een ander document/database.

In de formulieren is niet aangegeven hoelang de Servicedesk deze gegevens bewaart. Dit is onder de AVG wel verplicht. De ontvanger van de ICT-middelen weet nu niet waar hij aan toe is.

De verwerking is niet opgenomen in het verwerkingsregister van de PZH. Dit hoort wel alsnog te gebeuren.

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 IDMS-map staan zeer bijna 400 keuzeformulieren-ICT van medewerkers van de PZH. Na een steekproef wordt aangenomen dat van ongeveer 90% van de formulieren privé gegevens staan. Voorbeelden: Naam, adres, woonplaats, mailadres, telefoonnummer, handtekening.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	Onbekend.
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Alle medewerkers van de PZH hebben toegang tot de IDMS-map en kunnen de persoonsgegevens in de formulieren inzien. Alle hiernaast opgesomde verwerkingen zijn mogelijk. Daarnaast kunnen de persoonsgegevens ook gedeeld worden met derden via b.v. de mail.
Welke persoonsgegevens betreft het?	Privé persoonsgegevens. Naam, adres, woonplaats, mailadres, telefoonnummer, handtekening.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Ja. Een groot deel van de formulieren bevat een handtekening. Daarnaast is soms te herleiden aan welke politieke partij de ICT middelen zijn verstrekt en wie de aanvrager voor die politieke partij was. Lidmaatschap van een politieke partij is een bijzonder persoonsgegeven.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja. iDMS is niet toegankelijk voor niet-PZH-personeel.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Mogelijk. Niet bekend.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Ja.
Betreft het een datalek?	Ja.
Ondernomen beperkende maatregelen.	De map wordt afgeschermd voor algemene toegang.

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

Vraag	Antwoord
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Toewijzen van autorisaties voor toegang tot de iDMS-map van de Servicedesk door alleen bevoegden. Instructie bij de Servicedesk voor het niet meer bewaren van de persoonsgegevens indien ze niet meer nodig zijn. Verwerking alsnog opnemen in het verwerkingsregister. Onderaan het formulier dient opgenomen te zijn hoelang deze persoonsgegevens worden bewaard en wanneer ze worden vernietigd. De betrokkenen worden geïnformeerd.

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

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

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

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

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

Analyse van dit specifieke geval

Er is geen structurele autorisatie-instellingen bij de Servicedesk.
In het formulier ontbreekt een zin waarin de invuller duidelijk wordt waarvoor en hoelang deze persoonsgegevens worden bewaard.
De verwerking is niet opgenomen in het verwerkingsregister.
Er ontbreekt een instructie binnen de Servicedesk hoe deze gegevens moeten worden gewist.

Conclusie en advies

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

- Er is wel sprake van een datalek in de zin van de AVG.
- Het datalek wordt, gezien de omvang van het lek en het risico op misbruik, WEL gemeld bij de Autoriteit Persoonsgegevens.
- Compliancy maatregelen worden genomen.
- Betrokkenen worden WEL geïnformeerd.
- De melding en beoordeling worden zoals gebruikelijk geadministreerd in het provinciale logboek.


provincie
Zuid-Holland

Advies aan de griffier in het kader van de meldplicht datalekken

Melding gegevens

Aangemeld door	:	art.5.1-2e
Registratienummer van het incident	:	M23 07 00938
Datum en tijdstip van de melding	:	6 juli 2023
Route van de melding	:	Persoonlijk

Advies

Opgesteld door	:	art.5.1-2e
Datum en tijdstip advies	:	7 juli 2023
Advies besproken met	:	Besproken met art.5.1-2e (FG)
Strekking advies ter kennisgeving gedeeld met	:	Gedeeld met Eenheid Privacy

Situatie

Op 5 juli 2023 om 13:18 uur heeft een lid van de Statenfractie van D66, een mail gestuurd aan diverse Statenleden van overige fracties waarbij de gehele fractie van D66 in de CC is meegenomen.
In de aanhef is naast de acht Statenleden ook per abuis een negende ontvanger opgenomen, te weten art.5.1-2e, medewerker van de provincie Zuid-Holland. De medewerker van de provincie Zuid-Holland had deze mail niet mogen ontvangen.
Het is zeer aannemelijk dat het Statenlid een andere persoon had willen meenemen in de mail dan de betrokken medewerker die de mail ontvangen heeft.
De mail ging inhoudelijk over het percentage van belang (aandeelhouderschap) van diverse bedrijven in elkaar en hoort niet te worden geopenbaard.
De medewerker van de provincie Zuid-Holland heeft de verzender van de mail direct op de hoogte gebracht van haar fout. Het Statenlid wordt nog een tweede maal benaderd met een advies hoe verder te handelen. Dit zal neerkomen op het inlichten van de overige ontvangers van de fout.

Beoordeling van de ernst van de situatie

Vraag	Antwoord
Hoeveel persoonsgegevens zijn raadpleegbaar geweest voor anderen dan de betrokkene(n) (wiens persoonsgegevens het betreft)	E-mail adres van één medewerker van de provincie Zuid-Holland en 19 mailadressen van Statenleden. De mail adressen van de Statenleden zijn openbaar toegankelijke gegevens. Het mailadres van de medewerker van de provincie Zuid-Holland is niet openbaar toegankelijk.
Hoeveel personen hebben daadwerkelijk onterecht toegang gehad tot de persoonsgegevens?	19 Statenleden en 1 medewerker van de provincie Zuid-Holland
Wat is de aard van de inbreuk: (lezen, kopiëren, afdrukken, e-mailen, veranderen, verwijderen)	Lezen.

Vraag	Antwoord
Welke persoonsgegevens betreft het?	E-mailadressen.
Betreft het bijzondere persoonsgegevens[1] zoals bedoeld in artikel 9 AVG?	Nee. De emailadressen van de 19 Statenleden zijn van het type: Voorletter.achternaam@pspzh.nl Het mailadres van de medewerker van de provincie Zuid-Holland is van het type: Voorletter.achternaam@pzh.nl Aan de mailadressen van de Statenleden is niet direct te zien van welke fractie de fractieleden zijn. Aan de mailadressen is daarmee niet direct te zien van welke politieke partij de Statenleden zijn. Bovendien is lidmaatschap van een politieke partij dermate verbonden met de functie van een Statenlid dat het in dit geval niet moet worden beschouwd als een bijzonder gegeven als de medewerker van de Provincie dit kan herleiden naar een politieke partij.
Is de toegang beperkt gebleven tot personeel van PZH? Zo ja, tot welke gebruikersgroepen?	Ja. Één medewerker van de provincie Zuid-Holland heeft per abuis een mail ontvangen van een Statenlid welke bestand was voor overige Statenleden.
Houdt de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen in[2]?	Nee. De Statenleden kunnen elkaar vrij benaderen via het Microsoft adressenboek van de Provinciale Staten. De medewerker van de provincie Zuid-Holland is vertrouwelijk omgegaan met de verkeerd geadresseerde mail.
Betreft het een beveiligingsincident? *Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.*	Nee.
Betreft het een datalek?	Ja.
Ondernomen beperkende maatregelen.	Het Statenlid is geïnformeerd over haar fout in de mailing aan overige Statenleden.
Welke herstel- en verbeteracties moeten nog worden uitgevoerd en door wie?	Vanuit de eenheid Privacy wordt het Statenlid geadviseerd om de overige ontvangers van haar mail te informeren over haar fout.

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

Afweging

Toelichting op het wettelijke kader *(standaard tekst)*

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

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

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

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

Analyse van dit specifieke geval

Een Statenlid heeft abusievelijk een medewerker van de provincie Zuid-Holland meegenomen in de aanhef van een mail die alleen voor Statenleden bedoeld was.
De medewerker van de provincie Zuid-Holland heeft de inhoud van de mail tot zich genomen en realiseerde zich daarna dat de mail niet voor haar bestemd was. De medewerker is hier vertrouwelijk mee om gegaan en heeft dit direct terug gemeld aan de verzender.
Het Statenlid wordt nog geïnformeerd over het informeren van de andere ontvangers van de mail en welke acties ondernomen kunnen worden.

Conclusie en advies

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

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

Van: art.5.1-2e
Verzonden: 2023-10-02 17:03:22+00:00
Aan: art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e
CC:
Onderwerp: memo idms
"
Beste collega’s,

Ik heb van art.5.1-2e de aangepaste bijlagen ontvangen. Ik ga de voorgestelde wijzigingen in de memo doorvoeren en de memo “updaten” naar de stand van zaken van vandaag. Zonder tegenbericht van een van jullie verstuur ik de stukken daarna naar art.5.1-2e. Als er vandaag nog iemand wil meelezen voordat ik de memo verstuur, dan hoor ik dat uiteraard graag.

@art.5.1-2e art.5.1-2e mailto : art.5.1-2e pzh.nl> : ik zie jou aanvulling zoals afgesproken nog tegemoet.

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art.5.1-2e %40pzh.nl%7C0a50bd661db24b5e391808dbc358b8de%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638318558055799942%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=mDONYzPjPo%2FNVQKeeTp4oHpILNYtoRZqOoazqnrjD3U%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

"


provincie
Zuid-Holland

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: art.5.1-2e

Melddatum: 20 juli 2023

Meldtijdstip: 12:41

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	art.5.1-2e

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	art.5.1-2e
Functie	Privacy Officer
E-mailadres	art.5.1-2e @pz h.nl
Telefoonnnummer	art.5.1-2e
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

AUTORITEIT
PERSOONSGEGEVENS

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

[✓] Aantal inbreuken in bulk

[✓] Geselecteerde toezichthouders

2. Grensoverschrijdende inbreuk

[✓] Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

[✓] Gegevens verwerkingsverantwoordelijke

[✓] Gegevens over andere organisaties

4. Tijdlijn

[✓] Tijdlijn

5. Gegevens over de inbreuk

[✓] Aard van de inbreuk

[✓] Aard van het incident

[✓] Samenvatting van het incident

6. Betrokken persoonsgegevens

AUTORITEIT PERSOONSGEGEVENS

[✓] Welke persoonsgegevens

[✓] Hoeveelheid persoonsgegevens

7. Getroffen personen

[✓] Groep mensen dat getroffen is door de inbreuk?

[✓] Nadere omschrijving van de groep mensen dat getroffen is door de inbreuk.

8. Maatregelen vooraf

9. Gevolgen

[✓] Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens

[✓] Gevolgen voor de betrokkene(n) (Persoon of personen van wie gegevens zijn getroffen door de inbreuk)

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

[✓] Maatregelen om de inbreuk aan te pakken?

1 Introductie (vervolg)

Geef het aantal inbreuken aan dat u bij de AP in bulk wilt melden:	1

1.3 Andere toezichthouders

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

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

AUTORITEIT PERSOONSGEGEVENS

3 Uw contactgegevens

3.1 Gegevens verwerkingsverantwoordelijke

KvK-nummer (indien van toepassing)	27375169
Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Provincie

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Ja

Geef aan welke andere organisaties betrokken waren bij de inbreuk?

Naam	Op welke wijze betrokken	Toelichting (optioneel)
ICT-leverancier van IV-Groep	Verwerker	

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	31-3-2023
(Mogelijke) einddatum van de inbreuk	31-3-2023
Wanneer heeft u het datalek voor het eerst aan de AP gemeld?	4-7-2023

AUTORITEIT PERSOONSGEGEVENS

4.2 Wanneer is het incident ontdekt?	31-3-2023
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	De IV-Groep heeft dinsdag 4 juli een melding gedaan aan de Provincie Zuid-Holland. De IVGroep geeft aan dat door hun deze leverancier het volgende is geconstateerd: - het Azure Storage account waarmee de backups van onze Ftp-server werden gemaakt, was niet voldoende beveiligd, waardoor deze benaderbaar was vanaf internet. Deze back-up service is eind 2022 beëindigd. Dit is door een externe beveiligingsonderzoeker (ethische hacker) , aangesloten bij DIVD, geconstateerd. De IV-groep heeft zelf de melding gedaan bij AP op 4 mei 2023. Na verder intern onderzoek bij de IV-groep heeft de IV-groep de melding op 4 juli doorgezet richting de provincie Zuid-Holland, die op zijn beurt binnen 72 een voorlopige melding heeft gedaan bij de AP.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Nee
Wanneer heeft u kennis gekregen van het datalek?	4-7-2023

5 Gegevens over datalek

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

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

[✓] Hacking, malware (bijv. ransomware) en/of phishing

Meerdere opties zijn mogelijk binnen het gearceerde deel.

[✓] Ander type hacking en/of malware

AUTORITEIT PERSOONSGEGEVENS

Heeft u (digitaal forensisch) onderzoek uitgevoerd of laten uitvoeren naar de aard en de omvang van het datalek?	Ja, het onderzoek is afgerond

Optioneel: upload hier de rapportage van het onderzoek naar de inbreuk.

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Iv-Groep is een Nederlands ingenieurs bureau en is werkzaam in diverse marktsegmenten (water, infra, industrie, offshore & energy, bouw). Via één van haar werkmaatschappen zijn er werkzaamheden verricht voor de Provincie Zuid-Holland. Voor het uitwisselen van grote hoeveelheid bestanden is er gebruik gemaakt van een zogenaamde Ftp-server. Deze Ftp server wordt beheerd door één van de ICT-dienstverleners van IV-Groep. Hierop kan via een toegekende gebruikersnaam en wachtwoord toegang tot deze informatie verkregen worden, zowel door Iv-medewerkers als door Provincie Zuid-Holland als opdrachtgever. Door deze ICT-dienstverlener is geconstateerd dat het Azure Storage account waarmee de backups van de Ftp-server werden gemaakt, niet voldoende was beveiligd, waardoor deze benaderbaar was vanaf internet. Dit is geconstateerd door een externe beveiligingsonderzoeker (ethische hacker), aangesloten bij DIVD. Deze back-up service is eind 2022 beëindigd. Er is geen aanwijzing dat er onbevoegde toegang is geweest (anders dan de ethisch hacker). Er is onvoldoende logging beschikbaar om dit met zekerheid vast te stellen.

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

6 Betrokken persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Contactgegevens

[✓] Adres en woonplaats

AUTORITEIT PERSOONSGEGEVENS

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	698
Geef een toelichting op bovengenoemd aantal:	Het betreft een adressenlijst met 698 NAW gegeven van bewoners, gebruikt voor etikettering van een standaard brief.

7 Betrokkenen

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

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Inwoners van de gemeente Midden-Delfland (dorp Schipluiden)
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Aanwonenden van provinciale weg N468 aan wie een brief moest worden gestuurd.

9 Gevolgen

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

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

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

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

AUTORITEIT PERSOONSGEGEVENS

Namelijk:	Betrokkenen kunnen ongewenst worden aangeschreven.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Het betreft NAW gegevens die met minimale inspanning ook op andere manieren verkregen kunnen worden.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

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

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

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

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Na onderzoek heeft de provincie besloten om betrokkenen niet te informeren. De reden hiervoor is dat het onwaarschijnlijk is dat de inbreuk leidt tot een hoog risico voor de betrokkenen. Daarnaast zijn er direct na het datalek maatregelen genomen als bedoeld in artikel 34, lid 3 onder b waardoor eventuele risico's zich niet meer voor kunnen doen. Het is na onderzoek bekend geworden dat een ethisch hacker toegang heeft gehad tot een adressenbestand bestaande uit alleen achternaam, straatnaam en nummer, postcode en woonplaats. De (ethische) hacker was aangesloten bij de DIVD (Dutch Institute for Vulnerability

AUTORITEIT PERSOONSGEGEVENS

Disclosure). Er zijn geen andere gegevens zoals e-mailadressen of telefoonnummers bij betrokken. Het betreft een bestand uit 2010. Het datalek is op 31 maart 2023 ontdekt en diezelfde dag beëindigt. Er zijn geen aanwijzingen dat naast de ethisch hacker nog andere personen toegang hebben gehad, maar dit valt door afwezigheid van logging niet geheel uit te sluiten. Vervolgens is provincie als verwerkingsverantwoordelijke pas op 4 juli in kennis gesteld van het datalek.
De reden waarom de provincie wat later is komt doordat de IV-Groep direct na de constatering op 31 maart is gestart met een eigen intern onderzoek. Hierbij ontdekten zij in eerste instantie alleen gegevens van hun eigen werknemers. Hiervan is door de IV-groep een melding gedaan bij AP op 4 mei 2023. Verder onderzoek is op 4 juli door de IV-groep afgerond. Daarbij is door IV-groep nog een bestand met persoonsgegevens gevonden van een infrastructureel project in Schipluiden. Dat bestand is gebruikt tijdens het groot onderhoud aan de N468. De adreslijst is gebruikt voor aanschrijven en uitnodigen van omwonenden. Na de afronding is de provincie Zuid-Holland geïnformeerd.

Op basis van deze feiten is het onwaarschijnlijk dat de inbreuk een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt (mede gelet op rechtsoverweging 75 en 85 van de AVG). Het gegevensbestand is oud en niet meer actueel. Betrokken personen kunnen om meerdere redenen niet meer op het betreffende adres wonen. Daarnaast zijn adresgegevens op relatief eenvoudige wijze ook op een andere manier te verkrijgen (zoals bijvoorbeeld naambordjes bij een huis). Ook in de EDPB Guidelines (Guidelines 9/2022 on personal data breach notification van 28 maart 2023, nr. 107 op pagina 24) wordt aangegeven dat het onwaarschijnlijk is dat de bekendmaking van de naam en het adres van een persoon in normale omstandigheden aanzienlijke schade zal veroorzaken.

Communicatie aan betrokkenen is bedoeld om deze betrokkenen te helpen om maatregelen te nemen om zich tegen eventuele negatieve gevolgen te beschermen. Gelet op de datum van het bestand, de datum van het datalek en de maatregelen die daarbij zijn genomen en de datum waarop de provincie als verwerkingsverantwoordelijke geïnformeerd is, is het niet meer opportuun om deze betrokkenen nu nog te informeren. Het creëert eerder onnodige onrust, omdat personen geïnformeerd zouden worden over iets waaraan ze nu niets geen maatregelen meer tegen kunnen nemen.

In artikel 34, lid 3, onder b wordt aangegeven dat een inbreuk ook niet aan personen hoeft te worden gemeld (mocht er wel sprake zijn van een hoog risico) als er voldoende maatregelen achteraf zijn genomen. Het datalek is gemeld door een ethisch hacker die deze persoonsgegevens alleen heeft ingezien om het datalek te kunnen melden. Er zijn geen aanwijzingen dat er andere onbevoegde personen toegang hebben gehad. Direct na de melding van het datalek is door IV-Groep waardoor het risico vanaf dat moment niet meer bestond. Hierdoor deed het risico voor de rechten en vrijheden van betrokkenen zich niet meer voor.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	De IV-groep is gemeld om de persoonsgegevens te vernietigen.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:

AUTORITEIT PERSOONSGEGEVENS

Toelichting:	Er wordt na de zomer een voorlichtingssessie gehouden bij de project-assistenten over het afsluiten van verwerkersovereenkomsten en goed afronden van projecten.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	7737
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Personeel en Organisatie II
Kostenplaatscode	368

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	fout in rechten p-dossier ex-medewerker in archief,
Wat voor soort incident heeft er plaats gevonden?	Iemand kan bestanden inzien zonder de juiste rechten
Wanneer vond de inbreuk plaats? Indien bekend	
Wanneer vond de inbreuk plaats? Indien niet bekend	volgens idms is dossier geplaats 5-1-2018 tot heden,

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)	oud medewerker
Schatting van het aantal personen betrokken bij het datalek: minimaal	1
Schatting van het aantal personen betrokken bij het datalek: maximaal	1

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	0650057385
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Beleidscoördinatie en Advies
Kostenplaatscode	411

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Inzage in teveel persoonsgegevens in Youforce door medewerkers die deze gegevens niet nodig hebben voor de uitoefening van hun functie
Wat voor soort incident heeft er plaats gevonden?	Iemand kan bestanden inzien zonder de juiste rechten
Wanneer vond de inbreuk plaats? Indien bekend	5 oktober 2023 0:00
Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☑

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☑
Telefoonnummers	☐

E-mailadressen of andere adressen voor digitale communicatie	☐
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☑
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☑
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☑
Anders, namelijk	deels nog onbekend
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	2500

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	art.5.1-2e
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Verkenning en Monitoring
Kostenplaatscode	436

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	??
Bij een smartphone van de PZH. Wat is het 06 nummer?	??
Locatie, datum en tijdstip van vermissing, indien bekend?	Verhuizing juni 2021
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Ja

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Nee
Zijn de gegevens versleuteld?	Nee
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Ja
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Sinds de verhuizing in juni 2021 heb ik mijn smartphone niet meer kunnen vinden. Het abonnement is eerder al stopgezet. De authenticator is actief op mijn persoonlijk toestel.

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e ozh.nl
Organisatie-eenheid	rastructuur en Support
Kostenplaatscode	279

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	CI350110412013057
Bij een smartphone van de PZH. Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	Malosewaver, Geel te Belgie. Tussen 2:00 en 3:00 uur.
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Ja
Zo ja? Om welke gegevens gaat het?	Meer persoonlijke gegevens.
Zijn de gegevens versleuteld?	Ja
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Tijdens een bezoek aan een festival is mijn telefoon kwijtgeraakt. Ik denk dat deze uit de zak van mijn vest is gevallen.

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	art.5.1-2e
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Personeel en Organisatie II
Kostenplaatscode	368

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH. Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	Ergens in 2022
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Nee

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Nee
Zijn de gegevens versleuteld?	Onbekend
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Ja
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Heel waarschijnlijk ligt de mobiel thuis. Ivm verhuizing en aankomende verhuizing kan ik de mobiel niet zo snel vinden.

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Groen Blauwe Leefomgeving
Kostenplaatscode	483

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Anders;
Indien anders! Wat is er gestolen of vermist?	Ik ben de oplader van mn PZH-mobiel kwijt. Ik denk dat ik hem op het provinciehuis heb laten liggen afgelopen maandag
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH. Wat is het 06 nummer?	
Locatie, datum en tijdstip van vermissing, indien bekend?	Maandag heb ik hem op het provinciehuis (4e verdieping A) het laatst gezien
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Onbekend
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Onbekend

Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend
Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Onbekend
Zijn de gegevens versleuteld?	Onbekend
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Onbekend
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Alles even op onbekend gezet want niet relevant voor oplader.

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Projecten en Programma's III
Kostenplaatscode	355

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	mail verzonden aan omwonenden project over werkzaamheden aan de brug. Personen niet in BCC gezet. Op verzoek van collega meld ik dit. In de mail zelf stond geen vertrouwelijke informatie.
Wat voor soort incident heeft er plaats gevonden?	Anders
Anders? Graag toelichten	ipv BCC de omwonenden een mail gestuurd bij aan:
Wanneer vond de inbreuk plaats? Indien bekend	22 november 2022 13:51
Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☐
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☑

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☐
Telefoonnummers	☐

E-mailadressen of andere adressen voor digitale communicatie	☑
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☐
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	omwonenden van project
Schatting van het aantal personen betrokken bij het datalek: minimaal	30
Schatting van het aantal personen betrokken bij het datalek: maximaal	35

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Projecten en Programma's II
Kostenplaatscode	356

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	?
Bij een smartphone van de PZH. Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	zie melding M22 07 02299
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Ja

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Ja
Zo ja? Om welke gegevens gaat het?	naam en telefoonnummers contactpersonen
Zijn de gegevens versleuteld?	Ja
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	zie melding (M22 07 02299)

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	onbekend
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Beleidscoördinatie en Advies
Kostenplaatscode	411

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Er is vanuit Het Loket een mail verstuurd naar circa 420 medewerkers van PZH i.v.m. hun OV-chipkaart. In het Aan-veld zijn alle emailadressen van de medewerkers vermeld. In 49 gevallen gaat het om het persoonlijke emailadres. De emailadressen zijn inzichtelijk geweest voor ruim medewerkers. Er is ook eenantwoord gestuurd door tenminste 1 medewerker die ook aan allen is gestuurd. 1 medewerker heeft geklaagd en gevraagd of dit gemeld gaat worden als datalek. De melding is mondeling gedaan aan de FG PZH
Wat voor soort incident heeft er plaats gevonden?	Mail naar een verkeerde ontvanger
Wanneer vond de inbreuk plaats? Indien bekend	24 oktober 2019 14:30
Wanneer vond de inbreuk plaats? Indien niet bekend	
	Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)
Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☑
	Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)
Naam-, adres- en woonplaatsgegevens	☐
Telefoonnummers	☐

E-mailadressen of andere adressen voor digitale communicatie	☑
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☐
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	medewerkers PZH
Schatting van het aantal personen betrokken bij het datalek: minimaal	300
Schatting van het aantal personen betrokken bij het datalek: maximaal	450

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Corporate Communicatie
Kostenplaatscode	357

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Vandaag is er een werkgeversverklaring, voor het verkrijgen van een hypotheek, naar mijn collega met dezelfde achternaam gestuurd. Dit is niet de eerste keer dat er vertrouwelijke, persoonlijke en financiële informatie naar haar is gestuurd, die voor mij bestemd was.
Wat voor soort incident heeft er plaats gevonden?	Mail naar een verkeerde ontvanger
Wanneer vond de inbreuk plaats? Indien bekend	16 maart 2020 9:30
Wanneer vond de inbreuk plaats? Indien niet bekend	
	Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)
Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☐
	Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)
Naam-, adres- en woonplaatsgegevens	☐
Telefoonnummers	☐

E-mailadressen of andere adressen voor digitale communicatie	☐
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☑
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☑
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☑
Anders, namelijk	Salarisgegevens
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	werknemer
Schatting van het aantal personen betrokken bij het datalek: minimaal	1
Schatting van het aantal personen betrokken bij het datalek: maximaal	3

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Interim Consult
Kostenplaatscode	206

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Anders;
Indien anders! Wat is er gestolen of vermist?	sim-kaart
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH. Wat is het 06 nummer?	
Locatie, datum en tijdstip van vermissing, indien bekend?	Onbekend
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Onbekend
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Onbekend

Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend
Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Nee
Zijn de gegevens versleuteld?	Onbekend
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Onbekend
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Mijn simkaart heb ik deze zomer verwisseld zodat ik op vakantie niet per ongeluk data van de provincie in het buitenland gebruikte. Bij terugkomst kon ik deze simkaart niet meer vinden.

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Bedrijfsinformatie
Kostenplaatscode	278

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Hierbij de melding voor een beveiligingslek/data lek van het platform. waarbij het kan zijn dan niet geautoriseerde personen kunnen inloggen op het platform met @pzh.nl als account.
Wat voor soort incident heeft er plaats gevonden?	Iemand kan bestanden inzien zonder de juiste rechten
Wanneer vond de inbreuk plaats? Indien bekend	18 augustus 2022 11:00
Wanneer vond de inbreuk plaats? Indien niet bekend	geen inbreuk gemeld

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☐
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☑

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☐
Telefoonnummers	☑

E-mailadressen of andere adressen voor digitale communicatie	☑
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☐
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	werknemer
Schatting van het aantal personen betrokken bij het datalek: minimaal	10
Schatting van het aantal personen betrokken bij het datalek: maximaal	nnb

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Interim Consult
Kostenplaatscode	206

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Anders;
Indien anders! Wat is er gestolen of vermist?	SIM-kaart
Bij een apparaat van de PZH. Wat is het CI nummer?	-
Bij een smartphone van de PZH. Wat is het 06 nummer?	-
Locatie, datum en tijdstip van vermissing, indien bekend?	Thuis, half juni '22
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Onbekend
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Onbekend

Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend
Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Onbekend
Zijn de gegevens versleuteld?	Ja
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Onbekend
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Simkaart in mijn huis waarschijnlijk verloren. Dit formulier dinsdag al ingediend, maar hiervan geen bevestiging gekregen. Graag mijn telefoonnummer op de nieuwe sim zo snel mogelijk herstellen.

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	art.5.1-2e
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

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e pzh.nl
Organisatie-eenheid	Bureau Concern- en Interne Communicatie
Kostenplaatscode	380

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Ik heb gisteren naar de PZH collega's die aanwezig zullen zijn bij de nieuwjaarsreceptie een e-mail gestuurd met een excel overzicht van de aangemelde relaties die naar de Nieuwjaarsreceptie komen (zo'n 520 personen). Overzicht bestaat uit voornaam, achternaam, organisatie en functie). Dit zodat onze collega's zich gedegen kunnen voorbereiden en we zo een optimaal resultaat kunnen halen uit deze bijeenkomst. Deze collega's zijn ook aangemeld en vanuit dat excel bestand heb ik hen op organisatie gekopieerd, daar zijn 1 oud PS lid art.5.1-2e en 1 huidig PS lid art.5.1-2e tussendoor geglipt aangezien zij als organisatie ook Provincie Zuid-Holland hadden opgegeven. art.5.1-2e eldde dit bij mij. Ik heb hem gevraagd deze mail te verwijderen. Op advies van art.5.1-2e eld ik dit toch even.
Wat voor soort incident heeft er plaats gevonden?	Mail naar een verkeerde ontvanger
Wanneer vond de inbreuk plaats? Indien bekend	7 januari 2020 17:00
Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☐

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☐
Telefoonnummers	☐
E-mailadressen of andere adressen voor digitale communicatie	☐
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☑
Anders, namelijk	Voornaam, achternaam, organisatie en functie (waarvan een groot gedeelte publieke figuren zijn)
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	Aangemelde relaties van de Nieuwjaarsreceptie
Schatting van het aantal personen betrokken bij het datalek: minimaal	2
Schatting van het aantal personen betrokken bij het datalek: maximaal	2

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Huisvesting, Vastgoed en Kunst
Kostenplaatscode	455

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH. Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	26 september 15.00 uur
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Ja

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Ja
Zo ja? Om welke gegevens gaat het?	mail
Zijn de gegevens versleuteld?	Nee
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Ja
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	ik vermoed dat het toestel is 'meegenomen' door iemand bij pzh, Ik was bezig met een expositie en had al die tijd twee iphones(1 prive) en 1 van de zaak op de tafel bij de koffiekamer liggen. Ook lagen er anderen iphones van collega's. Thuis aangekomen had ik hem niet bij me. Ik heb meteen de beveiliging ingeschakeld in de ochtend niets gevonden. met vr g art.5.1-2e

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	BC Leidschendam
Kostenplaatscode	491

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Laptop
Bij een apparaat van de PZH. Wat is het CI nummer?	-
Bij een smartphone van de PZH. Wat is het 06 nummer?	-
Locatie, datum en tijdstip van vermissing, indien bekend?	1-5-2023
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Onbekend
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Onbekend
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Ja

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Onbekend
Zijn de gegevens versleuteld?	Onbekend
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Ja
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	laatst gebruikt 26 of 27 april.op woensdag 10 mei had ik een afspraak op de buiten lokatie leidschendam ,toen kwam ik achter dat de verhuizing had plaats gevonden.en ik merkte gelijk op dat het fout was want ik zag mijn ladekasten niet beide natuurlijk.deze was voorzien van pzh eigendom waar onder de laptop met oplader en al.getuigen ja dat hoop ik oa mijn teamleider.personeel van fz en de schoonmaker.

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Realisatie Water en Groen
Kostenplaatscode	405

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH. Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	Dinsdagmiddag 22 november, provinciehuis A5.
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Onbekend
Zijn de gegevens versleuteld?	Ja
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	I.r.t. 'vertrouwelijke gegevens': ja er is via de telefoon (na ontgrendeling) toegang tot mijn mailbox en whatsapp. Ik werk echter niet aan hoog-vertrouwelijke zaken. Na vertrek van A5 's middags bleek mijn telefoon (en bruin notitieboekje) niet in mijn tas te zitten. Einde dag zowel bij de balie als digitaal via loket melding gemaakt, maar niet gevonden. Graag een nieuwe simkaart. Om daarmee mijn nieuwe telefoon (Fairphone, reeds besteld ivm omwisseling telefoons) te kunnen ophalen/activeren.

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e art.5.1-2e
Telefoonnummer	art.5.1-2e
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Groen Blauwe Leefomgeving
Kostenplaatscode	483

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	niet bekend, toestel verloren...
Bij een smartphone van de PZH. Wat is het 06 nummer?	
Locatie, datum en tijdstip van vermissing, indien bekend?	NS trein Woerden-Rotterdam 12:45 uur, vrijdag 17 maart 2023
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Ja

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Ja
Zo ja? Om welke gegevens gaat het?	pzh werkomgeving + prive mail, betaal apps e.d.
Zijn de gegevens versleuteld?	Onbekend
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	verloren in trein of op station rotterdam CS

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e pzh.nl
Organisatie-eenheid	Bureau Concern- en Interne Communicatie
Kostenplaatscode	380

Benodigde gegevens

Is dit een diefstal of vermissing?	Diefstal
Is er al aangifte gedaan?	Nee
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH. Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	Op straat, 27-04-2023, omstreeks 20 uur.
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Ja
Zo ja? Om welke gegevens gaat het?	Namen en telefoonnummers (niet versleuteld). Emailadressen en emails (wel versleuteld).
Zijn de gegevens versleuteld?	Nee
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Ik was in Amsterdam aan het rondlopen op koningsdag en had mijn werktelefoon in mijn zak. Op gegeven moment had ik door dat mijn telefoon weg was. Dat was rond een uurtje of 8. Ik heb toen 'vind mijn telefoon' gebruikt met mijn persoonlijke mobiel om hem terug te vinden. Toen zag ik dat de telefoon bewoog in de stad en heb ik een aantal keer een geluid afgespeeld en de telefoon gebeld.. Helaas tevergeefs. Ook ben ik naar verschillende plekken in de stad geweest om de telefoon op te halen. Helaas zonder succes. De telefoon is voor het laatst gezien in Weesp op 27 april om 22:30 (volgens 'vind mijn telefoon'). Nu is hij uitgeschakeld en kan ik de telefoon niet meer bereiken. Ik hoopte dat de telefoon op een gegeven moment zou worden opgeladen door de vinder en ik na een belletje hem zou kunnen ophalen. Helaas is dit niet het geval.

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Corporate Communicatie
Kostenplaatscode	379

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Onbekend
Zijn de gegevens versleuteld?	Onbekend
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Ik ben de iphone kwijt geraakt, merkte het nadat ik thuis was. Hij kan verloren zijn op het provinciehuis of onderweg. Ik heb gecheckt bij beveiliging of hij gevonden is, dit is niet het geval. Dit check ik maandag nog een keer.

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Projecten en Programma's II
Kostenplaatscode	356

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	Vermoedelijk in randstadrail (aankomst woensdag17 mei 18:30 uur op halte Melanchtonweg)
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Ja
Zo ja? Om welke gegevens gaat het?	toegang tot mailaccount PZH en eigen Hotmail
Zijn de gegevens versleuteld?	Onbekend
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Ik heb gisteren 18 mei de vermissing ontdekt. Heb geprobeerd de Iphone thuis te traceren door het op te bellen en heb de route van de halte naar huis nagelopen. Vandaag nogmaals alles afgezocht in huis. Meen me te herinneren dat ik een bonk heb gehoord bij het uitstappen uit de voorzijde van de metro/randstadrail.

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e pzh.nl
Organisatie-eenheid	Bureau Mobiliteit en Milieu V
Kostenplaatscode	487

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	zondag 16 april, tussen 15:00 en 16:00 uur Mogelijk diefstal, kalverstraat, nieuwendijk, Amsterdam
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Ja
Zo ja? Om welke gegevens gaat het?	mijn persoonsgegevens
Zijn de gegevens versleuteld?	Onbekend
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	werkmobiel, stond op stand-by stand. Voor toegang zou men de 8-cijferige pin-code nodig hebben. Zondag 16 april: Mobiel had ik nog bij me bij het uitstappen op Amsterdam CS. Daarna ben ik met Metro van Amsterdam naar CS naar Metro-station Rokin gegaan om een aantal winkels te bezoeken. De telefoon was niet meer in mijn bezit rond 16u, in de winkel. Ik heb de telefoon niet in de tussentijd gebruikt of uit mijn zak gehaald.

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Advies en Beleid
Kostenplaatscode	275

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Ik heb een bestand met namen van I&A medewerkers inclusief arbeidsrelatie en indiensttreding naar de verkeerde persoon binnen I&A gestuurd. De naam is Mike Wijsen. Ik heb hem gevraagd het bestand te vernietigen.
Wat voor soort incident heeft er plaats gevonden?	Mail naar een verkeerde ontvanger
Wanneer vond de inbreuk plaats? Indien bekend	9 mei 2023 12:27
Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☑
Kopiëren	☑
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☐

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☑
Telefoonnummers	☐

E-mailadressen of andere adressen voor digitale communicatie	☐
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☑
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☑
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☐
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	werknemers en externe werknemers
Schatting van het aantal personen betrokken bij het datalek: minimaal	254
Schatting van het aantal personen betrokken bij het datalek: maximaal	254

Melden datalek

Aanmelder

Naam	art.5.1-2e art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Team Juridische Zaken
Kostenplaatscode	374

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Op 26 april en 1 mei zijn twee e-mails met stukken tbv een zitting van de bezwarencommissie van de PZH verzonden naar een (naar achteraf bleek) verkeerd e-mailadres. Stukken waar het om gaat zijn 2 voorbereidingsdocumenten met inhoudelijke gegevens over de bezwaarzaak + e-mailadressen en een besluit last onder dwangsom met inhoudelijke informatie over het bedrijf en een aantal emailadressen.
Wat voor soort incident heeft er plaats gevonden?	Mail naar een verkeerde ontvanger
Wanneer vond de inbreuk plaats? Indien bekend	26 april 2023 0:00
Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☐

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☐
Telefoonnummers	☐

E-mailadressen of andere adressen voor digitale communicatie	☑
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☐
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	1 medewerker van de PZH (ikzelf), 2 leden van de bezwarencommissie, 2 medewerkers van DCMR, 1 persoon van AVR Afvalverwerking
Schatting van het aantal personen betrokken bij het datalek: minimaal	6
Schatting van het aantal personen betrokken bij het datalek: maximaal	

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	art.5.1-2e
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Eenheid Audit en Advies
Kostenplaatscode	227

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Er heeft een Ransomware aanval plaatsgevonden op het P8 systeem van de afdeling Ontwikkeling en Grondzaken. De applicatie is extern gehost. P8 is de applicatie voor het registreren en beheren van verpachte en verhuurde eigendommen van de provincie. Vaak gaat het daarbij om percelen (vastgoed). In de applicatie worden contracten beheert en facturen opgemaakt. De applicatie draait nu weer normaal. Op moment van deze melding is niet duidelijk of er data verloren is gegaan of een andere verwerking heeft plaatsgevonden. ---------- zie: het NOS-bericht: https://nos.nl/artikel/2462701-grootschalige-aanval-met-gijzelsoftware-op-duizenden-servers-wereldwijd P8 draait op dit moment weer, ze hebben alles weer snel in de lucht gekregen. De vraag is nog of er data is gelekt. Vanmiddag hoor ik meer. Wie van jullie moet ik op de hoogte houden?
Wat voor soort incident heeft er plaats gevonden?	Anders
Anders? Graag toelichten	Ransomeware aanval
Wanneer vond de inbreuk plaats? Indien bekend	5 februari 2023 20:00
Wanneer vond de inbreuk plaats? Indien niet bekend	
	Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)
Lezen (vertrouwelijkheid)	☐
Kopiëren	☐

Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☑
	Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)
Naam-, adres- en woonplaatsgegevens	☑
Telefoonnummers	☐
E-mailadressen of andere adressen voor digitale communicatie	☑
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☑
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☑
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☑
Anders, namelijk	KVK gegevens
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	Van particulieren en bedrijven die percelen van de provincie pachten.
Schatting van het aantal personen betrokken bij het datalek: minimaal	niet bekend. Waarschijnlijk enkele honderden percelen.
Schatting van het aantal personen betrokken bij het datalek: maximaal	niet bekend. Waarschijnlijk enkele honderden percelen.

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e .pzh.nl
Organisatie-eenheid	Bureau Projecten en Programma's III
Kostenplaatscode	355

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Smartphone
Bij een apparaat van de PZH. Wat is het CI nummer?	
Bij een smartphone van de PZH. Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	08:00, Trein, Utrecht Centraal. Treinnummer 11720.
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Ja
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Ja
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Onbekend

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Nee
Zijn de gegevens versleuteld?	Nee
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Nee
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Melding gemaakt bij ICT en telefoon is geblokkeerd. Zoektocht loopt nu via de NS om het toestel te vinden.

Van: art.5.1-2e
Verzonden: 2023-09-21 19:27:57+00:00
Aan: art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e
CC:
Onderwerp: overige applicaties + eenheid privacy
"
Dag art.5.1-2e

1. Een van de sporen die wij zojuist hebben besproken ziet op mogelijk andere applicaties dan iDMS waarbij (grote) schendingen van de AVG mogelijk zijn. Kijkend naar het (incomplete) verwerkingsregister van PZH komen daarbij de volgende applicaties naar voren:
   a. Outlook
   b. Teams
   c. Sharepoint
   d. Onedrive
   e. Topdesk

   Van Topdesk is het mij bekend dat daar circa twee jaar geleden door de beheerder al eens is gekeken naar het voorkomen van documenten met (teveel) persoonsgegevens, waarna een opschoonactie heeft plaatsgevonden.

   Voor Teams en Sharepoint stel ik voor om dezelfde aanpak te gebruiken die ook gebruikt wordt voor iDMS.

   Bij Outlook en Onedrive spelen andere aspecten mee, namelijk mogelijke schendingen van de AVG omdat deze ook persoonlijke, lees privédocumenten, kunnen bevatten. Daar mag niet zomaar een zoekslag op plaatsvinden. Daar zal in overleg met de OR en de provinciesecretaris naar moeten worden gekeken. Wellicht dat een overleg met de AP daarin ook helderheid kan verschaffen.

   Met andere woorden, ik adviseer om de focus eerst te leggen op iDMS, Teams en Sharepoint. Volgens mij vergt dat al heel veel effort van de organisatie. Dat laat onverlet dat de overige applicaties niet buiten schot mogen blijven. Maar wellicht dat daar eerst met bewustwording het nodige gedaan kan worden. Daarbij doel ik dan op een verplichte e-learning voor privacy en informatieveiligheid en een e-learning over het omgaan met bijvoorbeeld iDMS.

2. Vanuit de Eenheid Privacy sluit art.5.1-2e aan als adviseur bij het crisisteam.

Met vriendelijke groet,

art.5.1-2e art.5.1-2e
Functionaris voor Gegevensbescherming
Gerechtelijk Deskundige

M art.5.1-2e
E
www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art.5.1-2e . art.5.1-2e %40pzh.nl%7C291653efbd1144524f4708dbbac8189d%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638309140795045823%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=OQTisi%2BnXuVEf0AduHvvWTYf3BOn4mE76pr0cLRyXcg%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Krachtig Zuid-Holland.
"


provincie
Zuid-Holland

13-03-2020 Controle door privacy officer art.5.1-2e op persoonsgegevens in:
"Reisgegevens en IDs" kan via de volgende koppeling worden geopend: http://idms/otcs/llisapi.dll/properties/539080145
Centraal 1 Primaire processen 1.1 Beleidsontwikkeling 01 Extern gericht beleid 07 Economische en agraris... 04 Energietransitie DOS-2015-0000284 Bio-econ... 05 Achtergrondinformatie Vanguard Initiative DemoCases Biogas beyond Energyprodu...

Reisgegevens en IDs

Mail	Persoonsgegevens (anders dan zakelijke contactgegevens)	art.5.1-2e	Afwijkende toegang? (anders dan map eigenaar Bart Verschoor, idms beheer en privacy officer)
2015-12-16 16.30	Nee		
2015-12-16 16.40	Kopie ID		Nee
2015-12-19 15.42	Kopie ID		Nee
2015-12-22 08.42	Nee		
2015-12-22 08.47	Kopie ID		Nee
2015-12-22 09.25	Nee		
2015-12-24 09.39	Nee		
2015-12-24 12.36	Nee		
2015-12-28 14.56	Kopie ID		Nee
2015-12-28 15.36	Nee		
2015-12-29 14.52	Nee		
2015-12-29 14.57	Nee		
2016-01-01 01.25	Nee		
2016-01-03 14.08	Kopie ID		Nee
2016-01-04 11.42	Kopie ID		Nee
2016-01-05 09.24	Nee		
2016-01-05 14.31	Kopie ID		Nee
2016-01-05 14.36	Nee		

Mail	Persoonsgegevens (anders dan zakelijke contactgegevens)	art.5.1-2e	Afwijkende toegang? (anders dan map eigenaar Bart Verschoor, idms beheer en privacy officer)
2016-01-05 14.37 (2x)	Nee		
2016-01-06 10.11	Nee		
2016-01-06 10.13	Nee		
2016-01-06 10.39	Nee		
2016-01-06 10.40	Nee		
2016-01-06 15.35	Nee		
2016-01-07 08.39	Nee		
2016-01-07 15.07	Kopie ID		Nee
2016-01-08 11.47	Nee		
2016-02-23 11.12	Nee		
2016-03-14 17.41	Nee		
2016-03-14 17.43	Nee		

art.5.1-2e

Van: art.5.1-2e art.5.1-2e
Verzonden: ember 2023 11:01
Aan: art.5.1-2e
CC: art.5.1-2e
Onderwerp: ortage -idms search 2

Hi art.5.1-2e

Het is art.5.1-2e gelukt om alle zoekopdrachten te doen en alle informatie is binnen.
Er wordt vanochtend nog gewerkt om dit op te nemen in een Power BI- dashboard.

Alleen door mijn volle agenda en afspraken buiten de deur kunnen we deze pas vrijdagochtend nader toelichten.

Omdat dit in een nieuwe power Bi- rapportage komt, moet ook daar de toegang ingeregeld worden. Hierbij houden we dezelfde eerder groep aan: art.5.1-2e art.5.1-2e en Jij als opdrachtgever.
Zodra het rapport klaar is, we richten op vanmiddag, komt er een bericht jouw kant op. Dan hebben jullie wellicht al inzage.

art.5.1-2e art.5.1-2e

Productowner/data officer voor Team Applicaties, innovatie en datascience

provincie Zuid-Holland

provincie Zuid-Holland

Phone art.5.1-2e
Email: art.5.1-2e @pzh. nl
Provincie Zuid-Holland
Zuid-Hollandplein 1
Postbus 90602 | 2509 LP Den Haag
www.zuid-holland.nl

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

art.5.1-2e

Van: art.5.1-2e art.5.1-2e
Verzonden: ember 2023 13:44
Aan: art.5.1-2e
Onderwerp:

Toegangsrechten tot de 2 power Bi rapporten.

art.5.1-2e
art.5.1-2e
art.5.1-2e
En ik zelf

art.5.1-2e art.5.1-2e

Productowner/data officer voor Team Applicaties, innovatie en datascience

provincie Zuid-Holland

provincie Zuid-Holland

Phone art.5.1-2e
Email: art.5.1-2e pzh. nl
Provincie Zuid-Holland
Zuid-Hollandplein 1
Postbus 90602 | 2509 LP Den Haag
www.zuid-holland.nl

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

M22 10 03600 Virus of vermoeden /malware/spyware/adware/ ransomware/etc.

art.5.1-2e

Aanmelder

Naam	art.5.1-2e
Gebouw	PZH
Personeelsnummer	563210
Inlognaam netwerk	art.5.1-2e
Telefoonnummer	
Mobiel nummer	
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Bureau Groen Blauwe Leefomgeving
Kostenplaatscode	483
Plaats	Den Haag

Details

Korte omschrijving	Virus of vermoeden /malware/spyware/adware/ ransomware/etc.
Soort melding	Verstoring
Categorie	Servicedesk (I&A)
Subcategorie	Security

Planning

Prioriteit	Hoog
Streefdatum	2 november 2022 10:50
Doorlooptijd	2 Dagen
On hold	Nee

Afhandeling

Behandelaarsgroep	Bestuur - Eenheid Privacy
Behandelaar	Bestuur - Eenheid Privacy
Status	Reactie ontvangen
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00
Onkosten	0,00

Verzoek

art.5.1-2e

31 oktober 2022 10:55

Omschrijving: via de Website https://rijnengouwewiericke.nl/, wordt er gevraagd om pup up notificaties toe te staan, indien de gebruiker dat doet, krijgen ze notificaties van gekke dingen met een McAfee melding dat er virussen zijn en met plaatjes van schaar geklede vrouwen.

Actie

art.5.1-2e

Mailimport 6 februari 2023 14:03

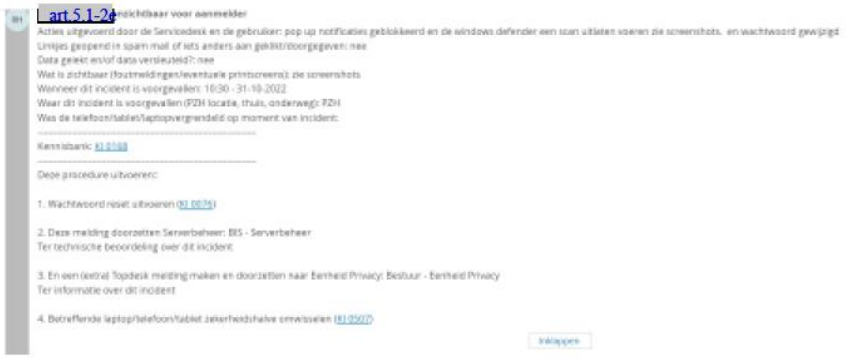
Beste collega's,

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

Dit ticket kan daarom worden afgesloten.

Hartelijk dank,
art.5.1-2e

image001.png


art.5.1-2e onzichtbaar voor aanmelder
Acties uitgevoerd door de Servicedesk en de gebruiker: pop up notificaties geblokkeerd en de windows defender een scan uitlaten voeren zie screenshots. en wachtwoord gewijzigd
Linkjes geopend in spam mail of iets anders aan geklikt/doorgegeven: nee
Data gelekt en/of data versleuteld?: nee
Wat is zichtbaar (foutmeldingen/eventuele printscreens): zie screenshots
Wanneer dit incident is voorgevallen: 10:30 - 31-10-2022
Waar dit incident is voorgevallen (PZH locatie, thuis, onderweg): PZH
Was de telefoon/tablet/laptopvergrendeld op moment van incident:

Kennisbank: KI 0168

Deze procedure uitvoeren::
1. Wachtwoord reset uitvoeren (KI 0076)
2. Deze melding doorzetten Serverbeheer: BIS - Serverbeheer
Ter technische beoordeling over dit incident
3. En een (extra) Topdesk melding maken en doorzetten naar Eenheid Privacy: Bestuur - Eenheid Privacy
Ter informatie over dit incident
4. Betreffende laptop/telefoon/tablet zekerheidshalve omwisselen (KI 0507)
Inkloppen

image002.png

Met vriendelijke groet,

art.5.1-2e
Privacy Officer

provincie Zuid-Holland

Eenheid Privacy
T art.5.1-2e **Mail** art.5.1-2e @pzh.nl

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

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

art.5.1-2e **onzichtbaar voor aanmelder** 31 oktober 2022 10:55

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

Kennisbank: KI 0168

Deze procedure uitvoeren::

1. Wachtwoord reset uitvoeren (KI 0076)

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

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

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

Informatie

Aanmelddatum	31 oktober 2022 10:50
Gerealiseerde doorlooptijd	00:00
Doorlooptijd 'On hold'	00:00
Aangepaste doorlooptijd	00:00
Doorlooptijd 'Afgerond'	00:00
Doorlooptijd 'Uitvoering'	00:00
Geregistreerde tijd	00:00
Totale onkosten	0,00

	Virus of vermoeden /malware/spyware/adware/ ransomware/etc.
Geëscaleerd	Ja
Behandelaar (de-)escaleren	art.5.1-2e
Bestede tijd	00:00

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.

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: art.5.1-2e

Melddatum: 20 juli 2023

Meldtijdstip: 12:41

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	art.5.1-2e

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	art.5.1-2e
Functie	Privacy Officer
E-mailadres	art.5.1-2e @pz h.nl
Telefoonnnummer	art.5.1-2e
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

AUTORITEIT
PERSOONSGEGEVENS

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

[✓] Aantal inbreuken in bulk

[✓] Geselecteerde toezichthouders

2. Grensoverschrijdende inbreuk

[✓] Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

[✓] Gegevens verwerkingsverantwoordelijke

[✓] Gegevens over andere organisaties

4. Tijdlijn

[✓] Tijdlijn

5. Gegevens over de inbreuk

[✓] Aard van de inbreuk

[✓] Aard van het incident

[✓] Samenvatting van het incident

6. Betrokken persoonsgegevens

AUTORITEIT
PERSOONSGEGEVENS

[✓] Welke persoonsgegevens

[✓] Hoeveelheid persoonsgegevens

7. Getroffen personen

[✓] Groep mensen dat getroffen is door de inbreuk?

[✓] Nadere omschrijving van de groep mensen dat getroffen is door de inbreuk.

8. Maatregelen vooraf

9. Gevolgen

[✓] Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens

[✓] Gevolgen voor de betrokkene(n) (Persoon of personen van wie gegevens zijn getroffen door de inbreuk)

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

[✓] Maatregelen om de inbreuk aan te pakken?

1 Introductie (vervolg)

Geef het aantal inbreuken aan dat u bij de AP in bulk wilt melden:	1

1.3 Andere toezichthouders

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

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

AUTORITEIT PERSOONSGEGEVENS

3 Uw contactgegevens

3.1 Gegevens verwerkingsverantwoordelijke

KvK-nummer (indien van toepassing)	27375169
Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Provincie

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Ja

Geef aan welke andere organisaties betrokken waren bij de inbreuk?

Naam	Op welke wijze betrokken	Toelichting (optioneel)
ICT-leverancier van IV-Groep	Verwerker	

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	31-3-2023
(Mogelijke) einddatum van de inbreuk	31-3-2023
Wanneer heeft u het datalek voor het eerst aan de AP gemeld?	4-7-2023

AUTORITEIT PERSOONSGEGEVENS

4.2 Wanneer is het incident ontdekt?	31-3-2023
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	De IV-Groep heeft dinsdag 4 juli een melding gedaan aan de Provincie Zuid-Holland. De IVGroep geeft aan dat door hun deze leverancier het volgende is geconstateerd: - het Azure Storage account waarmee de backups van onze Ftp-server werden gemaakt, was niet voldoende beveiligd, waardoor deze benaderbaar was vanaf internet. Deze back-up service is eind 2022 beëindigd. Dit is door een externe beveiligingsonderzoeker (ethische hacker) , aangesloten bij DIVD, geconstateerd. De IV-groep heeft zelf de melding gedaan bij AP op 4 mei 2023. Na verder intern onderzoek bij de IV-groep heeft de IV-groep de melding op 4 juli doorgezet richting de provincie Zuid-Holland, die op zijn beurt binnen 72 een voorlopige melding heeft gedaan bij de AP.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Nee
Wanneer heeft u kennis gekregen van het datalek?	4-7-2023

5 Gegevens over datalek

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

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

[✓] Hacking, malware (bijv. ransomware) en/of phishing

Meerdere opties zijn mogelijk binnen het gearceerde deel.

[✓] Ander type hacking en/of malware

AUTORITEIT PERSOONSGEGEVENS

Heeft u (digitaal forensisch) onderzoek uitgevoerd of laten uitvoeren naar de aard en de omvang van het datalek?	Ja, het onderzoek is afgerond

Optioneel: upload hier de rapportage van het onderzoek naar de inbreuk.

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Iv-Groep is een Nederlands ingenieurs bureau en is werkzaam in diverse marktsegmenten (water, infra, industrie, offshore & energy, bouw). Via één van haar werkmaatschappen zijn er werkzaamheden verricht voor de Provincie Zuid-Holland. Voor het uitwisselen van grote hoeveelheid bestanden is er gebruik gemaakt van een zogenaamde Ftp-server. Deze Ftp server wordt beheerd door één van de ICT-dienstverleners van IV-Groep. Hierop kan via een toegekende gebruikersnaam en wachtwoord toegang tot deze informatie verkregen worden, zowel door Iv-medewerkers als door Provincie Zuid-Holland als opdrachtgever. Door deze ICT-dienstverlener is geconstateerd dat het Azure Storage account waarmee de backups van de Ftp-server werden gemaakt, niet voldoende was beveiligd, waardoor deze benaderbaar was vanaf internet. Dit is geconstateerd door een externe beveiligingsonderzoeker (ethische hacker), aangesloten bij DIVD. Deze back-up service is eind 2022 beëindigd. Er is geen aanwijzing dat er onbevoegde toegang is geweest (anders dan de ethisch hacker). Er is onvoldoende logging beschikbaar om dit met zekerheid vast te stellen.

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

6 Betrokken persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Contactgegevens

[✓] Adres en woonplaats

AUTORITEIT PERSOONSGEGEVENS

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	698
Geef een toelichting op bovengenoemd aantal:	Het betreft een adressenlijst met 698 NAW gegeven van bewoners, gebruikt voor etikettering van een standaard brief.

7 Betrokkenen

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

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Inwoners van de gemeente Midden-Delfland (dorp Schipluiden)
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Aanwonenden van provinciale weg N468 aan wie een brief moest worden gestuurd.

9 Gevolgen

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

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

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

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

AUTORITEIT PERSOONSGEGEVENS

Namelijk:	Betrokkenen kunnen ongewenst worden aangeschreven.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Het betreft NAW gegevens die met minimale inspanning ook op andere manieren verkregen kunnen worden.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

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

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

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

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Na onderzoek heeft de provincie besloten om betrokkenen niet te informeren. De reden hiervoor is dat het onwaarschijnlijk is dat de inbreuk leidt tot een hoog risico voor de betrokkenen. Daarnaast zijn er direct na het datalek maatregelen genomen als bedoeld in artikel 34, lid 3 onder b waardoor eventuele risico's zich niet meer voor kunnen doen. Het is na onderzoek bekend geworden dat een ethisch hacker toegang heeft gehad tot een adressenbestand bestaande uit alleen achternaam, straatnaam en nummer, postcode en woonplaats. De (ethische) hacker was aangesloten bij de DIVD (Dutch Institute for Vulnerability

AUTORITEIT PERSOONSGEGEVENS

Disclosure). Er zijn geen andere gegevens zoals e-mailadressen of telefoonnummers bij betrokken. Het betreft een bestand uit 2010. Het datalek is op 31 maart 2023 ontdekt en diezelfde dag beëindigt. Er zijn geen aanwijzingen dat naast de ethisch hacker nog andere personen toegang hebben gehad, maar dit valt door afwezigheid van logging niet geheel uit te sluiten. Vervolgens is provincie als verwerkingsverantwoordelijke pas op 4 juli in kennis gesteld van het datalek.
De reden waarom de provincie wat later is komt doordat de IV-Groep direct na de constatering op 31 maart is gestart met een eigen intern onderzoek. Hierbij ontdekten zij in eerste instantie alleen gegevens van hun eigen werknemers. Hiervan is door de IV-groep een melding gedaan bij AP op 4 mei 2023. Verder onderzoek is op 4 juli door de IV-groep afgerond. Daarbij is door IV-groep nog een bestand met persoonsgegevens gevonden van een infrastructureel project in Schipluiden. Dat bestand is gebruikt tijdens het groot onderhoud aan de N468. De adreslijst is gebruikt voor aanschrijven en uitnodigen van omwonenden. Na de afronding is de provincie Zuid-Holland geïnformeerd.

Op basis van deze feiten is het onwaarschijnlijk dat de inbreuk een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt (mede gelet op rechtsoverweging 75 en 85 van de AVG). Het gegevensbestand is oud en niet meer actueel. Betrokken personen kunnen om meerdere redenen niet meer op het betreffende adres wonen. Daarnaast zijn adresgegevens op relatief eenvoudige wijze ook op een andere manier te verkrijgen (zoals bijvoorbeeld naambordjes bij een huis). Ook in de EDPB Guidelines (Guidelines 9/2022 on personal data breach notification van 28 maart 2023, nr. 107 op pagina 24) wordt aangegeven dat het onwaarschijnlijk is dat de bekendmaking van de naam en het adres van een persoon in normale omstandigheden aanzienlijke schade zal veroorzaken.

Communicatie aan betrokkenen is bedoeld om deze betrokkenen te helpen om maatregelen te nemen om zich tegen eventuele negatieve gevolgen te beschermen. Gelet op de datum van het bestand, de datum van het datalek en de maatregelen die daarbij zijn genomen en de datum waarop de provincie als verwerkingsverantwoordelijke geïnformeerd is, is het niet meer opportuun om deze betrokkenen nu nog te informeren. Het creëert eerder onnodige onrust, omdat personen geïnformeerd zouden worden over iets waaraan ze nu niets geen maatregelen meer tegen kunnen nemen.

In artikel 34, lid 3, onder b wordt aangegeven dat een inbreuk ook niet aan personen hoeft te worden gemeld (mocht er wel sprake zijn van een hoog risico) als er voldoende maatregelen achteraf zijn genomen. Het datalek is gemeld door een ethisch hacker die deze persoonsgegevens alleen heeft ingezien om het datalek te kunnen melden. Er zijn geen aanwijzingen dat er andere onbevoegde personen toegang hebben gehad. Direct na de melding van het datalek is door IV-Groep waardoor het risico vanaf dat moment niet meer bestond. Hierdoor deed het risico voor de rechten en vrijheden van betrokkenen zich niet meer voor.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	De IV-groep is gemeld om de persoonsgegevens te vernietigen.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:

AUTORITEIT
PERSOONSGEGEVENS

Toelichting:	Er wordt na de zomer een voorlichtingssessie gehouden bij de project-assistenten over het afsluiten van verwerkersovereenkomsten en goed afronden van projecten.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: art.5.1-2e

Melddatum: 27 januari 2023

Meldtijdstip: 09:02

1 Introductie

1.1 De melding van een inbreuk

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

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

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

1.3 Andere toezichthouders

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

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

AUTORITEIT PERSOONSGEGEVENS

Registratienummer van de FG (indien van toepassing)	art.5.1-2e
Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596 AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Provincie

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	art.5.1-2e
Functie	Plaatsvervangend FG
E-mailadres	art.5.1-2e p zh.nl
Telefoonnummer	art.5.1-2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee

AUTORITEIT PERSOONSGEGEVENS

(Mogelijke) startdatum van de inbreuk	21-1-2023
(Mogelijke) einddatum van de inbreuk	21-1-2023
4.2 Wanneer is het incident ontdekt?	23-1-2023
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Medewerker heeft melding gemaakt dat haar laptop is gestolen.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Nee
Wanneer heeft u kennis gekregen van het datalek?	26-1-2023

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

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

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

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Er is een laptop gestolen waarop lokaal enkele persoonsgegevens waren opgeslagen. De laptop was beveiligd met onder meer een wachtwoord. Er kan niet worden uitgesloten dat een onbevoegde zich toegang heeft verschaft.

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

AUTORITEIT PERSOONSGEGEVENS

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] E-mailadres

[✓] Telefoonnummer

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	15
Geef een toelichting op bovengenoemd aantal:	Het gaat om mogelijk 10-20 gegevens van verschillende personen

7 Getroffen personen

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

Meerdere opties zijn mogelijk.

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Het betreft enkele zakelijke contactgegevens van personen
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1

AUTORITEIT PERSOONSGEGEVENS

Het maximum aantal betrokkenen is:	20

8 Maatregelen vooraf

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

[✓] Nee

9 Gevolgen

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

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	mogelijk worden betrokkenen benaderd door een derde

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar
Licht uw keuze toe:	Het betreft enkel contactgegevens

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

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

AUTORITEIT PERSOONSGEGEVENS

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

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

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	De inbreuk vormt geen hoog risico voor betrokkenen

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Accounts op laptop zijn ontkoppeld.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Betrokkene is er op gewezen om lokaal geen gegevens op te slaan.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: art.5.1-2e

Melddatum: 28 juli 2023

Meldtijdstip: 14:55

1 Introductie

1.1 De melding van een inbreuk

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

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

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

1.3 Andere toezichthouders

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

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

AUTORITEIT
PERSOONSGEGEVENS

KvK-nummer (indien van toepassing)	27375169
Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Provincie

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	art.5.1-2e art.5.1-2e
Functie	Privacy Officer
E-mailadres	art.5.1-2e @pz h.nl
Telefoonnummer	art.5.1-2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee

AUTORITEIT PERSOONSGEGEVENS

(Mogelijke) startdatum van de inbreuk	28-7-2022
(Mogelijke) einddatum van de inbreuk	28-7-2023
4.2 Wanneer is het incident ontdekt?	26-7-2023
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Een nieuwe medewerker van de Provincie Zuid-Holland constateerde dat zijn telefoonnummer in een openbare map van de Servicedesk in het gemeenschappelijke documentensysteem bij de provincie stond. Het betrof zijn eigen invulling van het Keuzeformulier ICT-middelen. Deze had hij ingevuld bij zijn indiensttreding. In het formulier stond zijn privé NAW-gegevens, privé telefoonnummer, privé mailadres en handtekening.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

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

[✓] Netwerkmappen of -locaties met persoonsgegevens zijn te breed toegankelijk ingesteld binnen de organisatie

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Een nieuwe medewerker van de PZH constateerde dat zijn telefoonnummer en andere privé persoonsgegevens in een openbare netwerk-map stond van de Servicedesk. Het betrof zijn eigen Keuzeformulier ICT-middelen die hij had

AUTORITEIT PERSOONSGEGEVENS

ingevuld bij zijn indiensttreding.
In het formulier stond zijn privé NAW-gegevens, privé telefoonnummer, privé mailadres en handtekening.

Bij onderzoek door de Eenheid Privacy is daarnaast ook het volgende gebleken:
• Het formulier staat in een voor alle medewerkers toegankelijke IDMS-map.
• Bijna 400 formulieren staan opgenomen in deze iDMS-map, over een periode van meerdere jaren.
• De iDMS-map staat vol met privé persoonsgegevens van vele medewerkers van de PZH en politieke ambtsdragers als Statenleden en Gedeputeerden.
• Veel formulieren bevatten handtekeningen. Die vallen, onder de categorie bijzondere persoonsgegevens.

• Deze formulieren zijn na uitgifte van ICT-middelen in deze hoedanigheid niet meer nodig en dienen te worden gewist, hetgeen niet is gebeurd.
• In de formulieren is richting de aanvrager niet aangegeven hoelang de Servicedesk deze gegevens bewaart.
De ontvanger van de ICT-middelen weet nu niet waar hij aan toe is.
• De verwerking is niet opgenomen in het verwerkingsregister van de PZH. Dit dient alsnog te gebeuren.

De eerste beperkende maatregel, het beperken van de toegang van de netwerk-map, is al genomen. Overige herstel- en verbeteracties, waaronder het informeren van de betrokkene worden de komende week uitgevoerd.

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

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] E-mailadres

[✓] Telefoonnummer

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

[✓] Biometrische gegevens (bijvoorbeeld: vingerafdruk of irisscan)

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk

AUTORITEIT PERSOONSGEGEVENS

398

Geef een toelichting op bovengenoemd aantal: In de netwerk-map stonden 398 ICT-keuzeformulieren opgeslagen.

7 Getroffen personen

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

Meerdere opties zijn mogelijk.

[✓] Werknemers

[✓] Anders

Namelijk: Politieke ambtsdragers als Gedeputeerden en Statenleden.

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen. Medewerkers van de Provincie Zuid-Holland.
Statenleden
Gedeputeerden.

7.3 Is het exacte aantal betrokkenen bekend? Ja

Het exacte aantal is: 398

8 Maatregelen vooraf

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

[✓] Nee

9 Gevolgen

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

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

AUTORITEIT PERSOONSGEGEVENS

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Identiteitsdiefstal of -fraude

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Een Kwaadwillende zou met de persoonsgegevens identiteitsfraude kunnen plegen, al is de kans hierop nihil.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Ja
Aan hoeveel personen wilt u de inbreuk gaan melden?	398
Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?	31-8-2023
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Verslag van wat is voorgevallen. Aangeven dat hun persoonsgegevens door alle collega's waren in te zien. Dat maatregelen zijn genomen. de openbare map is afgesloten voor onbevoegden.

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

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

Meerdere opties zijn mogelijk.

[✓] Per e-mail

AUTORITEIT
PERSOONSGEGEVENS

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	De toegang tot de netwerk-map is binnen 72 uur na het melden van het incident beperkt.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	De betrokkene worden zeer spoedig geïnformeerd. Overige compliancy tekortkomingen worden spoedig aangepakt.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: art.5.1-2e

Melddatum: 05 oktober 2023

Meldtijdstip: 17:27

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	art.5.1-2e

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	art.5.1-2e
Functie	Functionaris voor Gegevensbescherming
E-mailadres	art.5.1-2e @pz h.nl
Telefoonnnummer	art.5.1-2e
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

AUTORITEIT
PERSOONSGEGEVENS

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

[✓] Tijdlijn

5. Gegevens over de inbreuk

[✓] Aard van de inbreuk

[✓] Samenvatting van het incident

6. Betrokken persoonsgegevens

[✓] Welke persoonsgegevens

[✓] Hoeveelheid persoonsgegevens

7. Getroffen personen

[✓] Groep mensen dat getroffen is door de inbreuk?

[✓] Nadere omschrijving van de groep mensen dat getroffen is door de inbreuk.

[✓] Aantal personen die door de inbreuk zijn getroffen

8. Maatregelen vooraf

AUTORITEIT PERSOONSGEGEVENS

9. Gevolgen

[✓] Gevolgen voor de betrokkene(n) (Persoon of personen van wie gegevens zijn getroffen door de inbreuk)

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

[✓] Maatregelen om de inbreuk aan te pakken?

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	7-9-2023
Wanneer heeft u het datalek voor het eerst aan de AP gemeld?	8-9-2023
4.2 Wanneer is het incident ontdekt?	7-9-2023
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	De Chief Information Security Officer (CISO) heeft tijdens een steekproef ontdekt dat er mogelijk toegangsrechten tot het intern document management systeem te ruim staan ingesteld. Hij heeft hiervan melding gemaakt aan de FG.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over datalek

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.3 Beschrijving van het incident

AUTORITEIT
PERSOONSGEGEVENS

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	De CISO zocht in het intern document management systeem op de termen ‘curriculum vitae’ en ‘paspoort kopie’. Hij had vervolgens toegang tot documenten met diverse persoonsgegevens. Daarnaast zocht hij ook op de term ‘BIBOB’ en had vervolgens toegang tot documenten welke als 'vertrouwelijk' zijn aangemerkt. Een deel van die documenten bleek daadwerkelijk persoonsgegevens te bevatten. In de periode na de melding van 8 september aan de AP zijn er verschillende query’s uitgevoerd op de aan de AP gemelde zoektermen. Het Intern Document Management Systeem (IDMS) bevat ongeveer 50 miljoen documenten. Het zoeken met de aan de AP gemelde zoektermen levert ongefilterd 33.000 hits op die ofwel in de titel of wel in het document een van de zoektermen bevatten. Op dit moment worden deze hits beoordeeld. Van de tot nu toe doorzochte documenten zijn inmiddels 2.071 documenten gevonden die daadwerkelijk een curriculum vitae, Bibob-informatie of een kopie van een paspoort bevatten. Deze zijn ontoegankelijk gemaakt. De resterende hits worden zo snel als redelijkerwijs mogelijk is beoordeeld en zo nodig geïsoleerd. Het op 8 september gemelde datalek vormde voor ons aanleiding om een breder onderzoek in te stellen naar onnodige toegangsmogelijkheden tot persoonsgegevens in IDMS. Hieruit is gebleken dat er meer persoonsgegevens dan ons op 7 september bekend was, toegankelijk zijn voor medewerkers die hier voor de uitoefening van hun functie geen toegang toe behoeven. Hiervoor worden mitigerend maatregelen getroffen en voorbereid. Omdat het IDMS zo veel documenten bevat en een cruciaal onderdeel van ons bedrijfsproces vormt vergt dit tijd. De impact wordt beperkt door de omstandigheid dat het een INTERN systeem betreft en de data van de meest precaire bedrijfsprocessen zich reeds in ontoegankelijke afgeschermde mappen bevinden.

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

AUTORITEIT
PERSOONSGEGEVENS

6 Betrokken persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Geboortedatum en/of leeftijd

[✓] Burgerservicenummer (BSN)

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] E-mailadres

[✓] Telefoonnummer

[✓] Financiële gegevens

[✓] Bankrekeningnummer / IBAN

[✓] Creditcardgegevens

[✓] Andere financiële gegevens

Namelijk: salarisinformatie

[✓] (Kopieën van) paspoorten of andere legitimatiebewijzen

[✓] Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

[✓] Gegevens over iemands gezondheid

AUTORITEIT PERSOONSGEGEVENS

[✓] Biometrische gegevens (bijvoorbeeld: vingerafdruk of irisscan)

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	2,071
Geef een toelichting op bovengenoemd aantal:	Dit is het aantal documenten waarvan op dit moment is vastgesteld dat de toegangsrechten te ruim stonden ingesteld.

7 Betrokkenen

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

Meerdere opties zijn mogelijk.

[✓] Werknemers

[✓] Anders

Namelijk:	andere relaties van de provincie Zuid-Holland
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	werknemers en andere relaties
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	52
Het maximum aantal betrokkenen is:	10,000

9 Gevolgen

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Identiteitsdiefstal of -fraude

[✓] Financieel verlies

AUTORITEIT PERSOONSGEGEVENS

[✓] Reputatieschade

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Aanzienlijk
Licht uw keuze toe:	Uit de logbestanden van de gevonden documenten die daadwerkelijk een curriculum vitae, Bibob-informatie of een kopie van een paspoort bevatten, blijkt dat van de ruim 2000 documenten er het afgelopen jaar slechts 52 documenten (in totaal 141 keer) zijn geraadpleegd. Er zijn geen aanwijzingen dat documenten door onbevoegden zijn bekeken. Het datalek is niet door een willekeurig persoon gemeld, er is door de CISO naar gezocht. De informatie is alleen INTERN toegankelijk. Wij schatten het risico daarom beperkter in. Omdat het IDMS ook bijzondere persoonsgegevens bevat, hebben wij ervoor gekozen om het in dit formulier als “aanzienlijk” te categoriseren.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Ja
Aan hoeveel personen wilt u de inbreuk gaan melden?	52
Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?	31-12-2023
Licht toe aan welke (groep) betrokkenen u de inbreuk heeft gemeld:	Op dit moment hebben we de betrokkenen nog niet geïnformeerd. De aard van de inbreuk maakt dat complex. We gaan hierover graag, conform overweging 86 in de considerans van de AVG, in gesprek met de AP.

AUTORITEIT
PERSOONSGEGEVENS

Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Zie melding. We gaan graag in overleg. art.5.1-2e art.5.1-2e G, art.5.1-2e p zh.nl art.5.1-2e

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

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

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	nog niet bekend

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

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

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Op dit moment hebben we de betrokkenen nog niet geïnformeerd. De aard van de inbreuk maakt dat complex. We gaan hierover graag, conform overweging 86 in de considerans van de AVG, in gesprek met de AP.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Een groot aantal documenten met persoonsgegevens is inmiddels geïdentificeerd en geïsoleerd. Zoals eerder aangegeven gaat dit proces onverminderd voor en worden er andere mitigerende maatregelen voorbereid.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Er is reeds een fors bedrag (23 miljoen) vrijgemaakt om de informatiehuishouding te verbeteren. Er zijn reeds een drietal actielijnen

AUTORITEIT PERSOONSGEGEVENS

geformuleerd. In actielijn 1 ‘Bewustzijn en vaardigheden verhogen’ bevorderen we een cultuur waarin medewerkers gaan handelen in lijn met de kaders van ‘goed’ informatiebeheer en data/informatie-gedreven werken. Initiëren en ondersteunen van activiteiten die het I-bewustzijn bevorderen en bijdragen aan het gewenste gedrag van directie, regisseurs, managers en medewerkers. In actielijn 2 ‘Opzetten I-governance en I–control & optimaliseren werkwijze’ zorgen we voor de juiste sturende en ondersteunende processen om risico’s te vermijden en waarde te verhogen. Ontwerpen en implementeren van een I-governance en gesloten I-control-cyclus & het ontwikkelen van kaders en een werkwijze die bijdragen aan het sturen op gewenste resultaten. In actielijn 3 ‘Saneren en moderniseren IV-middelen, platformen en informatie’ zorgen we voor een adequaat instrumentarium voor het toekomstbestendig informatiebeheer en data/informatiegedreven werken. Saneren en verbeteren van middelen en informatie, zodat daarmee de strategische doelen meer passend ondersteund worden.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: art.5.1-2e

Melddatum: 07 februari 2023

Meldtijdstip: 13:51

1 Introductie

1.1 De melding van een inbreuk

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

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

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

1.3 Andere toezichthouders

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

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

AUTORITEIT
PERSOONSGEGEVENS

Registratienummer van de FG (indien van toepassing)	art.5.1-2e
Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596 AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Provincie

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	art.5.1-2e
Functie	Plaatsvervangend functionaris gegevensbescherming
E-mailadres	art.5.1-2e @p zh.nl
Telefoonnummer	art.5.1-2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Ja

Geef aan welke andere organisaties betrokken waren bij de inbreuk?

AUTORITEIT PERSOONSGEGEVENS

Naam	Op welke wijze betrokken	Toelichting (optioneel)
P8 Software	Leverancier/verwerker	

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	5-2-2023
(Mogelijke) einddatum van de inbreuk	5-2-2023
4.2 Wanneer is het incident ontdekt?	6-2-2023
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	De leverancier heeft per e-mail melding gemaakt van een ransomware aanval waarbij mogelijkerwijs data in handen van derden is gekomen.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

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

[✓] Hacking, malware (bijv. ransomware) en/of phishing

Meerdere opties zijn mogelijk binnen het gearceerde deel.

[✓] Ransomware

AUTORITEIT PERSOONSGEGEVENS

Heeft u (digitaal forensisch) onderzoek uitgevoerd of laten uitvoeren naar de aard en de omvang van het datalek?	Ja, het onderzoek loopt

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	P8 is slachtoffer geworden van een ransomware aanval. Op dit moment doet een forensisch onderzoeksbureau onderzoek of er data in handen van derden is gevallen.

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

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

- [✓] Naam
- [✓] Geslacht
- [✓] Geboortedatum en/of leeftijd
- [✓] Contactgegevens
- [✓] Adres en woonplaats
- [✓] E-mailadres
- [✓] Telefoonnummer
- [✓] Anders

Namelijk:	kvk-nummers

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

AUTORITEIT PERSOONSGEGEVENS

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Aantal niet duidelijk; betreft enkele honderden percelen met per perceel een aantal persoonsgegevens

7 Getroffen personen

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

Meerdere opties zijn mogelijk.

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	het betreft pachters en huurders van provinciale eigendommen
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1
Het maximum aantal betrokkenen is:	1,000

8 Maatregelen vooraf

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

[✓] Nee

9 Gevolgen

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

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

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

AUTORITEIT PERSOONSGEGEVENS

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Betrokkenen verliezen het overzicht van welke organisaties hun persoonsgegevens verwerken en worden verhinderd controle uit te oefenen

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Het betreft geen bijzondere persoonsgegevens en de gegevens zijn voor een groot deel reeds verouderd. Betreft voornamelijk NAM-gegevens, huurprijzen, pachtprijzen en kvk-nummers.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

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

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

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

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	het forensisch onderzoek is nog niet afgerond. Het is nog niet duidelijk of er daadwerkelijk sprake is van een datalek.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nog niet bekend

AUTORITEIT PERSOONSGEGEVENS

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nog niet bekend

11 Verzenden

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

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

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

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

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	6-3-2023

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: art.5.1-2e

Melddatum: 08 september 2023

Meldtijdstip: 09:56

1 Introductie

1.1 De melding van een inbreuk

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

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

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

1.3 Andere toezichthouders

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

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

AUTORITEIT
PERSOONSGEGEVENS

KvK-nummer (indien van toepassing)	27375169
Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Provincie

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	art.5.1-2e
Functie	Privacy Officer
E-mailadres	art.5.1-2e pz h.nl
Telefoonnummer	art.5.1-2e
Tweede telefoonnummer	
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

AUTORITEIT PERSOONSGEGEVENS

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	1-9-2023
4.2 Wanneer is het incident ontdekt?	7-9-2023
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Een medewerker heeft een melding gemaakt aan de FG.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

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

[✓] Netwerkmappen of -locaties met persoonsgegevens zijn te breed toegankelijk ingesteld binnen de organisatie

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Medewerker zocht in het intern document management systeem op de termen ‘curriculum vitae’ en ‘paspoort kopie’. Hij had vervolgens toegang tot diverse documenten met persoonsgegevens. Daarnaast zocht medewerker ook op de term ‘BIBOB’ en had vervolgens toegang tot documenten welke als 'vertrouwelijk' zijn aangemerkt en mogelijk persoonsgegevens bevatten.

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

AUTORITEIT
PERSOONSGEGEVENS

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

- [✓] Naam
- [✓] Geslacht
- [✓] Geboortedatum en/of leeftijd
- [✓] Contactgegevens
- [✓] Adres en woonplaats
- [✓] E-mailadres
- [✓] Telefoonnummer
- [✓] (Kopieën van) paspoorten of andere legitimatiebewijzen
- [✓] Onbekend

U moet binnen 4 weken een vervolgmelding indienen, waarin u aangeeft welke persoonsgegevens bij het datalek betrokken zijn.

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	50
Geef een toelichting op bovengenoemd aantal:	Omdat het via een algemene zoekterm aan ons is gemeld, moeten we nog verder onderzoek verrichten om te specificeren om hoeveel gegevensrecords het daadwerkelijk gaat.

7 Getroffen personen

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

AUTORITEIT PERSOONSGEGEVENS

Meerdere opties zijn mogelijk.

[✓] Werknemers

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Werknemers omvat de zoektermen kopie paspoort en cv. Klanten omvat (mogelijk) eveneens kopie paspoort en mogelijke BIBOB-documenten.
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	3
Het maximum aantal betrokkenen is:	100

8 Maatregelen vooraf

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

[✓] Nee

9 Gevolgen

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

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

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

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Identiteitsdiefstal of -fraude

9.3 Inschatting risico

AUTORITEIT PERSOONSGEGEVENS

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Aanzienlijk
Licht uw keuze toe:	Kopieën van CV's en paspoorten zijn enkel toegankelijk geweest voor iedere medewerkers van de provincie. Ondanks geheimhoudingsplicht kunnen we echter niet uitsluiten dat deze gegevens gebruikt worden voor niet-wettelijke doeleinden. In het geval van de BIBOB-documenten is de mogelijke impact nog niet duidelijk. We weten nog niet hoe lang en voor wie de map open heeft gestaan en welke documenten, en daarmee persoonsgegevens, erin hebben gezeten. Deze map is na het vaststellen van het datalek wel onmiddellijk dichtgezet.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

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

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

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

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Zie 10.1, impact is nog niet duidelijk

10.3 Maatregelen om de inbreuk aan te pakken

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

AUTORITEIT PERSOONSGEGEVENS

In het geval van de BIBOB-documenten is de map	dichtgezet. In het andere geval is dit nog niet
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nog niet bekend

11 Verzenden

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

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

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

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

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	5-10-2023

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: art.5.1-2e

Melddatum: 29 juli 2022

Meldtijdstip: 13:28

1 Introductie

1.1 De melding van een inbreuk

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

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

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

1.3 Andere toezichthouders

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

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

AUTORITEIT
PERSOONSGEGEVENS

KvK-nummer (indien van toepassing)	27375169
Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Provincie

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	art.5.1-2e
Functie	Coördinator eenheid Privacy / Privacy Officer
E-mailadres	privacy@pzh.nl
Telefoonnummer	art.5.1-2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Ja

Geef aan welke andere organisaties betrokken waren bij de inbreuk?

AUTORITEIT PERSOONSGEGEVENS

Naam	Op welke wijze betrokken	Toelichting (optioneel)
Gemeente Gorinchem Gemeente Halderberge	Zij kregen een mail met daarin een niet afgelakte naam van een burger.	

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	26-7-2022
(Mogelijke) einddatum van de inbreuk	26-7-2022
4.2 Wanneer is het incident ontdekt?	27-7-2022
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	De gemeenten Gorinchem en Halderberge hebben een mail gekregen van de provincie Zuid-Holland met daarin een naam van een burger. Deze naam had afgelakt/ doorgehaald dienen te worden en dat is niet gebeurt. Dit is twee dagen later door de medewerker zelf ontdekt.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

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

[✓] Overig

Namelijk:

AUTORITEIT PERSOONSGEGEVENS

Mail verstuurd aan twee gemeenten waarbij de naam van een burger niet is afgelakt/doorgehaald

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	De gemeenten Gorinchem en Halderberge hebben een mail gekregen van de provincie Zuid-Holland met daarin een naam van een burger. Deze naam had afgelakt/ doorgehaald dienen te worden en dat is niet gebeurt.

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

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Alleen de achternaam. Niet de voornaam of voorletters. Geen overige contactgegevens.

7 Getroffen personen

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

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	één burger

AUTORITEIT PERSOONSGEGEVENS

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	De naam van één burger is gedeeld.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	1

8 Maatregelen vooraf

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

[✓] Nee

9 Gevolgen

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

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Niet bekend of het gevolgen heeft. De betreffende gemeenten is gevraagd de mail te verwijderen.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja

AUTORITEIT PERSOONSGEGEVENS

Aan hoeveel personen heeft u de inbreuk gemeld?	2
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	29-7-2022
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	De betreffende gemeenten is gemeld de mail te vernietigen.

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

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

Meerdere opties zijn mogelijk.

[✓] Telefonisch

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Contact op genomen met betreffende gemeenten, dat ze de mail moeten vernietigen.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Bij de medewerkers van het bureau voorlichting gegeven dat dit type delen niet is toegestaan.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk
Geef aan wanneer u (uiterlijk) een vervolgmelding doet	1-10-2022
Toelichting	Het voorval wordt nog onderzocht.

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

AUTORITEIT
PERSOONSGEGEVENS

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

art.5.1-2e

Van: art.5.1-2e
Verzonden: 6 :
Aan: art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e
CC: art.5.1-2e
Onderwerp: art.5.1-2e heeft 20200520_ Advies_in_het_kader_van_meldplicht_datalekken met u ged

Hoi art.5.1-2e

Ik heb op de e-mail van art.5.1-2e gereageerd. De 400 privételefoonnummers dienen geen doel en kunnen daarom gewist worden. Lijkt me goed om hier dinsdag over te spreken. Onze collega's hoeven dan niet uit te zoeken wie welke kleur heeft gebruikt .

Groeten,
art.5.1-2e

Van: art.5.1-2e < art.5.1-2e @ pzh.nl>
Verzonden: vrijdag 22 mei 2020 15:58
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 >
CC: art.5.1-2e < art.5.1-2e @ pzh.nl>
Onderwerp: RE: art.5.1-2e heeft 20200520_Advies_in_het_kader_van_meldplicht_datalekken met u gedeeld.

Hoi art.5.1-2e

Even een kleurtje zoeken.... Paars dan maar

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: vrijdag 22 mei 2020 15:49
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: art.5.1-2e < art.5.1-2e @ pzh.nl>; art.5.1-2e < art.5.1-2e @pzh .nl>
Onderwerp: RE: art.5.1-2e heeft 20200520_Advies_in_het_kader_van_meldplicht_datalekken met u gedeeld.

Hi art.5.1-2e

In oranje mijn reactie.

Groeten,
art.5.1-2e

Van: art.5.1-2e <art.5.1-2e @ pzh.nl>
Verzonden: vrijdag 22 mei 2020 11:56
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: art.5.1-2e <art.5.1-2e @ pzh.nl>; art.5.1-2e <art.5.1-2e @pzh .nl>
Onderwerp: RE: art.5.1-2e heeft 20200520_Advies_in_het_kader_van_meldplicht_datalekken met u gedeeld.

Hoi art.5.1-2e

Dan ga ik in het rood verder

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: vrijdag 22 mei 2020 11:39
Aan: art.5.1-2e <art.5.1-2e @ pzh.nl>; art.5.1-2e <art.5.1-2e pzh. nl>; art.5.1-2e <art.5.1-2e @pzh .nl>
Onderwerp: RE: art.5.1-2e heeft 20200520_Advies_in_het_kader_van_meldplicht_datalekken met u gedeeld.

Goedemorgen art.5.1-2e

Hartelijk dank voor je snelle reactie! Hieronder in **groen** mijn reactie.

Groeten,
art.5.1-2e

Van: art.5.1-2e <art.5.1-2e @ pzh.nl>
Verzonden: vrijdag 22 mei 2020 11:06
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: art.5.1-2e heeft 20200520_Advies_in_het_kader_van_meldplicht_datalekken met u gedeeld.

Goedemorgen art.5.1-2e

Het lijkt mij op zich een goed advies.

Ten aanzien van de te treffen maatregelen: begrijp ik goed dat de privénummers die vanuit het Binnenplein komen blijven bestaan en alle overige privénummers worden gewist?
Privénummers die voor het doel 'bereikbaarheid' op het Binnenplein zijn geplaatst blijven staan. Privénummers die voor MFA zijn gebruikt worden gewist.

Denk je aan de mail van art.5.1-2e van 12:46u? Bij de te nemen maatregelen is dat wel iets ter overweging, in de zin van aanvullende maatregelen.

Dan heb ik nog een vraag terzijde over de KRM. Dit is denk ik de tweede keer dat ik dit "systeem" hoor noemen in de anderhalf jaar dat ik bij PZH werk. Het is mij niet duidelijk wat dit voor systeem is. Ik kan het niet vinden in het verwerkingsregister.
De vraag blijft voor mij nog wel staan wat de KRM nou precies is. Maar wellicht dat art.5.1-2e daar uitsluitsel over kan geven.
Dat roept wel een volgende vraag op. Je geeft aan dat de gegevens vanuit KRM worden gesynchroniseerd met andere systemen. In hoeverre worden hierdoor de privénummers ook verwerkt in andere systemen waarvoor wellicht geen grondslag is? De uitwisseling van privénummers door KRM is verenigbaar met het oorspronkelijke verwerkingsdoel: bereikbaarheid (denk ik).
Hebben wij dan wel al duidelijk in beeld met welke andere systemen er gegevens worden uitgewisseld?

Ik heb enkele vragen uitstaan om bovenstaande uit te zoeken. Excuses ik had misschien in mijn vorige e-mail aan moeten geven dat ik actie ondernomen heb.

Prima, we wachten de antwoorden af.

Ik heb qua argumentatie voor het wel of niet melden bij de AP alleen mijn bedenkingen bij het gedeelte waar je het hebt over de betrouwbaarheid van de medewerkers en het feit dat zij gebonden zijn aan een geheimhouding. Dat argument speelt wat mij betreft een ondergeschikte rol. Ik wil daarmee overigens niet aangeven dat de medewerkers per definitie niet betrouwbaar zouden zijn. Wat ik ermee wil aangeven is, dat het voor mij geen onderscheidende factor is. Heel zwartwit gezegd (en ik weet dat er genoeg uitzonderingen op te bedenken zijn, maar het gaat even om het grote plaatje), dat zou dan dus inhouden dat eigenlijk zelden of nooit een inbreuk gemeld hoeft want er is geen hoog risico vanwege de eed of belofte…. De eed of belofte is m.i. een aardige stok achter de deur in arbeidsrechtelijk opzicht, maar is als argument voor de AVG niet sterk.
Volgens het document *'Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679'* speelt betrouwbaarheid wel degelijk een rol. Ik heb mij laten inspireren door de informatie op bladzijde 29 onder paragraaf *'ernst van gevolgen voor personen'*. Link naar het document:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf
Ik begrijp je onderbouwing, maar er staat op diezelfde pagina ook: "Nogmaals, dit verschilt van geval tot geval". Met andere woorden, in mijn visie is dat geen automatisme, geen zekerheidje en zal ik daar iedere keer weer op terugkomen. De WP29 maakt her en der in de tekst op deze pagina nog wel meer voorbehouden. Maar het mag zeker worden meegewogen!

Eens dat het van geval tot geval verschilt.

PS. Ik denk dat het goed is als art.5.1-2e wordt meegenomen in deze gedachtengang, aangezien hij over een paar weken het stokje overneemt van art.5.1-2e en art.5.1-2e aangezien het datalek ogenschijnlijk ook een verbinding heeft met P&O.
Ik ben zo vrij om ze nu maar in de CC te zetten

Oké

We kunnen dinsdag in het privacy team deze casus nog wel aan de orde laten komen, en dan met name ook de nog openstaande vragen en de vragen die wat meer hoog over gaan meenemen. En @ art.5.1-2e , misschien wil art.5.1-2e dan wat meer vertellen over KRM.

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: vrijdag 22 mei 2020 10:18
Aan: 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 >
Onderwerp: art.5.1-2e heeft 20200520_Advies_in_het_kader_van_meldplicht_datalekken met u gedeeld.

art.5.1-2e **ne eft een bestand met u gedeeld**

Beste collega's,

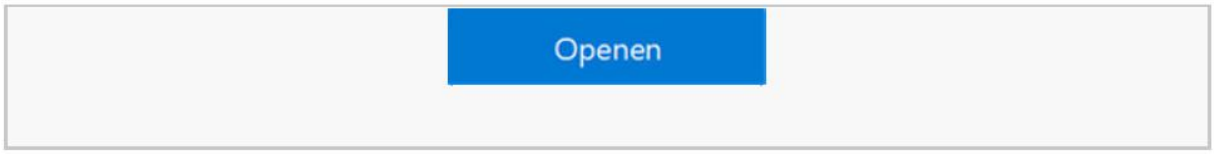
Er heeft zich, naar mijn mening, een datalek voorgedaan. Via onderstaande link is het adviesdocument te openen. Mag ik jullie feedback (op zowel taal als inhoud) ontvangen?

Alvast hartelijk dank!

Groeten,
art.5.1-2e

20200520_Advies_in_het_kader_van_meldplicht_datalekken

Deze koppeling werkt alleen voor de directe geadresseerden van dit bericht.



Privacyverklaring

Diefstal of vermissing ICT middel

LET OP ! Dit formulier is uitsluitend bedoeld om een diefstal of een vermissing te melden van een ICT middel.
Meld de diefstal of vermissing z.s.m.:
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in
dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de
Autoriteit Persoonsgegevens o.b.v. het Protocol meldplicht datalekken

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	
E-mail	art.5.1-2e pzh.nl
Organisatie-eenheid	Inkoop
Kostenplaatscode	372

Benodigde gegevens

Is dit een diefstal of vermissing?	Vermissing
Eigenaar van het verloren/gestolen voorwerp:	De Provincie Zuid-Holland
Wat is er gestolen/vermist:	Laptop
Bij een apparaat van de PZH. Wat is het CI nummer?	9ZNH2Z2
Bij een smartphone van de PZH. Wat is het 06 nummer?	art.5.1-2e
Locatie, datum en tijdstip van vermissing, indien bekend?	PZH hoofdkantoor, C gebouw 3e etage, 17.03 uur
Bij een smartphone van de PZH: Was het vergrendelingsscherm voorzien van een pincode of wachtwoord?	Onbekend
Bij een smartphone van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer pincode of wachtwoord geactiveerd)?	Onbekend
Bij een laptop/tablet van de PZH: Was het apparaat op het moment van verlies of diefstal vergrendeld (invoer wachtwoord geactiveerd)?	Ja

Staan er PZH-, vertrouwelijke- of persoonsgegevens op het apparaat?	Ja
Zo ja? Om welke gegevens gaat het?	werkzaamheden en prive
Zijn de gegevens versleuteld?	Nee
Stond het apparaat uitgeschakeld ten tijde van de diefstal of vermissing?	Ja
Toelichting (beschrijf de gebeurtenis, zijn er getuigen? etc.):	Na afloop van een vergadering in de vergaderzaal Beresteijn op C3 ben ik naar een toilet voor dames geweest die om de hoek op c3 bij de vergaderzaal zich bevindt. Daarna naar de parkeergarage. tijdens het overleg heb ik mijn laptop gebruikt. Daarna zag ik hem neit meer terug.

Van: art.5.1-2e
Verzonden: 2023-09-29 15:53:30+00:00
Aan: art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e
CC: art.5.1-2e
Onderwerp: RE: art.5.1-2e heeft 'Memo beschrijving iDMS' met u gedeeld
"
Ik zal het iDMS document nu definitief gaan maken. Mocht je toch nog wat aan willen passen, bel dan art.5.1-2e Ik moet zo mijn zoon wegbrengen.

Er is wat gedoe met de opmaak dus ik moet het in een nieuw document zetten.

Groet,

art.5.1-2e

Van: art.5.1-2e < art.5.1-2e pzh.nl>
Verzonden: vrijdag 29 september 2023 14:46
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 < 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: art.5.1-2e heeft 'Memo beschrijving iDMS' met u gedeeld

Dank je art.5.1-2e ik heb één inhoudelijke toevoeging gedaan over het beleid vertrouwelijke gegevens uit 2009. De actualisatie daarvan is langs het MT I&A geweest en gaat (met wat aanpassingen) door naar het DT. Dit betreft ook het open tenzij-beleid.

Groet,

art.5.1-2e

art.5.1-2e | CISO | 06 5155 9173

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Datum: vrijdag, 29 september 2023 om 14:34
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 < art.5.1-2e pzh.nl <mailto: art.5.1-2e pzh.nl> >, art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl <mailto: art.5.1-2e pzh.nl> >, art.5.1-2e < art.5.1-2e pzh.nl <mailto: art.5.1-2e pzh.nl> >, art.5.1-2e < art.5.1-2e pzh.nl <mailto: art.5.1-2e pzh.nl> >
Onderwerp: art.5.1-2e heeft 'Memo beschrijving iDMS' met u gedeeld

art.5.1-2e heeft een bestand met u gedeeld

Hoi allen,
Hierbij de bijlage over iDMS. @ art.5.1-2e @ art.5.1-2e zouden jullie je review nog willen geven voordat alles wordt doorgezet naar art.5.1-2e

<https://eur03.safelinks.protection.outlook.com/ap/w-59584e83/?url=https%3A%2F%2Fpzh-my.sharepoint.com%2F%3Aw%3A%2Fg%2Fpersonal art.5.1-2e _nl%2FEcCAyVHc-S1Pjl62j61hnbQBAXSaaRpv6SKNFzs4mnhv5Q% 0Y3%26fromShare%3Dtrue%26at%3D9&data=05%7C01% art.5.1-2e art.5.1-2e 40pzh.nl%7C5815899b1d664f5fd7e708dbc0f 5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638315924124405251%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=r3%2FB2Z6bm6dIieV19v6s%2BdUfVs5zr0QdarONDZRH4ew%3D&reserved=0>

Memo beschrijving iDMS <https://eur03.safelinks.protection.outlook.com/ap/w-595 s%3A%2F%2Fpzh-my.sharepoint.com%2F%3Aw%3A%2Fg%2Fpersonal %2 art.5.1-2e l%2FEcCAyVHc-S1Pjl62j61hnbQBAXSaaRpv6SKNFzs4mnhv5Q%3Fe %3D4%253ag4p0Y3%26fromShare%3Dtrue%26at%3D9&data=05%7C01 art.5.1-2e art.5.1-2e 40pzh.nl %7C5815899b1d664f5fd7e708dbc0f376e5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7 C638315924124405251%7CUnknown %7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3 D%7C3000%7C%7C%7C&sdata=r3%2FB2Z6bm6dIieV19v6s%2BdUfVs5zr0QdarONDZRH4ew %3D&reserved=0>

Deze koppeling werkt alleen voor de directe geadresseerden van dit bericht.

<https://eur03.safelinks.protection.outlook.com/ap ttps%3A%2F %2Fpzh-my.sharepoint.com%2F%3Aw%3A%2Fg%2Fpersonal%2 art.5.1-2e %2FEcCAyVHc-S1Pjl62j61hnbQBAXSaaRpv6SKNFzs4mnhv5Q%3Fe%3D4%253ag4p0Y3%26fromShare %3Dtrue%26at%3D9&data=05%7C01 art.5.1-2e art.5.1-2e 40pzh.nl %7C5815899b1d664f5fd7e708dbc0f376e5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7 C638315924124405251%7CUnknown %7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3 D%7C3000%7C%7C%7C&sdata=r3%2FB2Z6bm6dIieV19v6s%2BdUfVs5zr0QdarONDZRH4ew %3D&reserved=0>

Privacyverklaring <https://eur03.safelinks.protection.outlook.com/?url=https%3A %2F%2Fprivacy.microsoft.com%2Fprivacystatement%2F&data=05%7C01 art.5.1-2e art.5.1-2e %40pzh.nl %7C5815899b1d664f5fd7e708dbc0f376e5%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7 C638315924124405251%7CUnknown %7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3 D%7C3000%7C%7C%7C&sdata=M9LmUjBVBghd1CD1IfXj6qY067z4eIH97Uv3tQxu0OI %3D&reserved=0>

"

"Van: art.5.1-2e
Verzonden: 2019-11-14 11:12:07.307000+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 en 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.5.1-2epzh.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.5.1-2epzh.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 <mailto : art.5.1-2epzh.nl> >
Verzonden: donderdag 14 november 2019 10:44
Aan: art.5.1-2e <art.5.1-2epzh.nl <mailto : art.5.1-2epzh.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.5.1-2epzh.nl <mailto:art.5.1-2epzh.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 <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: 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 Willy.

Mvg, art.5.1-2e
"


provincie
ZUID HOLLAND

"Van: art.5.1-2e
Verzonden: 2019-11-14 10:45:08+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 <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: 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: 2020-01-24 18:07:08+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 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 L
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 secret es die nu niet aanwezig was.
   Dit was bijvoorbeeld het geval bij art.5.1-2e 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 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 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 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 18:27:11+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
"

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 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: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 art.5.1-2e pzh.nl <mailt o art.5.1-2e pzh.nl> >; art.5.1-2e L
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.5.1-2e 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 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 18:42:53+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 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: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> >; art.5.1-2e L
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.5.1-2e art.5.1-2e ie als afdelingshoofd ook als contactpersoon was opgevoerd.

In zijn geval: inloggegevens voor het netwerk en voor bepaalde websites en zijn e-sign code.
Bij enkele andere contactpersonen: zagen we ook inloggegevens en hier en daar een geboortedatum.
Is besproken met de aanwezige secretaresses en met art.5.1-2e 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: Zoete - van der Hout, WH, de"
Verzonden: 2020-01-24 23:47:31+00:00
"Aan: art.5.1-2e art.5.1-2e art.5.1-2e
"CC: art.5.1-2e art.5.1-2e
Onderwerp: Re: Aankondiging: adviesrapporten 2 datalekken komen er aan
"
Dank voor het melden en de genomen acties!

Willy de Zoete

Van: art.5.1-2e <art.5.1-2epzh.nl>
Verzonden: vrijdag, januari 24, 2020 6:42 PM
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.5.1-2epzh.nl>
Sent: Friday, January 24, 2020 6:27:11 PM
To: art.5.1-2e <art.5.1-2epzh.nl>; art.5.1-2e <art.5.1-2epzh.nl>
Cc: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl>; art.5.1-2e
<art.5.1-2epzh.nl>; art.5.1-2e art.5.1-2epzh.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.5.1-2epzh.nl>
Verzonden: vrijdag 24 januari 2020 18:07
Aan: art.5.1-2e <art.5.1-2epzh.nl>; art.5.1-2e <art.5.1-2epzh.nl>
CC: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl>; art.5.1-2e
<art.5.1-2epzh.nl>; art.5.1-2e <art.5.1-2epzh.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 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: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> >; art.5.1-2e L 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 secre es die nu niet aanwezig was.
   Dit was bijvoorbeeld het geval bij art.5.1-2e 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 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: 2023-09-28 12:57:42+00:00
Aan: art.5.1-2e
CC: art.5.1-2e art.5.1-2e
Onderwerp: RE: Acties TAB ivm dataonderzoek
"
Hoi art.5.1-2e

Het is inmiddels gelukt. Ik had de verkeerde ids gepakt. Nu met de juiste ids en jouw query ging het inderdaad goed.

Groet,

art.5.1-2e

Van: art.5.1-2e pzh.nl>
Verzonden: donderdag 28 september 2023 09:46
Aan: art.5.1-2e < art.5.1-2e pzh.nl>
Onderwerp: RE: Acties TAB ivm dataonderzoek

We moeten even kijken naar de excelsheet. Want deze lijkt niet volledig

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Verzonden: woensdag 27 september 2023 14:51
Aan: 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> >; art.5.1-2e art.5.1-2e
Agatz < art.5.1-2e h.nl <mailto : art.5.1-2e pzh.nl> >
Onderwerp: Acties TAB ivm dataonderzoek

Hoi art.5.1-2e

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

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

M23 09 03059 auditlog 4 dossiers

Verzoek om auditlog van de te isoleren stukken volgt nog.

Dank je wel alvast art.5.1-2e

Met vriendelijke groet,

art.5.1-2e

Functioneel Beheer

art.5.1-2e

"

Van: art.5.1-2e
Verzonden: 2023-09-14 10:04:05+00:00
Aan: art.5.1-2e art.5.1-2e
CC:
Onderwerp: RE: Additioneel onderzoek iDMS nav zeer ernstig datalek
"
Ha art.5.1-2e

Ah, wat fijn! Dank je!

Ik snap dat de timing allerminst prettig is en dat ik jullie hier zo mee overval, maar zoals je in de aangeleverde lijst waarschijnlijk al hebt gezien betreft het datalek mede Bibob-dossiers met zéér gevoelige informatie.

Bij voorbaat dank!

Met vriendelijke groet,

art.5.1-2e

Privacy Officer

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protecti
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7 art.5.1-2e
%40pzh.nl%7C8f4c16a8aa934cead88808dbb4f92a5f
%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638302754486711048%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=E%2B0OeMQV%2FW2btHDWzMa4aOWZv%2BtH%2FECiJnUJaaiY%2FMc
%3D&reserved=0>

Werkdagen: ma, di, wo, do

Elke dag beter. Zuid-Holland.

Van: art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl>
Verzonden: donderdag 14 september 2023 09:46

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>
Onderwerp: RE: Additioneel onderzoek iDMS nav zeer ernstig datalek

Hi art.5.1-2e

Ik ga kijken of ik dit met het team kan bespreken en kom dan even bij je terug.

Vanmiddag laat ik het je weten.

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Verzonden: dinsdag 12 september 2023 16:27
Aan: art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl
<mailto: art.5.1-2e pzh.nl> >
CC: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e
< art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Onderwerp: Additioneel onderzoek iDMS nav zeer ernstig datalek
Urgentie: Hoog

Goedemiddag art.5.1-2e

Tgv een zeer ernstige serie datalekken in iDMS heeft de FG mij dringend verzocht om, in het verlengde van het eerder verrichtte onderzoek, met spoed extra onderzoek te laten verrichten naar vrij toegankelijke persoonsgegevens in iDMS. Zodoende kom ik bij jullie uit.

Kunnen jullie een PowerBI-visualisatie creëren van de volgende additionele zoektermen, inclusief de iDMS-locatie van de gevonden bestanden?

* curriculum+vitae
* cv
* kopie+curriculum+vitae
* kopie+cv

(verfijnen op pdf, doc, docx en msg)

* paspoort

(verfijnen op pdf, jpg, jpeg, png en msg)

* bibob+vertrouwelijk
* bibob+weigeren
* bibob+intrekken
* bibob+ernstig+gevaar
* bibob+gevaarsbeoordeling

* bibob+strafbaar
* bibob+strafbare

Is het mogelijk om dit binnen een week te realiseren? Ivm de meldingstermijn van de Autoriteit Persoonsgegevens zullen wij zeer spoedig moeten handelen.

Bij voorbaat dank!

Met vriendelijke groet,

art.5.1-2e

Privacy Officer

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art.5.1-2e %40pzh.nl%7C8f4c16a8aa934cead88808dbb4f92a5f%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638302754486711048%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=E%2B0OeMQV%2FW2btHDWzMa4aOWZv%2BtH%2FECiJnUJaaiY%2FMc%3D&reserved=0>

Werkdagen: ma, di, wo, do

Elke dag beter. Zuid-Holland.

"


provincie
Zuid-Holland

"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.5.1-2epzh.nl>
Sent: Friday, January 10, 2020 10:36:50 AM
To: art.5.1-2e <art.5.1-2epzh.nl>
Cc: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl>; art.5.1-2e <art.5.1-2epzh.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.5.1-2epzh.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

art.5.1-2e

Van: Zoete - van der Hout, WH, de
Verzonden: 2 01
Aan: art.5.1-2e 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

Gevoeligheid: Vertrouwelijk

Zelfde geldt voor mij. Fijn om zo goed op de hoogte gehouden te worden.

Willy de Zoete

Van: art.5.1-2e <art.5.1-2e @pzh. nl>
Verzonden: Friday, May 29, 2020 10:59:36 AM
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 @p zh.nl>
Onderwerp: RE: Advies aan concerndirecteur in het kader van de meldplicht datalekken
SUPER! Ik ben gerustgesteld .

Van: art.5.1-2e <art.5.1-2e @ pzh.nl>
Verzonden: vrijdag 29 mei 2020 10:59
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 @p zh.nl>
Onderwerp: RE: Advies aan concerndirecteur in het kader van de meldplicht datalekken
Gevoeligheid: Vertrouwelijk
Dag art.5.1-2e
Terechte vragen!
Gelukkig is daar al op voorgesorteerd.
Er is een groepje medewerkers, onder leiding van art.5.1-2e met GSO n DBI, hier al sinds de ontdekking mee bezig geweest. Zij hebben oo art.5.1-2e geïnformeerd met het verzoek de betreffende gedeputeerde op de hoogte te houden.
De advocaat van betrokkene wordt ook regelmatig geïnformeerd door de advocaat van Pels Rijcken die namens de provincie op dit dossier zit.
Het voorstel aan Hennie vanuit die groep is om binnenkort een excuusbrief naar de betrokkene te sturen.
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: vrijdag 29 mei 2020 10:50
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> art.5.1-2e art.5.1-2e pzh .nl>
Onderwerp: RE: Advies aan concerndirecteur in het kader van de meldplicht datalekken
Gevoeligheid: Vertrouwelijk

Helder, ik volg het advies.
Ik vind dit wel een dingetje… Twee aanvullende zaken:

- Normaliter zou de getroffene geïnformeerd moeten worden, maar die weet er al van begrijp ik omdat de advocaat in het verweer is gekomen. Ik mag toch aannemen dat er goed met de advocaat wordt gecommuniceerd, maar mogelijk moet dat (ook) vanuit de inhoudelijke medewerkers ipv alleen vanuit datalek-perspectief. Mag ik daar een reactie op.
- Vanuit de inhoud lijkt me dat dit moet worden opgeschaald. Is het betreffende management op de hoogte van deze misser? Dan kan mogelijk ook de bestuurder geïnformeerd worden. Ik hoor graag terug hierover.

Hartelijke groet, art.5.1-2e

Van: art.5.1-2e <art.5.1-2e pzh. nl>
Verzonden: vrijdag 29 mei 2020 10:28
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>; art.5.1-2e art.5.1-2e @pzh .nl>
Onderwerp: Advies aan concerndirecteur in het kader van de meldplicht datalekken
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste art.5.1-2e
Bijgaand het aangekondigde advies over het datalek dat gisteren is gemeld.
Het advies is afgestemd met onze FG en met art.5.1-2e bij de afhandeling betrokken als privacy officer van DBI.
Zoals gebruikelijk is het datalek geregistreerd in onze provinciale administratie.
Het advies is om dit datalek te melden aan de Autoriteit Persoonsgegevens.
Ik hoor graag of je hiermee instemt.
Met vriendelijke groet,
art.5.1-2e art.5.1-2e

Van: art.5.1-2e
Verzonden: donderdag 28 mei 2020 17:15
Aan: art.5.1-2e <art.5.1-2e @pzh. nl>
CC: Zoete - van der Hout, WH, de <wh.de.zoete@pzh.nl>; art.5.1-2e <art.5.1-2e @pzh. nl>
Onderwerp: Datalek in behandeling

Hallo art.5.1-2e
Het Privacyteam heeft een datalek in behandeling.
Het betreft een vaststellingsbesluit met persoonsgegevens dat per ongeluk door GSO op de provinciale website is gepubliceerd.
Het besluit is inmiddels van de provinciale website verwijderd, maar is op dit moment nog zichtbaar in het webarchief van de provincie (https://zuidholland.archiefweb.eu) en enkele regels zijn nog zichtbaar in de zoekresultaten van Google.
Hier wordt actie op ondernomen.
Het adviesrapport volgt morgenochtend.
Met vriendelijke groet,

art.5.1-2e
Adviseur informatieveiligheid
Afdeling Informatisering & Automatisering
T art.5.1-2e | **M** art.5.1-2e
art.5.1-2e 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
Verzonden: 2019-04-03 11:07:03+00:00
"Aan: art.5.1-2e
"CC: art.5.1-2e Baljeu, J.N."
Onderwerp: RE: Advies datalek
"
Hallo allen,

Ik heb het datalek vanochtend gemeld aan de AP.

Ter informatie bijgaand de ontvangstbevestiging inclusief het meldingsformulier.

Met vriendelijke groet, art.5.1-2e

Van: art.5.1-2e
Verzonden: dinsdag 2 april 2019 19:13
Aan: art.5.1-2e
CC: art.5.1-2e Baljeu, J.N.
Onderwerp: Re: Advies datalek

Hoi art.5.1-2e

Een grensgeval mijns inziens mbt wel of niet melden aan de AP. Je overweging dat betrokkene het zelf als heftig ervaart én omdat hij heeft aangegeven het zelf aan de AP te melden, brengt me ertoe in te stemmen met je advies.

Hartelijke groet, art.5.1-2e

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

On Tue, Apr 2, 2019 at 6:14 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

Zoals je weet heeft een burger geklaagd bij art.5.1-2e over het feit dat de provincie een door hem in 2008 ingezonden stuk (in de vorm van een e-mail) heeft gepubliceerd in het Staten Informatie Systeem.

Het stuk is inmiddels gedepubliceerd en de betrokkene is hierover geïnformeerd.

Conform de procedure voor het afhandelen van datalekken brengt het privacyteam advies aan jou uit over het al dan niet melden van dit datalek aan de Autoriteit Persoonsgegevens (AP). Ook informeer ik hierbij Jeannette.

In het advies kun je lezen dat we de aard van de persoonsgegevens niet zodanig inschatten dat er sprake is van een risico voor de rechten en vrijheden van de betrokken persoon.

En toch adviseren we om het te melden bij de AP.

Daarbij wegen we mee dat de betrokkene het datalek ervaart als een forse inbreuk op zijn privéleven.

Ook zullen we ons beraden of SIS informatie van collegeperioden in het verdere verleden op de website moeten blijven staan.

Ik hoor graag of je het advies volgt.

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

Postbus 90602 | 2509 LP Den Haag

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


provincie
ZUID HOLLAND

AUTORITEIT PERSOONSGEGEVENS

Meldloket

Ontvangstbevestiging

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

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

  Tijdstip ontvangst
  03-04-2019 10:51:11
  Uniek nummer
  art.5.1-2e

---

0. Over deze melding

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

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

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

Wie meldt het datalek?

Naam
art.5.1-2e
Functie
Adviseur informatieveiligheid
E-mailadres
art.5.1-2e pzh.nl
Telefoonnummer
art.5.1-2e mmer
art.5.1-2e

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

De melder is contactpersoon
Ja

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?
Nee

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend
09-04-2008
Startdatum van de periode waarbinnen de inbreuk was
09-04-2008
Einddatum van de periode waarbinnen de inbreuk was
01-04-2019
Duurt de inbreuk op dit moment nog voort?
Nee
Wanneer werd de inbreuk ontdekt?
01-04-2019

3. Gegevens over het datalek

3.1 Aard van de inbreuk

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

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?
Overig
Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest
Betreft een e-mail van betrokkene aan de provincie die in 2008 als ingezonden stuk in het Staten Informatie Systeem is gepubliceerd en daarmee publiek toegankelijk is geworden. De e-mail bevat e-mailadres, naam, adres en telefoonnummer van betrokkene.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

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

Nee

4.2 Bijzondere categorieën van persoonsgegevens

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

4.3 Hoeveelheid persoonsgegevens

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

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

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

Nee
Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
Betrokkene heeft in 2008 een e-mail als ingezonden stuk aan de provincie gestuurd.
Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
1
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
1

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

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

7. Gevolgen van het datalek

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

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

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

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

Discriminatie
Nee
Identiteitsdiefstal of -fraude
Nee
Financiële verliezen
Nee
Reputatieschade
Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens
Nee
Ongeoorloofde ongedaanmaking van pseudonimisering
Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen
Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen
Nee
Andere gevolgen, namelijk:
Op basis van contactgegevens, zou betrokkene benaderd kunnen worden. Het is ons niet bekend of dit daadwerkelijk is gebeurd. Betrokkene heeft aangegeven inmiddels een ander e-mailadres te hebben. Betrokkene ervaart de situatie als een forse inbreuk op zijn privéleven.
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen
1. Verwaarloosbaar

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?
Ja
Wanneer heeft u het datalek gemeld aan de betrokkenen?
01-04-2019
Wat is de inhoud van de melding aan de betrokkenen?
Betrokkene heeft zelf op 01-04-2019 contact opgenomen met de FG van de provincie . Daarna is er contact geweest over de afhandeling.
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?
1

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?
telefoon

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
De betrokkene is op 2 april 2019 geïnformeerd dat de e-mail uit het Staten Informatie Systeem is verwijderd. De functionaris gegevensbescherming heeft betrokkene geinformeerd dat melding bij de Autoriteit Persoonsgegevens gedaan wordt.

8.3 Internationale aspecten

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

9. Overig

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

---

"Van: art.5.1-2e
Verzonden: 2019-04-02 19:12:59+00:00
"Aan: art.5.1-2e
"CC: art.5.1-2e Baljeu, J.N."
Onderwerp: Re: Advies datalek
"
Hoi art.5.1-2e

Een grensgeval mijns inziens mbt wel of niet melden aan de AP. Je overweging dat betrokkene het zelf als heftig ervaart én omdat hij heeft aangegeven het zelf aan de AP te melden, brengt me ertoe in te stemmen met je advies.

Hartelijke groet, art.5.1-2e

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

On Tue, Apr 2, 2019 at 6:14 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

Zoals je weet heeft een burger geklaagd bij art.5.1-2e over het feit dat de provincie een door hem in 2008 ingezonden stuk (in de vorm van een e-mail) heeft gepubliceerd in het Staten Informatie Systeem.

Het stuk is inmiddels gedepubliceerd en de betrokkene is hierover geïnformeerd.

Conform de procedure voor het afhandelen van datalekken brengt het privacyteam advies aan jou uit over het al dan niet melden van dit datalek aan de Autoriteit Persoonsgegevens (AP). Ook informeer ik hierbij Jeannette.

In het advies kun je lezen dat we de aard van de persoonsgegevens niet zodanig inschatten dat er sprake is van een risico voor de rechten en vrijheden van de betrokken persoon.

En toch adviseren we om het te melden bij de AP.

Daarbij wegen we mee dat de betrokkene het datalek ervaart als een forse inbreuk op zijn privéleven.

Ook zullen we ons beraden of SIS informatie van collegeperioden in het verdere verleden op de website moeten blijven staan.

Ik hoor graag of je het advies volgt.

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/>

"


provincie
ZUID HOLLAND

"Van: Baljeu, J.N."
Verzonden: 2019-07-25 15:51:39+00:00
"Aan: art.5.1-2e art.5.1-2e
CC:
Onderwerp: RE: Advies_in_kader_van_meldplicht_datalekken_05_06_2019
"
Gezien, dank voor analyse.

Jeannette

Van: art.5.1-2e
Verzonden: donderdag 25 juli 2019 15:08
Aan: art.5.1-2e
CC: Baljeu, J.N.
Onderwerp: Advies_in_kader_van_meldplicht_datalekken_05_06_2019

Dag art.5.1-2e

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

Met vriendelijke groet,

art.5.1-2e

Functionaris voor Gegevensbescherming

M art.5.1-2e

art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

Provincie Zuid-Holland | Zuid-Hollandplein 1

Postbus 90602 | 2509 LP Den Haag

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

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

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


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: 2019-07-11 11:44:22.025000+00:00
"Aan: art.5.1-2e
CC:
Onderwerp: RE: Adviezen datalekken
"
Dag art.5.1-2e

Het lijkt mij wijs om wel naar elkaar te verwijzen en in het kort aan te geven waarom het twee verschillende meldingen zijn. Over een jaar weten we dat anders niet meer.

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: donderdag 11 juli 2019 11:37
Aan: art.5.1-2e
Onderwerp: Adviezen datalekken

Hallo art.5.1-2e

Bijgaand de adviezen voor beide datalek situaties. Graag eerst jouw opmerkingen, daarna stuur ik door naar art.5.1-2e

* 1: http://idms/otcs/llisapi.dll/properties/PZH-2019-700090092
* 2: http://idms/otcs/llisapi.dll/properties/PZH-2019-699927905

Vragen die ik nog heb:

* Moet er in de adviezen naar elkaar verwezen worden
* Moet er een verklaring opgenomen worden waarom we de splitsing hebben aangebracht?

Zoals met art.5.1-2e besproken is dit de administratieve vastlegging van de situatie.

De melding bij de Autoriteit Persoonsgegevens heb ik op 21 juni 2019 melding gedaan.

Groet, art.5.1-2e


provincie
ZUID HOLLAND

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	0618309564
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Eenheid Audit en Advies
Kostenplaatscode	227

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Datalek bij IV-goep
Wat voor soort incident heeft er plaats gevonden?	Anders
Anders? Graag toelichten	Server stond open voor toegang via internet
Wanneer vond de inbreuk plaats? Indien bekend	4 juli 2023 12:00
Wanneer vond de inbreuk plaats? Indien niet bekend	Eind december 2022

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)	Aanwonenden van een provinciale weg
Schatting van het aantal personen betrokken bij het datalek: minimaal	700
Schatting van het aantal personen betrokken bij het datalek: maximaal	700

Van: art.5.1-2e
Verzonden: 2023-10-02 14:16:57+00
Aan: art.5.1-2e art.5.1-2e art.5.1-2e
CC:
Onderwerp: RE: betrouwbaarheid zoekmethodiek
"
Hoi art.5.1-2e

Ik wil daar graag op reageren. Zie onder in rood.

Groet,

art.5.1-2e

Van: art.5.1-2e < art.5.1-2e pzh.nl>
Verzonden: maandag 2 oktober 2023 14:06
Aan: art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl>; art.5.1-2e
< art.5.1-2e pzh.nl>
Onderwerp: RE: betrouwbaarheid zoekmethodiek

Hi art.5.1-2e

Dank voor je reactie.

Wij zijn met de eenheid gestart met handmatig IDMS doorzoeken op “kopie paspoort” en “curriculum vitae” om persoonsgegevens te isoleren. Een paar constateringen:

1. Het is tijdrovend; bij een hoop resultaten kun je het niet uit de documentnaam afleiden

Als je niet uit de documentnaam kunt afleiden dat het om persoonsgegevens gaat, kan een buitenstaander dat in principe ook niet. Isoleren we datgene wat wel herkenbaar is als persoonsgegevens, dan zijn we een heel eind en hebben we voor de 5e een resultaat (geïsoleerde persoonsgegevens). We kunnen daarna aan de slag met het analyseren van de zoekresultaten van het datateam. We bereiken daar voor de 5e niets/weinig concreets mee dat ten gunste komt van de melding bij de AP.

2. Met 2 personen tegelijk aan zelfde zoekterm resulteert in veel dubbelwerk omdat beide collega’s regelmatig dezelfde hits noteren.

Dit had ik om die reden ook afgeraden. Er zijn drie zoektermen (en evt differentiaties daarvan, als dat mag).

3. Bij iedere persoon wijkt de volgorde van zoekresultaten af; je kunt dus niet afspreken ik zoek tot pagina 20 en jij vanaf pagina 20
4. Als je IDMS afsluit en opnieuw start krijg je weer een andere volgorde van hits te zien.
5. Ook geïsoleerde documenten staan in de zoekresultaten

art.5.1-2e had beloofd om je hier tijdens de lunch over de informeren. Jullie rechten mbt privacy zitten hier in de weg. Ik zal de geïsoleerde documenten verplaatsen naar een locatie buiten “Centraal”, dan kom je ze niet tegen.

6. Per persoon en per sessie verschilt het aantal zoekresultaten

Dat komt omdat jullie rechten niet helemaal gelijk zijn. Die van jou, art.5.1-2e en art.5.1-2e zijn gelijk. art.5.1-2e heeft meer rechten.

@art.5.1-2e <mailto :art.5.1-2e pzh.nl> : zie bovenstaand

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto :art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%art.5.1-2e%40pzh.nl%7C5733cdc86e524dd950af08dbc34178ff%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638318458192769333%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=sL%2F%2BbyCVgGvzv5MHmVJNoj7J2PHWpt2E%2FVM%2BCqPSB1E%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art.5.1-2e art.5.1-2e <art.5.1-2e pzh.nl
<mailto:art.5.1-2e pzh.nl> >
Verzonden: maandag 2 oktober 2023 13:37
Aan: art.5.1-2e <art.5.1-2e pzh.nl <mailto :art.5.1-2e pzh.nl> >
Onderwerp: RE: betrouwbaarheid zoekmethodiek

Hi art.5.1-2e

Ja, zeker, de “index” een onderdeel in idms was overvraagd en ontregeld.

Afgelopen weekend is dat als het goed is hersteld. Die index hebben we nodig om de juiste informatie eruit te halen. Daarom zouden daar waar we twijfels hebben opnieuw de zoekopdracht willen doen. Ik zal met art.5.1-2e een lijst voor je maken, waar we twijfel hebben.

Deze termen moeten nog: IBAN- Afschrift- CV

Vrijdag konden we nog rekeningnummer doen, met meer dan 170.000 resultaten. Die resultaten worden morgen ochtend aan het Power BI dashboard toegevoegd.

De vraag is nu wanneer we de volgende opdracht aan idms kunnen starten. (art.5.1-2e is vandaag vrij)

Ik zou graag alles compleet en volledig maken, uit de 1e en 2e zoekopdracht. Deze week en misschien nog volgende week. Voordat we zoekopdracht 3 starten.

Tegelijkertijd kloppen de aantallen uit IDMs op hoofdlijnen vaak wel. Die kan je wel als controle of uitgangspunt nemen voor deze fase. (terug rapporteren aan de A.P.)

Onze opdrachten via computer zijn wel diepgravender en volledi ger, met veel aantallen en details. Waarvan ik merk dat collega’s erdoor overweldigd worden. Het gedoseerd aanpakken zal een uitdaging worden.

Groetjes art.5.1-2e

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Verzonden: maandag 2 oktober 2023 12:47
Aan: art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl
<mailto: art.5.1-2e pzh.nl> >; art.5.1-2e < art.5.1-2e pzh.nl
<mailto: art.5.1-2e pzh.nl> >
CC: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Onderwerp: RE: betrouwbaarheid zoekmethodiek

Is hier nog een verklaring uitgekomen waarom de cv plus naam niet in het powerBI rapport voorkwamen?

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art.5.1-2e %40pzh.nl%7C5733cdc86e524dd950af08dbc34178ff%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638318458192769333%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=sL%2F%2BbyCVgGvzv5MHmVJNoj7J2PHWpt2E%2FVM%2BCqPSB1E%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl <mailto: art.5.1-2e pzh.nl> >
Verzonden: vrijdag 29 september 2023 11:08
Aan: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
CC: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Onderwerp: RE: betrouwbaarheid zoekmethodiek

Hi all

art.5.1-2e gaat even meekijken, heeft als het goed is het id van deze melding bij art.5.1-2e opgevraagd. Zodat we kunnen checken…

Groetjes art.5.1-2e

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Verzonden: vrijdag 29 september 2023 10:07
Aan: art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl <mailto: art.5.1-2e pzh.nl> >; art.5.1-2e < art.5.1-2e pzh.nl <mailto: art.5.1-2e pzh.nl> >
CC: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Onderwerp: betrouwbaarheid zoekmethodiek

Beste art.5.1-2e en art.5.1-2e

Onderstaand een door mij aangetroffen cv. De namen komen voor in de namenlijst…..

https://idms/otcs/llisapi.dll?func=ll&objId=635223922&objAction=Open&nexturl=%2Fotcs%2Fllisapi%2Edll%3Ffunc%3Dll%26objId%3D635221425%26objAction%3Dbrowse%26logStopConditionID%3D29004033_%2D132945365_24_loc

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7 art.5.1-2e %40pzh.nl%7C5733cdc86e524dd950af08dbc34178ff%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638318458192769333%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=sL%2F%2BbyCVgGvzv5MHmVJNoj7J2PHWpt2E%2FVM%2BCqPSB1E%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

"


provincie
Zuid-Holland

Van: art.5.1-2e
Verzonden: 2023-10-02 14:05:54+00:00
Aan: art.5.1-2e art.5.1-2e art.5.1-2e
CC:
Onderwerp: RE: betrouwbaarheid zoekmethodiek
"
Hi art.5.1-2e

Dank voor je reactie.

Wij zijn met de eenheid gestart met handmatig IDMS doorzoeken op “kopie paspoort” en “curriculum vitae” om persoonsgegevens te isoleren. Een paar constateringen:

1. Het is tijdrovend; bij een hoop resultaten kun je het niet uit de documentnaam afleiden
2. Met 2 personen tegelijk aan zelfde zoekterm resulteert in veel dubbelwerk omdat beide collega’s regelmatig dezelfde hits noteren.
3. Bij iedere persoon wijkt de volgorde van zoekresultaten af; je kunt dus niet afspreken ik zoek tot pagina 20 en jij vanaf pagina 20
4. Als je IDMS afsluit en opnieuw start krijg je weer een andere volgorde van hits te zien.
5. Ook geïsoleerde documenten staan in de zoekresultaten
6. Per persoon en per sessie verschilt het aantal zoekresultaten

@art.5.1-2e <mailto : art.5.1-2e pzh.nl> : zie bovenstaand

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7 art.5.1-2e %40pzh.nl
%7C1afbb7ce21bd4398408308dbc33fedb3%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638318451575836172%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=2375FKTm7Lh%2FBFXB%2B61%2FO8aBVGI7iGDOpm05DcriWAA
%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art.5.1-2e art.5.1-2e <art.5.1-2e pzh.nl>
Verzonden: maandag 2 oktober 2023 13:37
Aan: art.5.1-2e <art.5.1-2e pzh.nl>
Onderwerp: RE: betrouwbaarheid zoekmethodiek

Hi art.5.1-2e

Ja, zeker, de “index” een onderdeel in idms was overvraagd en ontregeld. Afgelopen weekend is dat als het goed is hersteld. Die index hebben we nodig om de juiste informatie eruit te halen. Daarom zouden daar waar we twijfels hebben opnieuw de zoekopdracht willen doen. Ik zal met art.5.1-2een lijst voor je maken, waar we twijfel hebben.

Deze termen moeten nog: IBAN- Afschrift- CV

Vrijdag konden we nog rekeningnummer doen, met meer dan 170.000 resultaten. Die resultaten worden morgen ochtend aan het Power BI dashboard toegevoegd.

De vraag is nu wanneer we de volgende opdracht aan idms kunnen starten. (art.5.1-2e is vandaag vrij)

Ik zou graag alles compleet en volledig maken, uit de 1e en 2e zoekopdracht. Deze week en misschien nog volgende week. Voordat we zoekopdracht 3 starten.

Tegelijkertijd kloppen de aantallen uit IDMs op hoofdlijnen vaak wel. Die kan je wel als controle of uitgangspunt nemen voor deze fase. (terug rapporteren aan de A.P.)

Onze opdrachten via computer zijn wel diepgravender en vollediger, met veel aantallen en details. Waarvan ik merk dat collega’s erdoor overweldigd worden. Het gedoseerd aanpakken zal een uitdaging worden.

Groetjes art.5.1-2e

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Verzonden: maandag 2 oktober 2023 12:47
Aan: art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl
<mailto: art.5.1-2e pzh.nl> >; art.5.1-2e < art.5.1-2e pzh.nl
<mailto: art.5.1-2e pzh.nl> >
CC: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Onderwerp: RE: betrouwbaarheid zoekmethodiek

Is hier nog een verklaring uitgekomen waarom de cv plus naam niet in het powerBI rapport voorkwamen?

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%art.5.1-2e%40pzh.nl%7C1afbb7ce21bd4398408308dbc33fedb3%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638318451575836172%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=2375FKTm7Lh%2FBFXB%2B61%2FO8aBVGI7iGDOpm05DcriWAA%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl
<mailto: art.5.1-2e pzh.nl> >
Verzonden: vrijdag 29 september 2023 11:08
Aan: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
CC: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Onderwerp: RE: betrouwbaarheid zoekmethodiek

Hi all

art.5.1-2egaat even meekijken, heeft als het goed is het id van deze melding bij art.5.1-2e opgevraagd. Zodat we kunnen checken…

Groetjes art.5.1-2e

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Verzonden: vrijdag 29 september 2023 10:07
Aan: art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl
<mailto: art.5.1-2e pzh.nl> >; art.5.1-2e < art.5.1-2e pzh.nl
<mailto: art.5.1-2e pzh.nl> >
CC: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Onderwerp: betrouwbaarheid zoekmethodiek

Beste art.5.1-2e en art.5.1-2e

Onderstaand een door mij aangetroffen cv. De namen komen voor in de namenlijst…..

https://idms/otcs/llisapi.dll?func=ll&objId=635223922&objAction=Open&nexturl=%2Fotcs%2Fllisapi%2Edll%3Ffunc%3Dll%26objId%3D635221425%26objAction%3Dbrowse%26logStopConditionID%3D29004033_%2D132945365_24_loc

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art.5.1-2e %40pzh.nl
%7C1afbb7ce21bd4398408308dbc33fedb3%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638318451575836172%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=2375FKTm7Lh%2FBFXB%2B61%2FO8aBVGI7iGDOpm05DcriWAA
%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

"


provincie
Zuid-Holland

art.5.1-2e

Van: art.5.1-2e
Verzonden: ember 2023 08:47
Aan: art.5.1-2e art.5.1-2e
Onderwerp: paciteit idms vraag.

Dank art.5.1-2e

Groeten,
art.5.1-2e

Van: art.5.1-2e art.5.1-2e < art.5.1-2e @pzh. nl>
Verzonden: woensdag 27 september 2023 08:33
Aan: art.5.1-2e < art.5.1-2e @pzh.nl >
Onderwerp: capaciteit idms vraag.

Hi art.5.1-2e

Nog even een korte up dat t.a.v. de capaciteit voor het idms vraagstuk in relatie tot het datascience team of andere teamleden. Op dit moment voorzien wij nog geen problemen.
We hebben geen werk wat nu uitvalt en op een kritisch pad ligt. In overleg is het tot nu toe te regelen.
Mocht dit anders worden, dan kom ik bij je terug.

art.5.1-2e art.5.1-2e

Productowner/data officer voor Team Applicaties, innovatie en datascience

provincie Zuid-Holland

provincie Zuid-Holland

Phone art.5.1-2e
Email: art.5.1-2e @pzh. nl

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

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art.5.1-2e
Verzonden: 2023-10-03 20:25:13+00:00
Aan: art.5.1-2e art.5.1-2e
CC:
Onderwerp: Re: concept advies aan art.5.1-2e omtrent melden aan AP en melden aan betrokkenen
"
Hi art.5.1-2e

Dank je voor het delen. Ik heb een paar (tekstuele) aanvullingen gedaan. Het juridische deel heb ik nu niet diepgaand gelezen.

Groet,

art.5.1-2e

art.5.1-2e | CISO | art.5.1-2e

Van: art.5.1-2e <art.5.1-2e pzh.nl>
Datum: dinsdag, 3 oktober 2023 om 17:57
Aan: art.5.1-2e <art.5.1-2e pzh.nl>, art.5.1-2e <art.5.1-2e pzh.nl>
Onderwerp: concept advies aan art.5.1-2e omtrent melden aan AP en melden aan betrokkenen

Dag art.5.1-2e en art.5.1-2e

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

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

Ik hoop dat jullie nog tijd vinden om ernaar te kijken voordat ik het naar art.5.1-2e stuur. Mijn deadline voor he versturen heb ik op 22.00 uur vanavond gezet….

Met vriendelijke groet,

art.5.1-2e art.5.1-2e

Functionaris voor Gegevensbescherming

Gerechtelijk Deskundige

art.5.1-2e

E art.5.1-2e pzh.nl

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C0 art.5.1-2e art.5.1-2e 40pzh.nl%7Caad599da5cd341941ffe08dbc43e15bd%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638319543537685977%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=Qz2UhMborVqHiqpevm1R9ghZeZGdpwflbOxrI0rG6B4%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Krachtig Zuid-Holland.
"


provincie
Zuid-Holland

Advies aan concerndirecteur omtrent melding datalek aan AP en aan betrokkenen

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

Er zijn meerdere ~~datalekken~~ inbreuken geconstateerd in iDMS. Eén datalek, met drie zoektermen, is aan de Autoriteit Persoonsgegevens (AP) gemeld op 8 september 2023. Daarnaast zijn er tijdens het onderzoek naar het gemelde datalek (7/9) meerdere inbreuken geconstateerd zowel met handmatige acties door de FG en de Eenheid Privacy als bij geautomatiseerde zoekslagen door de functioneel beheerders van iDMS in samenwerking met het BI-team van I&A.
De vraag die voorligt is of deze datalekken separaat gemeld moeten worden aan de AP of dat dit in één 'container'-melding kan worden gevangen, en wanneer betrokkenen moeten worden geïnformeerd.

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

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

Situatiebeschrijving
Op 7 september jl. ontvingen de FG en de eenheid Privacy (EP) van PZH een melding van de CISO dat hij waarschijnlijk ongeoorloofd toegang heeft gehad tot persoonsgegevens in het IDMS. De CISO had

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

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

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

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

middels de zoektermen “curriculum vitae”, “kopie paspoort” en “Bibob” toegang tot documenten waar hij uit hoofde van zijn functie geen toegang toe behoeft.

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

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

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

Definitie datalek:
Artikel 4 AVG: Definities
12) „inbreuk in verband met persoonsgegevens”: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

De hierboven beschreven scenario's zien met name op de ongeoorloofde verstrekking of ongeoorloofde toegang tot (in de oorspronkelijke wettekst unauthorised disclosure of, or access to) persoonsgegevens.

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

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

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

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

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

art.5.1-2e

Van: art.5.1-2e
Verzonden: o
Aan: art.5.1-2e art.5.1-2e
Onderwerp: dv art.5.1-2e rent mel den aan AP en melden aan betrokkenen

Dag art.5.1-2e

Ook dank voor jouw bijdrage. Ik heb het nu diagonaal gelezen en het lijkt erop dat ik ook daarmee wel kan leven, maar ik ga het zo nog eens grondig herlezen.

Ten aanzien van jouw onderstaande vragen.
Of er meer inbreuken bekend waren op 7 september? Ja en nee (fijn hè, antwoorden van juristen). Ja, er is voor de zomer door een andere medewerker al een datalek uit idms gemeld, dat is ook gemeld aan de AP. En mede naar aanleiding daarvan is het BI-team onderzoek gaan doen naar mogelijke inbreuken. Dat onderzoek liep nog op 7 september toen er de bewuste melding van de CISO kwam. Op basis van die melding zijn wij nog verder gaan zoeken én tezelfdertijd kwamen ook de eerste resultaten van het BI-team binnen. In mijn ogen is de beschreven situatie dus zeker niet onjuist,
Ik vermoed naar aanleiding van jouw vragen dat je mijn brief aan de gedeputeerde en aan art.5.1-2e niet kent.

Bij het tweede punt heb je gelijk, dat is nu niet meer relevant en kan nu weggelaten worden. Voor mijzelf wel handig om te onthouden voor de toekomst .

Met vriendelijke groet,

art.5.1-2e art.5.1-2e
Functionaris voor Gegevensbescherming
Gerechtelijk Deskundige

provincie Zuid-Holland

art.5.1-2e
E art.5.1-2e @p zh.nl
www.zuid-holland.nl/contact

Werkdagen: ma, di, wo, do, vr

Krachtig Zuid-Holland.

Van: art.5.1-2e <art.5.1-2e @pzh. nl>
Verzonden: dinsdag 3 oktober 2023 21:54
Aan: art.5.1-2e <art.5.1-2e @pzh.nl >; art.5.1-2e <art.5.1-2e @p zh.nl>
Onderwerp: RE: concept advies aan art.5.1-2e omtrent melden aan AP en melden aan betrokkenen

Dag allebei,

Ik heb naar je stuk gekeken art.5.1-2e Ik heb een alternatieve versie gemaakt van het stuk en nodig je van harte uit dat te lezen. Volgens mij staat hetzelfde er in, staat het alleen duidelijker verwoord en is de volgorde logischer. Ik heb wel twee wezenlijke vragen: als ik jouw tekst lees (en helemaal als mijn tekst met wat verschuivingen zie) lijk ik

duidelijk te lezen dat we op 7 september al wisten van meer inbreuken dan de drie die zijn genoemd in de melding. Waarom zijn er dan toch maar drie gemeld? En waarom deze drie? Of lees ik het niet goed? Als het anders zit, moet dat ook echt anders in de tekst staan, zeker als je denkt dat mijn versie een verbetering is van je werk. Daar staat het glashelder in namelijk: op 7 september kregen we een melding, er is meer onderzoek gedaan en er kwam meer boven en op 8 september hebben we een melding gedaan…

Het tweede betreft je afsluitende tekst uit Europa. Volgens mij is dat niet relevant, als ik het goed lees. Er staat het een en ander over het langer dan 72 uur wachten met een melding maar we hebben gewoon op tijd gemeld. Dit artikel bood je op 8 september de gelegenheid om te wachten met je melding omdat je onderzoek aan het doen was en je tijdens het onderzoek meer vergelijkbare inbreuken tegenkwam. Die mogelijkheid is toen niet gebruikt en voor zover ik het nu kan overzien is hij dus ook niet meer relevant.

Ik ben heel erg benieuwd wat je van mijn alternatieve tekst vindt. Als je er niks mee kan, stuur dan vooral je eigen tekst door. Ik heb mijn tekst niet voor niks gebakken dus die vind ik fijner maar als je dat anders ziet kan ik ook leven met jouw tekst.

Groeten van art.5.1-2e

art.5.1-2e
Manager Expertisecentrum Communicatie

M art.5.1-2e
E art.5.1-2e @ pzh.nl

Werkdagen: maandag, dinsdag, woensdag, donderdag, vrijdag

www.zuid-holland.nl/contact
Krachtig Zuid-Holland.

Van: art.5.1-2e <art.5.1-2e @pzh.nl >
Verzonden: dinsdag 3 oktober 2023 20:25
Aan: art.5.1-2e <art.5.1-2e @pzh.nl>; art.5.1-2e <art.5.1-2e @ pzh.nl>
Onderwerp: Re: concept advies aan art.5.1-2e omtrent melden aan AP en melden aan betrokkenen

Hi art.5.1-2e

Dank je voor het delen. Ik heb een paar (tekstuele) aanvullingen gedaan. Het juridische deel heb ik nu niet diepgaand gelezen.

Groet,
art.5.1-2e

art.5.1-2e | CISO | art.5.1-2e

Van: art.5.1-2e <art.5.1-2e @pzh.nl >
Datum: dinsdag, 3 oktober 2023 om 17:57

Aan: art.5.1-2e <art.5.1-2e@pzh.nl>, art.5.1-2e <art.5.1-2e@pzh.nl>
Onderwerp: concept advies aan art.5.1-2e omtrent melden aan AP en melden aan betrokkenen

Dag art.5.1-2e en art.5.1-2e

Het was een worsteling om er een beetje een verhaal van te maken op zo korte termijn.
Mijn conclusie is in elk geval om wel in één keer te melden aan de AP, maar voorlopig nog niet te melden aan betrokkenen. Daarvoor heb ik een juridische onderbouwing gevonden die wel moet worden afgestemd met en goedgekeurd door de AP.

Ik hoop dat jullie nog tijd vinden om ernaar te kijken voordat ik het naar art.5.1-2e stuur. Mijn deadline voor he versturen heb ik op 22.00 uur vanavond gezet….

Met vriendelijke groet,

art.5.1-2e art.5.1-2e
Functionaris voor Gegevensbescherming
Gerechtelijk Deskundige

provincie Zuid-Holland

M art.5.1-2e
E art.5.1-2e@p zh.nl
www.zuid-holland.nl/contact

Werkdagen: ma, di, wo, do, vr

Krachtig Zuid-Holland.

Van: art.5.1-2e
Verzonden: 2023-03-20 09:44:33+00:00
Aan: art.5.1-2e
CC: art.5.1-2e
Onderwerp: RE: Conceptadvies datalek A 97859
"
Dag art.5.1-2e

Akkoord met dien verstande dat er met de Servicedesk gesproken moet worden over het wissen van devices.

Met vriendelijke groet,

art.5.1-2e art.5.1-2e

Functionaris voor Gegevensbescherming

M art.5.1-2e

E art.5.1-2e pzh.nl

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%art.5.1-2e art.5.1-2e 40pzh.nl%7C6605af9e4a314b0b622008db291f53f1%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638148986740058730%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=HAOHDaX3FU7C3yNHzdCfn1qm5p488Y0D4smKt6KBTC4%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art.5.1-2e < art.5.1-2e pzh.nl>
Verzonden: maandag 20 maart 2023 09:36
Aan: art.5.1-2e < art.5.1-2e pzh.nl>
CC: art.5.1-2e < art.5.1-2e pzh.nl>
Onderwerp: RE: Conceptadvies datalek A 97859

Akkoord?

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art.5.1-2e art.5.1-2e 40pzh.nl
%7C6605af9e4a314b0b622008db291f53f1%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638148986740058730%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C
%7C&sdata=HAOHDaX3FU7C3yNHzdCfn1qm5p488Y0D4smKt6KBTC4%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Verzonden: maandag 20 maart 2023 08:58
Aan: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Onderwerp: Conceptadvies datalek A 97859

Goedemorgen art.5.1-2e

Bijgaand de definitieve versie van de datalek die vrijdag is gemeld. Laat weten
of er nog iets moet worden aangepast!

Met vriendelijke groet,

art.5.1-2e

Junior Privacy Officer

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art.5.1-2e art.5.1-2e 40pzh.nl
%7C6605af9e4a314b0b622008db291f53f1%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638148986740058730%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C
%7C&sdata=HAOHDaX3FU7C3yNHzdCfn1qm5p488Y0D4smKt6KBTC4%3D&reserved=0>

Werkdagen: ma, di, do, vr

Elke dag beter. Zuid-Holland.

"


provincie
Zuid-Holland

Van: art.5.1-2e
Verzonden: 2023-05-02 16:42:17+00:00
Aan: art.5.1-2e art.5.1-2e
CC:
Onderwerp: Re: Conceptadvies FW: Melding mogelijk datalek A 99100
"
Ja, akkoord. Maak gerust ook nog even een opmerking dat ze dit eerder had moeten melden.

<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAAb9ysg&data=05%7C01 art.5.1-2e. art.5.1-2e 40pzh.nl%7Cbc955ce1fa2c42fe28eb08db4b1b6d98%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638186353404445725%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=O8nC17LYPkfyhrodT2k3TW4Rl6QJkz3PXdUMc2emDK8%3D&reserved=0>

Met vriendelijke groet,

art.5.1-2e art.5.1-2e

Functionaris voor Gegevensbescherming

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

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art.5.1-2e. art.5.1-2e 40pzh.nl%7Cbc955ce1fa2c42fe28eb08db4b1b6d98%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638186353404445725%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=DiuB3XJ4nYYUyNGj1xOKZAjV6vjKBmY0i%2FVk7nICUhU%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Outlook voor Android <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Faka.ms%2FAAb9ysg&data=05%7C01 art.5.1-2e art.5.1-2e 40pzh.nl%7Cbc955ce1fa2c42fe28eb08db4b1b6d98%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638186353404445725%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=O8nC17LYPkfyhrodT2k3TW4Rl6QJkz3PXdUMc2emDK8%3D&reserved=0> downloaden

---

From: art.5.1-2e < art.5.1-2e pzh.nl>
Sent: Tuesday, May 2, 2023 4:34:20 PM

To: art.5.1-2e < art.5.1-2e pzh.nl>
Cc: art.5.1-2e < art.5.1-2e pzh.nl>
Subject: RE: Conceptadvies FW: Melding mogelijk datalek A 99100

Paar hele kleine aanpassingen. Monitor je dat de wipe van de telefoon snel plaatsvindt?

art.5.1-2eakkoord?

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01 art.5.1-2e art.5.1-2e 40pzh.nl%7Cbc955ce1fa2c42fe28eb08db4b1b6d98%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638186353404445725%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=DiuB3XJ4nYYUyNGj1xOKZAjV6vjKBmY0i%2FVk7nICUhU%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art.5.1-2e < art.5.1-2e pzh.nl>
Verzonden: dinsdag 2 mei 2023 13:11
Aan: art.5.1-2e < art.5.1-2e pzh.nl>
Onderwerp: Conceptadvies FW: Melding mogelijk datalek A 99100

Hi art.5.1-2e

Bijgaand het conceptadvies m.b.t. A99100. Graag je feedback!

Met vriendelijke groet,

art.5.1-2e

Privacy Officer

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art.5.1-2e art.5.1-2e 40pzh.nl
%7Cbc955ce1fa2c42fe28eb08db4b1b6d98%7C6d99bc288f284a73a50163 b3040%7C0%7C0%7
C638186353404445725%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=DiuB3XJ4nYYUyNGj1xOKZAjV6vjKBmY0i%2FVk7nICUhU
%3D&reserved=0>

Werkdagen: ma, di, do, vr

Elke dag beter. Zuid-Holland.

Van: loket@pzh.nl <mailto:loket@pzh.nl> <loket@pzh.nl <mailto:loket@pzh.nl> >
Verzonden: maandag 1 mei 2023 15:07
Aan: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e
< art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e
< art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e
< art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e
< art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e
< art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; privacy <privacy@pzh.nl
<mailto:privacy@pzh.nl> >
Onderwerp: Melding mogelijk datalek A 99100

Beste collega,

Er is een melding gedaan van een mogelijk datalek:

Zie voor meer informatie:
Activiteitnummer: A 99100
Wijzigingsnummer: W23 05 00017

Hier kan je de activiteit <https://eur03.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fpvzh.topdesk.net%2Ftas%2Fsecure%2Fcontained%2Fchangeactivity

%3Funid%3D367e7d1504994ac6a8c9855606d17930&data=05%7C01% art.5.1-2e art.5.1-2e 40pzh.nl
%7Cbc955ce1fa2c42fe28eb08db4b1b6d98%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638186353404445725%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=TP0YRxrWtB4Dx32IGH3sl69cqSykUc%2FEjcolAq4YZ8M
%3D&reserved=0> bekijken.

Met vriendelijke groet,

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

Het Loket telefoon 070 4417777 pvzh.topdesk.net
<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F
%2Fpvzh.topdesk.net%2F&data=05%7C01% art.5.1-2e art.5.1-2e 40pzh.nl
%7Cbc955ce1fa2c42fe28eb08db4b1b6d98% 9bc288f284a73a50163a8e1eb3040%7C0%7C0%7
C638186353404445725%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C%7C&sdata=3mNKlP4a3O7wRWHj1AezTECTNM4OPZxI1zXXFBFWhSM
%3D&reserved=0>

"


provincie
Zuid-Holland

Melden datalek

Aanmelder

Naam	art.5.1-2e
Telefoonnummer	0650025057
E-mail	art.5.1-2e @pzh.nl
Organisatie-eenheid	Eenheid Audit en Advies
Kostenplaatscode	227

Benodigde gegevens

Geef een korte samenvatting van het incident/datalek, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan	Mail ontvangen die niet voor mij bestemd was (melding heeft al mondeling plaatsgevonden en handelingen zijn al in gang gezet)
Wat voor soort incident heeft er plaats gevonden?	Mail naar een verkeerde ontvanger
Wanneer vond de inbreuk plaats? Indien bekend	6 juli 2023 13:18
Wanneer vond de inbreuk plaats? Indien niet bekend	

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

Lezen (vertrouwelijkheid)	☑
Kopiëren	☐
Veranderen (integriteit)	☐
Verwijderen of vernietigen (beschikbaarheid)	☐
Diefstal	☐
(Nog) niet bekend	☐

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

Naam-, adres- en woonplaatsgegevens	☐
Telefoonnummers	☐

E-mailadressen of andere adressen voor digitale communicatie	☑
Toegangs- of identificatiegegevens	☐
Financiële gegevens	☐
Burgerservicenummer (BSN) of andere persoonsidentificatienummers	☐
Kopieën van identificatie- en legitimatiebewijzen	☐
Geslacht, geboortedatum en/of leeftijd	☐
Bijzondere persoonsgegevens	☐
Andere gevoelige persoonsgegevens	☐
Anders, namelijk	☐
Wiens persoonsgegevens betreft het (bijvoorbeeld, werknemers, burgers, kinderen)	PS leden, fractieleden D66
Schatting van het aantal personen betrokken bij het datalek: minimaal	19
Schatting van het aantal personen betrokken bij het datalek: maximaal	19

Van: art.5.1-2e
Verzonden: 2023-10-02 19:57:21+00:00
Aan: art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e
CC:
Onderwerp: RE: Data IDMS
"
Beste art.5.1-2e

We hebben geprobeerd om jouw verzoeken zo goed mogelijk te verwerken. Bijgaand tref je de documenten aan. Mocht je toch nog iets missen, laat het me dan weten dan probeer ik er voor te zorgen dat dit morgenochtend zo vroeg mogelijk wordt opgelost.

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01%7 art.5.1-2e %40pzh.nl
%7Ca71b43acf5e04836fefe08dbc3710685%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638318663921425494%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=mwF1f%2FeT2g0RumhoFp6n%2F6bc%2BBlrdOzjf%2FftxbctcMg%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

Van: art.5.1-2e < art.5.1-2e pzh.nl>
Verzonden: zaterdag 30 september 2023 17:25
Aan: art.5.1-2e < art.5.1-2e pzh.nl>; art.5.1-2e < art.5.1-2e pzh.nl>; art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl>; art.5.1-2e < art.5.1-2e pzh.nl>; art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl>; art.5.1-2e < art.5.1-2e pzh.nl>; art.5.1-2e < art.5.1-2e pzh.nl>; art.5.1-2e

art.5.1-2e < art.5.1-2e pzh.nl>
Onderwerp: FW: Data IDMS
Gevoeligheid: Vertrouwelijk

Beste art.5.1-2e en alle anderen,

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

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

Dan de uitwerking van bovenstaande punt 2:

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

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

Hartelijke groet, art.5.1-2e

Van: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Verzonden: vrijdag 29 september 2023 16:39
Aan: art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >; art.5.1-2e < art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl> >
Onderwerp: Data IDMS
Gevoeligheid: Vertrouwelijk

Beste art.5.1-2e

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

Met vriendelijke groet

art.5.1-2e

Privacy jurist

Eenheid Privacy

M art.5.1-2e

E art.5.1-2e pzh.nl <mailto : art.5.1-2e pzh.nl>

www.zuid-holland.nl/contact <https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.zuid-holland.nl%2Fcontact&data=05%7C01% art.5.1-2e %40pzh.nl
%7Ca71b43acf5e04836fefe08dbc3710685%7C6d99bc288f284a73a50163a8e1eb3040%7C0%7C0%7C638318663921425494%7CUnknown
%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=mwF1f%2FeT2g0RumhoFp6n%2F6bc%2BBlrdOzjf%2FftxbctcMg%3D&reserved=0>

Werkdagen: ma, di, wo, do, vr

Elke dag beter. Zuid-Holland.

"

provincie
Zuid-Holland

Memo

Contact

art.5.1-2e

art.5.1-2e @pzh.nl

Datum

29 september 2023

Aan

art.5.1-2e

Kopie aan

art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e, art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e

Onderwerp

Beschrijving iDMS

Het huidige informatiebeheersysteem van de PZH is opgebouwd rondom iDMS: het integraal document managementsysteem. De hiermee verbonden techniek was in 2007, toen het werd aangeschaft, de logische keuze in een periode waarin de transformatie van een papieren naar een digitale werkwijze plaatsvond. Toentertijd was er binnen de provincie een sterke focus op control van de stukkenstromen. De inrichtingskeuzes van iDMS zijn gemaakt op basis van de toen door de organisatie gestelde randvoorwaarden, de aanwezige kennis en de beschikbare technieken. Momenteel bevat iDMS zo'n 50 miljoen documenten verdeeld over primaire-, ondersteunende processen, organisatieomgeving en digitale archiefomgeving. Daarnaast heeft elke gebruiker een persoonlijke werkomgeving. De medewerker is vanaf dit moment zelf verantwoordelijk voor de compleetheid van zijn of haar informatie.

Ondanks verschillende acties en voorlichtingscampagnes de afgelopen jaren, is IDMS feitelijk nooit helemaal gevuld zoals bedoeld. Er zijn de afgelopen jaren vele voorlichtingscampagnes en acties geweest om betere dossiervorming te stimuleren, van De Week van het E-dossier alweer heel wat jaren terug, programma Archief op Koers, tot Up-to-Data van recente datum. Het vestigt even de aandacht op het onderwerp, daarna verslapt deze weer.

Kaders en ontwikkeling

De inrichting en het gebruik van iDMS zijn onderhevig aan verschillende wettelijke kaders , beleid en andere regelingen. Bij de ingebruikname van iDMS in 2007 waren andere kaders van toepassing. Destijds is gekozen voor het principe “Openbaar, tenzij” wat nog steeds gehanteerd wordt, de AVG was nog niet van kracht.

Vanuit wetgeving worden steeds meer eisen gesteld die van toepassing zijn op informatiebeheer. iDMS is niet in alle gevallen voldoende aangepast op deze veranderingen. Denk bijvoorbeeld aan de AVG die in 2018 in werking is getreden. Het beleid dat thans wordt gebruikt voor het opslaan van vertrouwelijke informatie stamt uit 2009. Vanuit Team Informatieveiligheid heeft in het kader van de ISO 27001 implementatie hier onlangs een

actualisatie voor plaatsgevonden. Het AOG I&A heeft met dit voorstel ingestemd en het wordt binnenkort aan het DT voorgelegd. In dat voorstel wordt ook het 'open tenzij'-beleid aangepast.

Voor zover er gegevens aangetroffen worden die niet voldoende zijn afgeschermd, wordt indien nodig hiervan melding gemaakt bij de Autoriteit Persoonsgegevens. De structurele verbetering voor AVG-conform informatiebeheer wordt de komende jaren opgepakt vanuit het programma Informatietransitie door onder andere het opschonen van de huidige informatie, het stevig sturen op informatiebeheer, kennisvergroting en gedragsverandering bij alle medewerkers en het moderniseren en saneren van onze middelen.

Beheer en onderhoud
Voor de continuïteit en veiligheid in Zuid-Holland zijn we mede afhankelijk van iDMS. De beschikbaarheid van iDMS is essentieel; hier is het beheer ook op ingericht.

Het dagelijks beheer iDMS wordt procesmatig uitgevoerd door interne functioneel- en technisch beheerders en staan direct in contact met de organisatie. Wijzigingen met functionele impact worden samen met de gebruiker afgestemd en getest.

IDMS krijgt met regelmaat een software update. Deze is in beginsel technisch van aard en zorgt in zeer beperkte mate voor impact op de gebruikers. Bijna maandelijks worden kleine wijzigingen uitgevoerd ten behoeve van continuïteit en betrouwbaarheid. Technisch is iDMS in alle jaren goed onderhouden, de inrichting is grotendeels zoals die in 2007 is opgebouwd.

Autorisatie en rechten
Een PZH medewerker, met toegang tot ICT, krijgt automatisch toegang tot iDMS. Statenleden en fractiemedewerkers hebben geen toegang. Bij uitdiensttreding vervalt de toegang ook weer automatisch. Zoals eerder genoemd geldt in iDMS het principe “Openbaar, tenzij” waarmee het grootste deel van de documenten voor alle accounts in te zien is; ofwel alles wat niet beperkt toegankelijk is gemaakt.

Op basis van ‘beleid vertrouwelijke informatie’ uit 2009 is informatie beperkt toegankelijk gemaakt, dit zijn onder andere alle concurrentiegevoelige stukken m.b.t. verwerven en aannemen, bestuurs- en kabinetszaken, managementzaken, vergunningverlening, toezicht en handhaving, financiële zaken, Bibob en ICT beheer. Daarnaast zijn dossiers met een vertrouwelijk karakter beperkt toegankelijk gemaakt, zoals stikstof en warmte. Medewerkers die gezien hun rol met deze vertrouwelijke informatie moeten werken krijgen, op basis van hun rol of op verzoek van hun leidinggevende, toegang.

Stappen gezet afgelopen jaren sinds ongeveer 2013

Dit overzicht pretendeert zeker niet volledig te zijn, het geeft 'slechts' een impressie weer van een aantal onderzoeken, initiatieven en uitgevoerde activiteiten in de afgelopen jaren.

Audit - Eenheid Audit & Advies (EAA), 2013

De afdeling I&A heeft in 2013 het bureau Eenheid Audit en Advies (EAA) een onderzoek naar het informatiebeheer laten uitvoeren. Op grond van de uitkomsten en gedane aanbevelingen is veel energie gestoken in het opschonen van de dossiers en het overbrengen van kennis op ambtenaren in de zogenaamde 'week van het e-dossier'.

Enterprise Content Management (ECM) visie door Cap Gemini, 2015

ECM is er primair op gericht om de levenscyclus van ongestructureerde informatie (van initiële creatie via bijvoorbeeld publicatie tot aan archivering en vernietiging) te ondersteunen. Belangrijke aspecten hierbij zijn het terugvinden van de betreffende content, en het bewaken van de integriteit ervan. Het resultaat hiervan is efficiëntie en transparantie voor de medewerker en de organisatie.

Governance en Compliancy

Compleet inzicht in de aanwezige content, volgend ook vanuit het eerder genoemde volledig in control zijn, gaat verder dan alleen records management. *De informatie lifecycle management en compliancy moet gelden voor alle content.*

Beleid en organisatie (information governance)

Capgemini raadt aan het project om te komen tot een goede inbedding van Information Governance voor content, en bij voorkeur ook voor data, zo spoedig mogelijk op te zetten ten einde tijdig randvoorwaarde stellend voor andere programma's te kunnen zijn.

Beveiliging en autorisatie

Het algemeen geldend principe van "alle content is voor iedereen beschikbaar, tenzij… " wordt voor de toekomstige ECM ontwikkelingen op het gebied van kennisdelen, content analyse, openheid en samenwerking als meest van toepassing zijnde gezien. Aansluiting bij, opname door of opvolging vanuit het project Informatie Veiligheid dat momenteel loopt wordt geadviseerd.

nav Coalitieakkoord – toezegging coalitie van 5 miljoen voor vernieuwing IDMS is besteed aan TOP (nu DZH), 2015

Vooraf aangeleverd aan coalitietafel: 7 mln gevraagd waarvan 6 mln voor vervanging iDMS en 1 mln voor transparantie.

In het Hoofdlijnenakkoord is opgenomen dat Zuid-Holland voorop wil lopen in het transparant maken van de provincie en daarvoor incidenteel € 5 miljoen investeert in ICT-infrastructuur en werkprocessen die een grotere transparantie mogelijk maken. In een brief van gedeputeerde is later toegelicht aan PS dat deze investering nadrukkelijk is bedoeld als impuls voor het transparant maken van de provincie. Er wordt dus geen regulier werk mee bekostigd. Voor dit bedrag is daardoor dan ook geen vervanging iDMS gerealiseerd, maar het vernieuwdDataWarehouse waarbij de governance nog niet geregeld is.

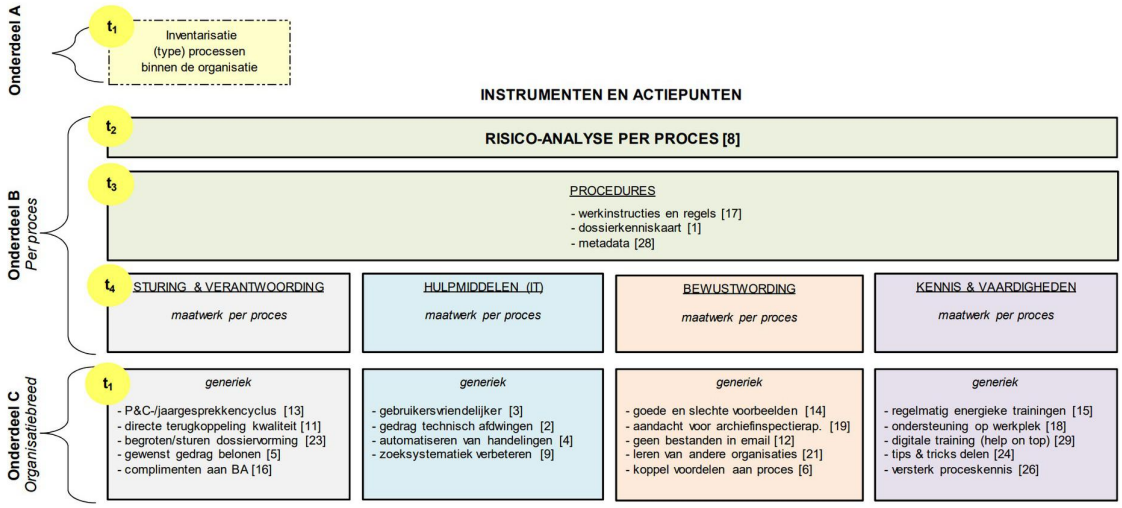
Archiefinspectie, 2016

Een van de belangrijkste conclusies uit de inspectie is dat de digitale archivering in het daartoe ingerichte documentmanagementsysteem (iDMS) in vergelijking met vier jaar geleden nog steeds niet

op orde is. De behandelend ambtenaren zijn op grond van provinciale regelgeving verplicht zelf hun dossiers te vormen en te beheren.

EAA: Meervoudige kennis onderzoek, 2016

Naar aanleiding van het inspectierapport van de provinciearchivaris 2015 is aan Provinciale Staten toegezegd om de conclusies en aanbevelingen hieruit met alle directeuren te bespreken en op basis hiervan vóór het zomerreces van 2016 te komen met een concreet plan van aanpak (‘archief op koers’) met maatregelen en acties ter verbetering van de situatie van het archief- en informatiebeheer. EAA bevelen aan om het advies, zoals weergegeven in de onderstaande roadmap, te integreren in een plan van aanpak. Op deze manier wordt voortgebouwd op de inspanningen en resultaten die in de afgelopen periode zijn geleverd met een grote groep betrokken medewerkers.



Figuur 1: Roadmap actiepunten t.b.v. dossiervorming en archivering

NB.: De instrumenten zijn onderstreept. De actiepunten zijn voorzien van een nummer [X]. Op basis hiervan kan de uitwerking van het actiepunt worden gevonden in bijlage 3.

Uitkomst: mensen zien dat hun gedrag bepalend is, echter bij oplossingsmogelijkheden wordt vooral naar een systeem/IT verwezen.

Besluit directeur concernzaken, 2016

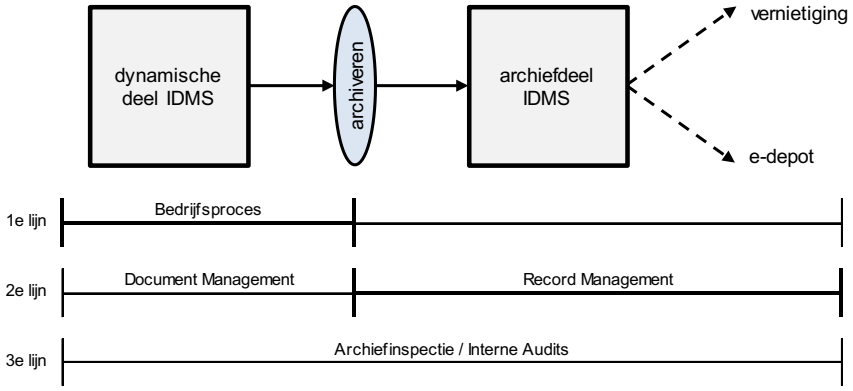
ECM-visie gaat geen vervolg krijgen, alleen de urgente zaken uit de archiefinspectie worden opgepakt uit middelen van I&A. Daaruit is het programma Archief op Koers ontstaan.

Archief op Koers, 2016-2018

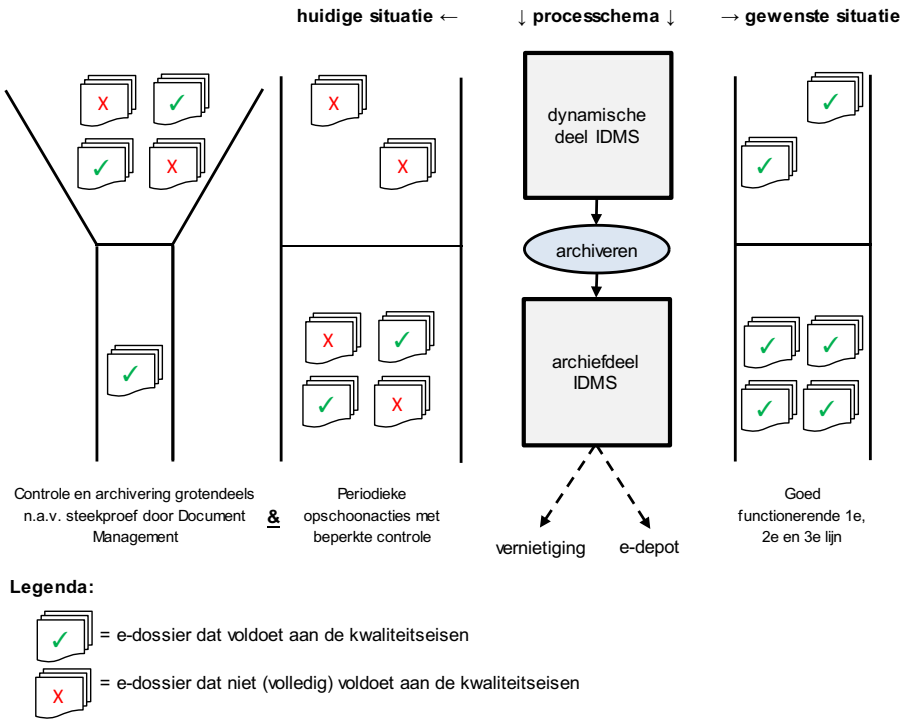
Met de oplevering van Archief op Koers zijn de aanbevelingen en verbeterpunten van de provinciearchivaris en van EAA uitgevoerd. Al eerder namelijk in 2012/2013 is een programma uitgevoerd om de kwaliteit van dossiervorming te verbeteren.
Om te voorkomen dat om de paar jaar programma’s uitgevoerd moeten worden om achterstanden in te halen en dossiervorming weer op niveau te brengen heeft de programmanager AoK de eenheid Audit en Advies gevraagd, het programma tegen het licht te houden en aanbevelingen te doen voor de structurele inbedding van de resultaten in de organisatie.

EAA, Management Letter onderzoek naar inbedding informatiebeheer, 2017

- Diverse afdelingshoofden hebben geen duidelijk beeld bij informatiebeheer en/of hun verantwoordelijkheid daarvoor.
- Afdelingshoofden vinden over het algemeen dat ze onvoldoende zijn toegerust om hun verantwoordelijkheid voor informatiebeheer te nemen. Het schort volgens hen met name aan managementinformatie en duidelijke kaders, maar ook over de andere stellingen oordelen ze weinig positief.
- Bij de meeste, maar niet alle, afdelingen zijn bureauhoofden ook verantwoordelijkheid voor informatiebeheer. Slechts een deel van de afdelingshoofden geeft antwoord op de vraag welke taken bureauhoofden in dat kader hebben. Sommigen geven expliciet aan dat hierover geen scherpe afspraken zijn gemaakt.



Figuur 1: verdeling verantwoordelijkheden tussen 1e, 2e en 3e lijn



Figuur 2: huidige en gewenste situatie

Startbrief 2018- Overzicht integrale bedrijfsvoeringonderwerpen, 2017

Een I-strategie ontwikkelen met betrokkenheid van collega's uit de hele organisatie.

Versterken van centrale agendering en coördinatie (CIO-functie) om een goede verbinding te leggen met ontwikkelingen op het gebied van Public Intelligence en TOP.

Versterken van de afdeling I&A waar het gaat om actief en alert ontwikkelen en faciliteren van de I-kant richting beleid en uitvoering, om zo bij te dragen aan een moderne en responsieve provincie.

Elke afdeling heeft dit jaar het onderdeel informatie op moeten nemen in zijn jaarplan, dit is enkel dit jaar zo uitgevraagd.

Beoogd resultaat: Een PZH die voldoende toegerust is voor de toekomst als het gaat om de wijze waarop wij omgaan met informatie in samenhang met de opgaven waar we voor staan.

Evaluatie proces bestemmingsplan Zwethof, 2018

Eindconclusie

Niet tijdig onderkennen gevoeligheid locatie Zwethof heeft belangrijke invloed op verloop proces en besluitvorming. Zorg voor een betere informatievoorziening naar Provinciale Staten, bijvoorbeeld door het beschikbaar stellen van informatie over de voorgeschiedenis bij stukken en het expliciet maken van deze locaties in het Programma ruimte en attendeer Provinciale Staten hierop.

Rapportage Archiefinspectie, 2018

Archief op Koers heeft grote verbeteringen in de digitale dossiervorming weten te realiseren.

Aanbevelingen

Digitaal archief- en informatiebeheer

De digitale archivering in iDMS is verbeterd, evenals de ondersteuning van de behandelend ambtenaren. Een nieuwe manier van dossiervorming is geïntroduceerd, die het werken met iDMS heeft vereenvoudigd en de archivering in applicaties buiten het iDMS is onderzocht en beheermaatregelen worden per applicatie geregeld.

ICT-beheer en informatiebeveiliging

Het ICT-beheer en de informatiebeveiliging zijn waar het de archief wettelijke aspecten aangaat op orde. De aanbevelingen die de Eenheid Audit en Advies doet voor het informatiebeheer in relatie tot de invoering van de Algemene Verordening Gegevensbescherming worden onderschreven.

Digitale archivering buiten IDMS

Buiten het iDMS zijn er meerdere systemen waarin digitale informatie in de vorm van documenten of data wordt opgeslagen en gedeeld, waarbij dit soms in interne applicaties geschied, maar ook in de Cloud of bij derden. Sinds 2016 zijn over de opslag van informatie goede afspraken gemaakt en maatregelen genomen om de archiefwaardige bescheiden in de intern in gebruik zijnde applicaties goed te (laten) beheren, te archiveren en duurzaam op te slaan.

Jaarverslag FG, 2019

De volgende belangrijkste adviezen zijn door de FG benoemd die betrekking hebben op de risico's bij de verwerking van persoonsgegevens.

- Zorg op korte termijn dat de rollen en rechten op orde zijn in iDMS. Vervang iDMS en stel daarbij deadlines voor de keuze van een nieuw programma en de implementatie. Reactie: Dit is deels overgenomen. iDMS wordt geupdate, vernieuwd en er zullen diverse verbeteringen doorgevoerd worden.

- PZH beschikt niet over een beleid ten aanzien van het omgaan met persoonsgegevens, niet op afdelingsniveau en niet als concern. Er is soms wel wat beleid op deelaspecten. Daarnaast beschikt PZH wel over een privacyverklaring, welke is gepubliceerd op haar website. De AVG vereist echter een beleid op het gebied van privacy waarin ook is vastgelegd op welke wijze de kwaliteit van het omgaan met persoonsgegevens is geborgd.
- Zet ook in 2020 vol in op bewustwording binnen de organisatie door middel van campagnes waarbij het thema datalek centraal staat.

EAA-onderzoek (0-meting) bewuste omgang met informatie, 2019

Conclusies:

- Bewustzijn is aanwezig: men weet dat we wat te beschermen hebben. Dilemma hierbij is de transparantie
- Men heeft behoefte aan meer informatie over veilig werken: omgang met wachtwoorden, gebruik wifi, verlies tablet/telefoon, bij wie melden, opslaan van info, delen van info met derden, omgaan met updates e.d.
- FG en informatiebeveiligingsspecialist zijn onbekend
- Er zijn verschillende opvattingen over (de noodzaak van) het vergrendelen. Er is niet veel verschil tussen de antwoorden van managers en die van overige medewerkers. Met betrekking tot het vergrendelen van de computer moet bepaald worden wat vanuit beveiliging wenselijk is
- Delen van gebruikersnamen en wachtwoorden is een belangrijk aandachtspunt. Dit heeft soms een technische oorzaak, maar ook gemak. De privacy als bv secretaresses inloggen als leidinggevende, wordt hierbij genoemd als zorgpunt
- Als oorzaak dat dossiers niet op orde zijn wordt de gebruikersonvriendelijkheid van IDMS vaak genoemd
- Men maakt zich zorgen over het gebruik van SAAS-oplossingen (Amerikaanse bedrijven), whats app, beheer van informatie

Bewustwordingscampagne Up to data opgestart, 2019

In 2019 is na een 0-meting een eerste campagne, “Up to data”, geïnitieerd door I&A in samenwerking met bestuur (AVG, Woo en provinciaal archivaris) en P&O (integriteit). De onderwerpen van deze campagne zijn: Data- en informatiekwaliteit, Informatie veiligheid, Privacy, Informatiebeheer en Integriteit. Diverse succesvolle acties zijn opgezet en in de organisatie gedeeld.

Vernieuwing IDMS, 2019

Projectleider is gestart met ID (Initiatie Document) voor een traject dat na afronding van de onderhanden iDMS upgrade moet leiden tot een verbeterde/gewijzigde inzet van het iDMS in de ondersteuning van de organisatie. Is gebaseerd op functionaliteit die straks met de nieuwe versie beschikbaar komt, en de ‘noodzaak’ beter in te spelen op wensen t.a.v. betere samenwerking, inzet van nieuwe tooling als Teams (office365 traject), data gedreven werken. De analyse voor dit vernieuwingstraject willen we al parallel aan de upgrade opstarten. Dit traject is uiteindelijk niet doorgezet ivm ontbreken financiële middelen.

Warmtedossier, 2019

Vertrouwelijke stukken gekopieerd naar openbaar deel van iDMS. Dit is vertrouwelijk opgeruimd en dichtgezet.

Wob verzoek Shell, 2019

Een omvangrijk Wob-verzoek van een juridisch adviseur over Shell (zgn. Shellpapers). Het verzoek is in november 2019 nader ingeperkt/gepreciseerd, wat niet heeft geresulteerd in een Wob-verzoek die

in behandeling genomen kon worden, het Wob-verzoek is daarom door PZH buiten behandeling gesteld (afgewezen). Inmiddels (2023) is dit verzoek weer relevant en krijgt deze mogelijk een vervolg.

Archiefinspectie, 2020

Aanbevelingen

Het beheer van digitale documenten en data is onvoldoende. Ontvangen of verzonden informatie is slecht of niet terug te vinden en dat vereist niet alleen beter beheer van documenten en data door betrokken medewerkers, maar ook daartoe ingerichte en veilige informatiesystemen. Aanbevelingen van de provinciearchivaris zijn om meer voorlichting en scholing over archivering, informatiebeheer, privacybescherming en informatieveiligheid te geven en archieven en databestanden daadwerkelijk te schonen en te inventariseren. Dit vraagt onder meer om een structurele vernieuwing van het archiefsysteem iDMS en de aanpassing van andere applicaties om de duurzame vastlegging van data mogelijk te maken.

De duurzame bewaring en beveiliging van de fysieke en digitale informatie is grotendeels op orde. De risico's op datalekken in de provinciale informatiesystemen, waaronder in het archiveringssysteem iDMS, zijn wel zorgelijk. De aanbevelingen die de Functionaris Gegevensbescherming in zijn Jaarverslag Privacy over 2019 doet over informatiebeheer en informatieveiligheid onderschrijft hij.

Hefbrug Boskoop, 2020

Dossier is niet volledig en versnippert over verschillende digitale mappen en bronnen.

Aanbeveling EAA

De onderzoekers hebben veel tijd moeten investeren in het achterhalen van de juiste stukken. Er zijn veel digitale mappen over de hefbrug Boskoop (in IDMS en op de Q-schijf van DBI). De samenhang tussen deze mappen is gebrekkig en de erin opgenomen informatie niet altijd volledig. Goede dossiervorming en het eigenaarschap hiervoor zijn voorwaarden voor kennisborging en om het leerproces van de organisatie verbeteren.

Wij bevelen DBI aan om zorg te dragen voor verbetering van de kwaliteit en volledigheid van dossiers en het eigenaarschap hiervoor te organiseren.

Professionaliteit

Informatiebeheer vraagt blijvend inzet van alle ambtenaren. Dit is niet altijd leuk, maar is een onderdeel van de professionaliteit/verantwoordelijkheid van elke medewerker. Positief gevolg van goed informatiebeheer door iedereen is de terugvindbaarheid van onze bescheiden.

Blijvend aandacht

Het onderwerp informatiebeheer heeft blijvend aandacht nodig, we zijn nooit klaar. Elke dag wordt er nieuwe informatie/data toegevoegd aan onze systemen, daar zal altijd over nagedacht moeten worden: hoe slaan we dit op? waarom slaan we dit op? voor wie moet het beschikbaar/vindbaar zijn? etc.

Gedrag

Het gedrag van mensen blijft de grootste uitdaging, een systeem staat of valt met hoe goed dit gebruikt en nageleefd wordt. Er kan en wordt veel ondersteund, echter niet alles is af te vangen.

Jaarverslag Functionaris voor Gegevensbescherming, 2021

De provincie voldoet niet altijd aan gegevensminimalisatie, vooral niet bij haar document management systeem (iDMS). De FG wees hier al op in het jaarverslag over 2019. Ondanks dat de organisatie het systeem verbeterde, blijft duidelijk dat het systeem niet is ingericht op een adequate

naleving van de AVG. Daarnaast weten medewerkers vaak niet goed hoe ze persoonsgegevens in het iDMS moeten verwerken, waardoor gevoelige en soms ook bijzondere persoonsgegevens in strijd met de AVG worden verwerkt. In 2021 kwam de afdeling I&A met een nieuwe visie op het informatiebeheer binnen de provincie, waarin ook het document management systeem een plaats heeft. De provincie blijft de AVG schenden totdat er een nieuw en/of sterk verbeterd DMS is, met alle risico's op sancties door de Autoriteit Persoonsgegevens

EAA onderzoek (1-meting), 2021

Conclusies

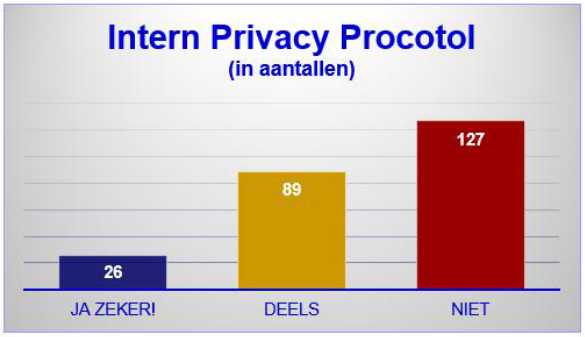
1. De bekendheid met de Campagne Up-to-Data is wisselend: sommige activiteiten uit de campagne zijn redelijk goed bekend bij de respondenten en anderen zijn minder opgevallen. Recente initiatieven zijn het meest bekend.
2. Uit ons onderzoek blijkt dat respondenten bewust zijn van de waarde van informatie.
3. Bewustzijn van provinciale medewerkers met betrekking tot privacy, informatiekwaliteit/-integriteit, informatieveiligheid, informatiebeheer en archivering is aanwezig, maar moet wel verbeterd worden.
4. Er volgen hierna aandachtspunten die de waarde van informatie en de bewustzijn bij de omgang met informatie kunnen vergroten.
5. Kracht van herhaling: bewustzijn is een "on going" proces.

Aanbevelingen om bewustzijn te vergroten

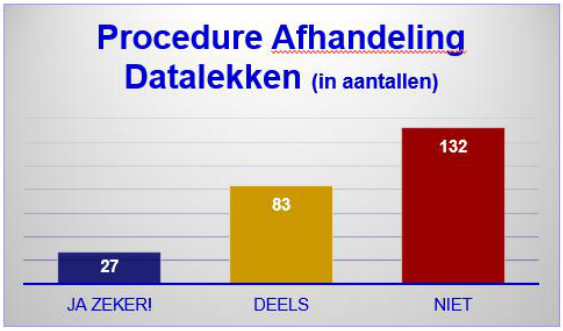
1. Bewustzijn bij de omgang met informatie is een continu proces. Gebruik de kracht van herhaling en sluit de campagne aan op de behoefte aan informatie van de respondenten.
2. Er is behoefte aan training, webinars, opleiding op specifieke gebieden (cybersecurity, veilig thuiswerken, iDMS, enz.). Deze zijn belangrijk voor nieuwe medewerkers, maar opfriscursussen kunnen helpen om bewustzijn op peil te houden.
3. Geef aandacht aan de richtlijnen voor archiveren (iDMS, Teams, OneDrive, Whatsapp enz.). De bekendheid met de richtlijnen is verschillend bij de respondenten.
4. Geef aandacht aan de vindbaarheid en gebruikersvriendelijkheid van documenten met relevante procedures, beleid en richtlijnen. Hierbij gaat het ook om op het werkproces en de opgaven gerichte informatie.

Kennis van interne procedures en richtlijnen over AVG kan worden verbeterd

Intern Privacy Protocol is bij 52% van de respondenten niet bekend



Procedure Afhandeling Datalekken is niet bekend bij 55% van de respondenten



Visie op toekomstbestendig informatiebeheer- met Gartner, 2021

Fundament van het informatiebeheer is niet op orde en vereist dringend actie

Er is een veelheid aan technologieën, platforms en een wildgroei aan informatie. Er dreigt op dit punt een onbeheersbare situatie te ontstaan

Er is in het I-domein geen werkende en gesloten I-besturingscyclus

Door een gebrek aan sturing is er te weinig focus en onvoldoende richting. Veel initiatieven bestaan 'los' van elkaar en eindigen door een gebrek aan regie in het 'niets'

Het verder ontwikkelen van het data/informatie-gedreven werken is essentieel

In het werkveld van het data/informatie-gedreven werken worden de komende jaren 'de kaarten opnieuw geschud'. Als PZH zich niet nadrukkelijk op dit vlak ontwikkelt, wordt het lastiger haar rol te behouden

Het betreft een omvangrijke PZH-brede veranderopgave met een aanzienlijke ICT-component

De verandering zal alle medewerkers beïnvloeden. Veel aandacht voor verandermanagement en communicatie is cruciaal. Voorbeeldgedrag van directeuren, regisseurs en leiders is essentieel

De organisatie is nooit 'klaar'

Informatiebeheer en data/informatie-gedreven werken blijven in ontwikkeling en vergen voortdurende verandering en investeringen. Het is 'nooit af'.

Memo aan MT I&A Persoonsgegevens, 2022

In 2022 is er door twee adviseurs Recordmanagement onderzoek gedaan naar persoonsgegevens in de schadedossiers in het iDMS en onderzocht hoelang deze gegevens bewaard moeten worden op grond van de AVG en de Archiefwet. De volgende persoonsgegevens zijn bij het onderzoek in de schadedossiers in het iDMS naar voren gekomen:

- Naam van de persoon die schade geleden of veroorzaakt heeft
- Bankrekeningnummer van de persoon aan wie schade vergoed wordt
- Bankrekeningnummer van de PZH.

In het geval van schadedossiers gaat het om een beperkt aantal persoonsgegevens, maar dat kan in andere dossiers wellicht veel meer zijn. Het is dan ook aan te bevelen om te onderzoeken welke

andere dossiers in iDMS persoonsgegevens bevatten. Tegelijkertijd is het zaak ook andere informatiesystemen en applicaties buiten iDMS hierop te onderzoeken. Deze aanvullende vraag heeft geresulteerd in deze memo over de wijze waarop onze organisatie dient om te gaan met persoonsgegevens. De inhoud van deze memo is afgestemd met de Functionaris voor Gegevensbescherming, de provinciearchivaris, de bestuurlijk-juridisch adviseur en strategisch adviseur informatiebeveiliging.

Advies aan MT

Gezien de urgentie en de risico's die samenhangen met dit onderwerp vragen wij het MT om op korte termijn iemand aan te wijzen die het beleid gaat formuleren. Daarnaast vragen wij het MT om mee te denken wat de meest effectieve manier is om het beleid binnen de organisatie uit te dragen.

Nota van bevinding- Randstedelijke Rekenkamer, 2022

Grotendeels werkt de provincie al volgens het nieuwe regime van de Woo. Zo is elektronische indiening van Wob-verzoeken al mogelijk en worden besluiten (inclusief achterliggende documenten) op Wob-verzoeken gepubliceerd op de website. De beslistermijnen zijn nog een aandachtspunt op weg naar de Woo.

Stukken beter bewaard, 2022

Met Stukken Beter Bewaard (SBB) zal PZH haar efficiëntie en effectiviteit van de informatiehuishouding verbeteren. De "Visie op een toekomstbestendig Informatiebeheer" van Gartner1 geeft aan wat er nodig is om de informatiehuishouding sterkte verbeteren. Dit zal gerealiseerd worden door onder anderen het optimaal inzetten van kaders, opleidingen, technologie, veranderingsbeheer. Mede door het inzetten van een organisatie brede bewustwordingscampagne, zal het besef vergroot worden dat 'een informatiehuishouding op orde' een gemeenschappelijke verantwoordelijkheid is. Stukken Beter Bewaard is opgegaan in het programma Informatietransitie.

Programma Informatietransitie, 2023

De PZH investeert de komende jaren fors in digitalisering. De digitale provincie is één van de speerpunten. Als basis voor de digitalisering wordt de komende jaren het informatiebeheer op orde gebracht. Op 31-1-2023 heeft GS besloten 23 mln toe te kennen aan het programma Informatietransitie, verdeeld over een periode van 6 jaar.

Met het op orde brengen van het informatiebeheer zet de PZH ook belangrijke stappen in het proces van actieve openbaarmaking van informatie. De uitvoering van het programma zorgt voor een belangrijke andere manier van kijken naar en omgaan met data en informatie binnen de provincie.

Ook wordt met de uitvoering van het programma een grote stap gezet in het data- en informatie-gedreven werken van de provincie. Dit betekent dat de provincie in toenemende mate in de beleidsontwikkeling en besluitvorming in staat is om gebruik te maken van inzichten die uit haar data en informatie met geavanceerde hulpmiddelen worden ontsloten.

Informatieveiligheidsbeleid "Open tenzij" vs "Gesloten tenzij"- AOG-I&A, 2023

- Akkoord met de voorgestelde memo, met de kanttekening dat er een impact analyse uitgevoerd moet worden op (consequenties huidige systemen en gedrag mensen). Ook meenemen lopende ontwikkelingen/trajecten waarbij dit nieuwe beleid niet bij start is meegegeven (bijvoorbeeld programma Informatietransitie).
- Er moet goede aansluiting zijn bij lopende initiatieven zoals het werkend maken van OGO, spoor 2, de systemen en processen, met het OGO geschikt van systemen. Deze aspecten zullen ook in scope moeten komen van deze projecten.

- Daarnaast is het belangrijk om alles by design (zowel archivering, informatieveiligheid, privacy, ethics, transparantie etc) in te regelen, én het makkelijk werken by design moet ook altijd een belangrijk principe zijn.

Vervolg bewustwordingscampagne, 2023

"Zo doen we dat", start november 2023

In 2021 is er door EAA een 1-meting uitgevoerd over de bewuste omgang met informatie, de resultaten daarvan zijn gebruikt om te komen tot een nieuwe campagne, "Zo doen we dat", die binnenkort van start gaat. In deze campagne wordt er vanuit gedragsleer gekeken naar wat er nodig is om mensen het 'gewenste gedrag' te laten vertonen.

Conclusie:

Er zijn vele initiatieven en onderzoeken geweest, vaak is daar opvolging aan gegeven, echter is de urgentie op diverse niveaus vaak niet voldoende onderkend en zijn financiële middelen daardoor veelal niet geboden. De conclusies uit het rapport opgeleverd door Gartner "visie op toekomstbestendig informatiebeheer" komen niet uit de lucht vallen.

Memo

Contact
art.5.1-2e

art.5.1-2e @pzh.nl

Datum
2 oktober 2023

Aan
art.5.1-2e

Kopie aan
art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e

Onderwerp
Data IDMS

Geachte art.5.1-2e

In deze memo beschrijven wij op uw verzoek de stand van zaken met betrekking tot de omgang met persoonsgegevens in IDMS.

Aanleiding en voorgeschiedenis

De directe aanleiding voor deze memo is de melding van een datalek[1] op 7 september door de Chief Information Security Officer (CISO) van PZH. Ook in de periode voor 7 september hebben zich al datalekken voorgedaan in IDMS. In de periode van 2019 tot 7 september 2023 zijn er zeven datalekken geconstateerd en gemeld. De Functionaris voor Gegevensbescherming (FG) heeft in zijn jaarverslagen van 2019 en 2021 erop gewezen dat IDMS niet is ingericht op een adequate naleving van de AVG. De provinciearchivaris heeft in zijn jaarverslag van 2020 benoemd dat hij de risico's op datalekken in IDMS zorgelijk vindt. Dit heeft, zo moeten wij nu constateren, niet geleid tot een voldoende besef van de gebrekkige staat van IDMS ten aanzien van AVG compliancy.

Wij beschrijven in deze memo achtereenvolgens:

1. De aanleiding voor deze memo: het datalek
2. De tot dusver ondernomen acties
3. De voorgenomen acties
4. Reeds lopende verbeteringen
5. Overige acties

1

[1] In de wet wordt een datalek als volgt gedefinieerd: *"een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens."*

Datalek van 7 september 2023

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

IDMS is het centrale document- archiefsysteem van PZH en is alleen intern toegankelijk voor alle medewerkers van PZH (ong. 2460 medewerkers d.d. 22 september '). Er is voor dit datalek geen aanleiding te veronderstellen dat persoonsgegevens onterecht buiten PZH terecht zijn gekomen.

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

De tot dusver ondernomen acties

Voorlopige melding bij de Autoriteit Persoonsgegevens

PZH heeft op 8 september (binnen de wettelijke termijn van 72 uur) bij de Autoriteit Persoonsgegevens (AP) een voorlopige melding gedaan dat er mogelijk sprake is van een datalek dat risico’s inhoudt voor de rechten en vrijheden van betrokkenen[2]. PZH moet uiterlijk op 5 oktober de AP informeren of er sprake is van een datalek met risico voor betrokkenen. De EP bereidt dat voor en meldt dit na akkoord van u.

Onderzoek naar ernst en beëindiging van datalek

De ernst van het datalek en de impact voor betrokkenen is afhankelijk van meerdere factoren. Het hangt onder meer af van het aantal betrokkenen, de aard van de persoonsgegevens en of daadwerkelijk ongeoorloofde toegang heeft plaatsgevonden. PZH voert op dit moment met een interdisciplinair team een onderzoek uit naar de omvang van het gemelde datalek en de mogelijke impact daarvan voor betrokkenen. PZH onderzoekt in hoeverre documenten met de gemelde trefwoorden vrij toegankelijk zijn en of, en zo ja wanneer, die door welke medewerkers ongeoorloofd zijn geraadpleegd. De resultaten komen in verschillende iteraties naar boven en of een definitief inzicht in de omvang en ernst voor 5 oktober is verkregen, is uiterst onzeker. Onderstaand treft u een overzicht aan van de resultaten op de zoektermen van het datalek van 7 september.

Aantallen m.b.t melding AP

Zoekterm	Volledige rechten / api search	Beperkte rechten /api search	Specificeren / filter	Login opgevraagd	Actie genomen	Controle idms search
Paspoort	4705	21120	Naam in titel= 50	Ja, bezig	Ja / deels	39.000?
Curriculum+vitae	47.177	12.305	Naam in titel =69	Ja, bezig	Ja/ deels	
Bibob+vertrouwelijk	216	113		ja	ja	
Bibob+weigeren	111	62		ja	ja	
Bibob+intrekken	59	12		ja	ja	
Bibob+ernstig+gevaar	25	5		ja	ja	
Bibob+strafbaar	11	Correct dicht gezet, niet meer gevonden		ja	ja	
Bibob+gevaarsbeoordeling	2	Correct dichtgezet niet meer gevonden		ja	ja	

[2] Een betrokkene is degene wiens persoonsgegeven het betreft.

Tot dusver is nog geen efficiënte methodiek gevonden die voldoende zekerheid gaat bieden om de vraag naar omvang en impact te kunnen beantwoorden. PZH spant zich de komende dagen tot het uiterste in om het datalek van 7 september zoveel als mogelijk te doen eindigen. Op 4 oktober informeren wij u over de resultaten van die inspanningen.

Bredere steekproef op toegankelijkheid persoonsgegevens in IDMS
Om te onderzoeken of er sprake is van een incidenteel datalek hebben de FG en EP parallel aan het lopende onderzoek een aantal steekproeven uitgevoerd in IDMS met andere trefwoorden naar persoonsgegevens in IDMS die mogelijk te ver open staan. Dit heeft tot de voorlopige conclusie geleid dat er mogelijk meer datalekken in IDMS zijn opgetreden die nog niet zijn opgemerkt en gemeld.

Onderzoek naar oorzaak van het datalek
De melding betreft informatie die onvoldoende afgeschermd stond in IDMS. Toegangsrechten tot gevoelige documenten en/of mappen moeten worden beperkt tot medewerkers die daar voor hun functie toegang toe moeten hebben. In het onderzoek is voorlopig vastgesteld dat map-/documenteigenaren onvoldoende gebruik hebben gemaakt van de afschermingsmogelijkheden die IDMS biedt.

Communicatie richting AP
Strikt genomen kunnen de uitgevoerde steekproeven als meldingsplichtige datalekken worden aangemerkt. De FG, de CISO en manager Interne communicatie adviseren u op 3 oktober over hoe de communicatie richting de AP het best kan worden vormgegeven. Het advies gaat onder meer in of het verstandig is om de uitgevoerde steekproeven als nieuwe datalekken te melden danwel of dat deze bijvoorbeeld beter in de datalekmelding van 8 september aan de AP kunnen worden meegenomen.

Ten aanzien van het datalek van 7 september kan PZH de AP op 5 oktober informeren over de verwachte omvang van het datalek en impact maar kan de AP naar verwachting niet berichten dat het datalek is opgehouden te bestaan. Uiteraard kunnen wel de tot dan getroffen mitigerende maatregelen worden gerapporteerd, de bevindingen tot dusver alsmede het verdere actieplan.

Verantwoordelijkheden t.a.v. IDMS
De verantwoordelijkheden voor informatiesystemen zijn beschreven in het Informatieveiligheidsbeleid van PZH. Er wordt onderscheid gemaakt in (1) zg. *business* applicaties die door een specifieke afdeling/opdracht voor een afgebakende taak worden ingezet en in (2) *generieke* informatiesystemen die door de hele organisatie worden gebruikt. Generieke informatiesystemen betreffen de kantoorautomatisering (email, tekstverwerking) en documentmanagement en archief zoals IDMS. Voor generieke informatiesystemen ligt volgens het informatieveiligheidsbeleid een centrale verantwoordelijkheid bij het DT c.q. concerndirecteur met uitvoering door I&A. Proceseigenaren (binnen OGO: domeindirecteuren/ambtelijk opdrachtgevers) blijven zoals beschreven in het Informatieveiligheidsbeleid en de Baseline Informatiebeveiliging Overheid (BIO) binnen generieke informatiesystemen verantwoordelijk voor o.a. de verwerking en afscherming van hun informatie. DT en I&A moeten zorgdragen dat een informatiesysteem zoals IDMS beveiligingstechnisch op orde is en proceseigenaren in staat stelt hun informatie veilig te verwerken.

<u>De voorgenomen acties</u>
De hiervoor genoemde gebeurtenissen geven aanleiding tot een structureler onderzoek naar de omgang met persoonsgegevens in systemen van PZH.

Doorzoeking van IDMS op ongeoorloofde toegangsmogelijkheden
PZH gaat IDMS risico gebaseerd[3] iteratief doorzoeken op mogelijk ongeoorloofde toegangsmogelijkheden voor medewerkers tot privacygevoelige informatie. Leidt dit onderzoek tot de conclusie dat medewerkers toegang hebben tot privacygevoelige informatie die zij niet nodig hebben in hun functie dan worden de autorisaties

[3] PZH start het onderzoek met de meest privacy gevoelige informatie zoals bijzondere persoonsgegevens.

gecorrigeerd. Daarnaast worden er logbestanden gecontroleerd om te zien of er ongeoorloofd toegang is verkregen tot documentatie in afstemming met HR en P-manager en zo nodig passende acties jegens de medewerker. De eerste doorzoekingen op privacy gevoelige zoektermen hebben plaatsgevonden en geven het volgende beeld:

Volledige versus beperkte rechten (2e search)

Zoekterm	Volledige rechten	Beperkte rechten	Actie genomen
Paspoort	67.296	21.120	Ja> Ap -melding
Curriculum+vitae	47.177	12.305	Ja> ap melding
Cv	16.666	gestopt	-
Bibob+vertrouwelijk	216	113	ja
Bibob+weigeren	111	62	ja
Bibob+intrekken	59	12	ja
Bibob+ernstig+gevaar	25	5	ja
Bibob+strafbaar	11	Correct dicht gezet, niet meer gevonden	Nvt
Bibob+gevaarsbeoordeling	2	Correct dichtgezet niet meer gevonden	nvt

Conclusie: voor wat we kunnen vergelijken, blijft met beperkte rechten gemiddeld 35% over (gemiddelde over beide searches).

Uitkomsten gestructureerd zoeken Volledige versus beperkte rechten (1e search)

Zoekterm	Volledige rechten(api)	Beperkte rechten (api)	Gespecificeerd (specificatie noemen buiten tabel)	Login opgevraagd	Actie genomen	Controle idms search
IBAN	166k-470k	Gestopt		-		
Rekeningnummer	134k-160k	173 922	Regex inzetten?	-		
Afschrift	71k-490k	Gestopt		-		
Vergunningsaanvraag	38.885	25.259				
Legitimatie	39.178	21.809				
BSN	Niet gedraaid de 1e keer?	21.196				
Burgerservicenummer	56.831	16.288				
Personeelsdossier	17.026	3.385				
Kopie+ identiteitsbewijs	17.495	1.942				Advies opnieuw doen, zonder term kopie
Loonstrook	15.030	2.865				
Paspoort	4.705	21120	Filter op naam =50		ja	39.000
Kopie+rijbewijs	226	71				Advies opnieuw doen, zonder term kopie
Lidmaatschap+vakbond	750	57				

Onderzoek naar andere systemen die persoonsgegevens bevatten

Daarnaast is PZH gestart met een voorbereidend onderzoek naar andere systemen die mogelijke persoonsgegevens bevatten. Op advies van de FG worden twee informatiesystemen die ook (ongestructureerde) documenten bevatten aan het vervolgonderzoek toegevoegd (MS Teams en MS Sharepoint). Mogelijk volgt op een later moment nog een onderzoek naar Topdesk. De risico's van dit systeem worden op dit moment lager ingeschat. Dit systeem is namelijk vrij recent nog doorzocht op mogelijke privacy-issues.

<u>Reeds lopende verbeteringen</u>

PZH heeft de afgelopen jaren de inspanning op het gebied van informatiehuishouding, privacy en informatieveiligheid sterk geïntensiveerd. Hieronder worden deze op hoofdlijnen toegelicht:

Informatietransitie

31 januari jl. heeft GS besloten 23 miljoen toe te kennen, over een periode van 6 jaar aan het programma Informatietransitie. Hoe de weg is verlopen naar deze mijlpaal, is te vinden in de bijlage.
In de voorafgaande “visie op een toekomstbestendig informatiebeheer” is vastgesteld dat er een aantal zaken ernstig te kort schiet binnen PZH. Ook is er een aanzet gegeven tot een programmalijn om te komen tot een toekomstbestendig informatiebeheer. Een belangrijke notie daarin: als organisatie ben je hier nooit mee ‘klaar’.

In actielijn 1 ‘Bewustzijn en vaardigheden verhogen’ bevorderen we een cultuur waarin medewerkers gaan handelen in lijn met de kaders van ‘goed’ informatiebeheer en data/informatie-gedreven werken. Initiëren en ondersteunen van activiteiten die het
I-bewustzijn bevorderen en bijdragen aan het gewenste gedrag van directie, regisseurs, managers en medewerkers.

In actielijn 2 ‘Opzetten I-governance en I–control & optimaliseren werkwijze’ zorgen we voor de juiste sturende en ondersteunende processen om risico’s te vermijden en waarde te verhogen. Ontwerpen en implementeren van een I-governance en gesloten
I-control-cyclus & het ontwikkelen van kaders en een werkwijze die bijdragen aan het sturen op gewenste resultaten.

In actielijn 3 ‘Saneren en moderniseren IV-middelen, platformen en informatie’ zorgen we voor een adequaat instrumentarium voor het toekomstbestendig informatiebeheer en data/informatiegedreven werken. Saneren en verbeteren van middelen en informatie, zodat daarmee de strategische doelen meer passend ondersteund worden.

Privacy
De EP is in juni 2022 opgericht om het privacy volwassenheidsniveau van PZH te verbeteren. Op dat moment bleek uit een onderzoek van de eenheid Audit en Advies dat het volwassenheidsniveau zich nabij de 1 bevond. Een niveau van 3 is minimaal gewenst om aantoonbaar aan de AVG te kunnen voldoen. PZH heeft zich ten doel gesteld dit niveau in 2025 bereikt te hebben. De EP heeft zich gericht op het ontwikkelen van een organisatie breed privacy beleid. Dit is enige tijd geleden voorgelegd aan het DT en bevindt zich in fase richting vaststelling door GS. Daarnaast is de EP onder meer actief om het privacy bewustzijn binnen PZH te vergroten, het register van verwerkingen up-to-date te krijgen en de achterstand met betrekking tot het uitvoeren van Data Protection Impact Assessments in te halen. De EP constateert dat er op onderdelen binnen PZH nog onvoldoende urgentie wordt gevoeld voor het belang en (verplichte) karakter van de AVG.

Informatieveiligheid
Informatieveiligheid heeft een bredere taak dan het beschermen van persoonsgegevens en heeft betrekking op de algehele beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening van PZH. Informatieveiligheid raakt onderwerpen zoals governance en verantwoordelijkheden, IT, security testen, personeel, bewustwording en fysieke beveiliging.

In 2022 is een CISO betrokken en is er geïnvesteerd om aantoonbaar aan de verplichte Baseline Informatiebeveiliging Overheid (BIO), de interprovinciaal afgesproken ISO 27001, en straks de NIS2, te voldoen. Vanaf 2022 is de implementatie van de ISO 27001 projectmatig vormgegeven en het strategische informatieveiligheidsbeleid is geactualiseerd. Tactische beleidsdocumenten zijn eveneens geactualiseerd of ontwikkeld, zoals wachtwoordbeleid of risicomanagementbeleid. PZH voert regelmatig pentesten uit. Momenteel wordt er een aanbesteding voor een IT-monitoring, detectie en responsedienst voorbereid om de incidentresponse van de provincie te verbeteren. Daarnaast neemt PZH deel aan alle interprovinciale ontwikkelingen op het gebied van informatieveiligheid, zoals het IP CSIRT, waardoor provincies dreigingsinformatie vanuit het NCSC kunnen ontvangen.
De BIO en de ISO zijn nog niet aantoonbaar in de hele organisatie geïmplementeerd. Het gestelde doel van volwassenheidsniveau 3 wordt naar verwachting eind 2024 aantoonbaar bereikt. Implementatie van nieuw

vastgesteld beleid en werkwijzen, het uitvoeren van bredere recovery testen en crisisoefeningen, versterken van het ISMS (PDCA-cyclus voor informatieveiligheid) en het uitbreiden van trainingen en bewustwording zijn nog belangrijke aandachtspunten.

Bewustwordingscampagne(s)
In 2019 is na een 0-meting een eerste campagne, “Up to data”, geïnitieerd door I&A in samenwerking met bestuur (AVG, Woo en provinciaal archivaris) en P&O (integriteit). De onderwerpen van deze campagne zijn: Data- en informatiekwaliteit, Informatie veiligheid, Privacy, Informatiebeheer en Integriteit. In 2021 is er door EAA een 1-meting uitgevoerd over de bewuste omgang met informatie, de resultaten daarvan zijn gebruikt om te komen tot een nieuwe campagne, “Zo doen we dat”, die binnenkort van start gaat. In deze campagne wordt er vanuit gedragsleer gekeken naar wat er nodig is om mensen het ‘gewenste gedrag’ te laten vertonen.

Overige acties
Voorgestelde beleidsaanpassing 'open tenzij'
Op 14 september '23 heeft het AOG I&A op voorstel van de CISO ingestemd met een beleidsaanpassing voor de informatiehuishouding van 'open tenzij', naar 'gesloten tenzij'. Het voorstel wordt binnenkort aangeboden aan het DT ter vaststelling. PZH heeft momenteel een op de uitgangspunten van 'open tenzij'-gebaseerde informatievoorziening. Dit betekent dat alle informatie voor alle PZH-medewerkers toegankelijk zijn, *tenzij* de documenten actief worden afgeschermd. Dit is foutgevoelig en kan daarmee leiden tot risico's voor de bescherming van persoonsgegevens en andere gevoelige informatie. Het voorstel is om alle informatiesystemen, waar mogelijk, in te richten zodat informatie in beginsel niet voor alle PZH-medewerkers beschikbaar is, *tenzij* deze actief (door een handeling) worden opgesteld. Dit is in lijn met het uitgangspunt van de AVG dat persoonsgegevens alleen mogen worden verwerkt als dat noodzakelijk is.

Tot slot
PZH onderzoekt verder welke andere acties effectief en nuttig kunnen zijn om het risico op datalekken te verminderen. Duidelijk is wel dat proces-/systeemeigenaren actiever op hun rol en verantwoordelijkheden moeten worden aangesproken. Voor advies en ondersteuning bij de invulling van hun rol kunnen zij terecht bij de EP en CISO. Daarnaast moet het privacy bewustzijn bij proceseigenaren en medewerkers worden vergroot. Hierover informeren wij u op een ander moment nader.

art.5.1-2e (EP)
art.5.1-2e Communicati e)
art.5.1-2e FB IDMS)
art.5.1-2e (CISO)
art.5.1-2e art.5.1-2e (BI)
art.5.1-2e I&A)
art.5.1-2e I&A)

art.5.1-2e

Van: art.5.1-2e art.5.1-2e
Verzonden: e p :5
Aan: art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e
Onderwerp:

Goeden morgen all,

Even een korte update

De eerste resultaten zijn binnen en zijn in te zien in de power Bi. Voor diegene die toegang hebben. (link staat waarschijnlijk in de mailbox overig)
Kijk onderin goed naar welk tabblad je bekijkt. Alle rechten of beperkte rechten m.b.t de zoekopdracht. (ook de totalen zijn er nog niet)
Om 13. 00 uur (dinsdag) bespreken we de rapportage in kleine groep verder.

Helaas is wel de "run" van het script opnieuw onderbroken. (dit is de derde keer)
We wachten daarom nog op de resultaten van 5 zoektermen (cv, paspoort, iban, rekening nummer, afschrift)
Als er geen onderbrekingen meer zijn, dan is morgenochtend alles compleet in het dashboard.

Tot zover, art.5.1-2e art.5.1-2e

-----Oorspronkelijke afspraak-----
Van: art.5.1-2e
Verzonden: maandag 25 september
Aan: art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e art.5.1-2e
Onderwerp: Data (incl. lunch)
Tijd: woensdag 27 september 2023 12:00-13:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
Locatie: C3.84.12 - art.5.1-2e (Den Haag)
Gevoeligheid: Privé

Met vriendelijke groet,

art.5.1-2e
Senior Secretaresse van art.5.1-2e
Concerndirecteur/ loco-provinciesecretaris Provincie Zuid-Holland

T art.5.1-2e
E art.5.1-2e @ pzh.nl

Microsoft Teams-vergadering

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

Klik hier om deel te nemen aan de vergadering

Vergadering-id: 399 221 147 162
Wachtwoordcode: R8BqEV
Teams downloaden | Deelnemen op het web

Meer informatie | Opties voor vergadering

Datalek TMS

Afdeling Samenleving en Economie, Bureau Cultuur en Vrije tijd

art.5.1-2e

The Museum System (TMS)

Systeem

Processen:	• Processen Provinciaal Archeologisch Depot.
Functionaliteit:	• Registratie onderzoeken / opgravingen en bijbehorende objecten • Registratie bruiklening tbv tentoonstelling of onderzoek • Selecteren van op de website http://archeologie.zuid-holland.nl te tonen objecten. (*) (*) In samenwerking met de applicatie CollectionConnection.
Gebruikersgroepen:	Er zijn 5 actieve gebruikers: 2 met bewerk rechten, 3 met leesrechten. art.5.1-2e
Autorisatie:	art.5.1-2e s contactpersoon met de leverancier, C'IT. De leverancier maakt indien gewenst extra accounts aan.

Gegevens

Input:	• Afbeeldingen van gevonden objecten. Deze worden op een Share van de leverancier geplaatst en vanaf daar in TMS geïmporteerd.
Verwerking:	• Administratieve gegevens rondom onderzoeken, objecten, uitleningen ed • Beeldmateriaal + beschrijvende kenmerken van objecten • Criteria op basis waarvan publicatie op een website wordt afgeleid
Output:	• Direct vanuit systeem: niet van toepassing • Op database niveau wordt er een dagelijkse export (van een aantal velden) gebruikt om CollectionConnection te voeden. Zowel TMS als CollectionConnection worden technisch en functioneel extern beheerd door de leverancier. Het exacte mechanisme is daarom niet in beeld.
Opslagplaats:	De applicatie, gegevens en documenten worden bij C'IT gehost.

Privacy

Persoonsgegevens:	• Gegevens van contactpersonen

	• Namen van personen die een opgraving hebben gedaan
Doel verwerking:	• Contactgegevens • Classificatie
Categorieën:	Zie de checklist persoonsgegevens ().
Aantal persoonsgegevens per persoon:	.Plm 7
Aantal personen met persoonsgegevens:	Er zijn plm. 500 contacten.
Eerste oordeel privacy:	.

Checklist persoonsgegevens

Gebruikersnamen, wachtwoorden en andere inloggegevens	Gebruikersnamen en wachtwoorden (plm. 10 personen)
NAW-gegevens • Naam, adres, woonplaats	• Namen van mensen die een opgraving hebben gedaan • Complete naam van contactpersonen, Naam
Extra NAW-gegevens (privé mailadres, telefoonnummer, etc.)	Emailadres en telefoonnummer contactpersonen
Gegevens die kunnen worden misbruikt voor (identiteits)fraude • Burgerservicenummer (BSN), Kopieën van identiteitsbewijzen	Nee
Burgerlijke staat	Nee
Bijzondere persoonlijke gegevens • Godsdienst • Levensovertuiging • Ras • Politieke gezindheid • Seksuele leven • Lidmaatschap van een vakvereniging	Nee (Applicatieveld Nationaliteit bestaat wel, wordt niet gebruikt)
Gegevens over de financiële of economische situatie van de betrokkene • Fiscale gegevens (belastingaangifte, bankafschriften) • BKR-gegevens (Bureau Krediet Registratie)	Nee
Justitiële gegevens • strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag	NVT
Gegevens m.b.t. sociale activiteiten (lid verenigingen)	Nee
Medische gegevens	Nee
Gegevens m.b.t. communicatiegedrag (bel- en surfgedrag)	Nee

Beeldmateriaal van personen	Nee
(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene Hieronder vallen bijvoorbeeld gegevens over • gokverslaving, • prestaties op school of werk of • relatieproblemen	Nee
Gegevens die betrekking hebben op mensen uit kwetsbare groepen Het gaat hier bijvoorbeeld om • mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven • klokkenluiders • informanten van de politie of het Openbaar Ministerie	Nee

Vragen

Wie zijn de gebruikers van TMS	art.5.1-2e geen pzh groepsaccount voor vrijwilligers, extern bedrijf art.5.1-2e
Gebruiken ze PZH inloggegevens?	
Welke persoonsgegevens?	
Contact gehad met de leverancier? art.5.1-2e art.5.1-2e CIT Collecti ons Information Technology	
Wat is Collection Connection?	
Hoe is de toegang tot de WEBDAV-share geregeld? Is er verkeer naar binnen mogelijk?	Extern bureaublad naar CIT server = koppeling naar binnen Daar worden foto's en rapportages op geplaatst Vanuit objectrecord fotos seleteren en dan Via api naar collection connection.

Maandagochtend 7:30 problemen servers niet beschikbaar

Op website

Van: art.5.1-2e @go2cit.nl >
Verzonden: dinsdag 9 februari 2021 13:33
Aan: info <info@go2cit.nl>
Onderwerp: Update stand van zaken 1, maandag 9 februari 2021, 13:30

art.5.1-2e

Gisteren hebben wij u geïnformeerd over het feit dat wij problemen ondervinden met onze servers in ons datacenter. Deze problemen worden veroorzaakt doordat vreemden zich toegang hebben verschaft tot onze servers. Wij zijn hard aan het werk om de infrastructuur zo snel als mogelijk weer te herstellen, data vanuit back-ups weer beschikbaar te maken en de applicaties en websites weer toegankelijk te maken. Ook het onderzoek naar hetgeen precies is gebeurd en de gevolgen daarvan gaat uiteraard door. Wij worden daarbij ondersteunt door een beveiligingsbedrijf.

Wij begrijpen dat u zich zorgen maakt over hetgeen er gaande is en over wat er mogelijk met uw gegevens kan zijn gebeurd. Dit is uiteraard ook een belangrijk deel van het onderzoek dat wij uitvoeren. Wij zullen u ook hierover blijven informeren.

Voor wat betreft de herstelwerkzaamheden hebben wij voortgang geboekt, maar er moet ook nog het nodige werk worden verricht. Helaas kunnen wij nog geen planning geven van het moment waarop alles weer beschikbaar komt.

Wel is duidelijk dat wij de wachtwoorden van alle accounts die kunnen inloggen op onze servers moeten resetten. Dat is een belangrijk deel van de herstelwerkzaamheden en daarbij zijn wij ook afhankelijk van uw medewerking, omdat wij niet beschikken over de persoonsgegevens en e-mailadressen die behoren bij deze accounts.

Voor het opnieuw instellen van de wachtwoorden van de gebruikersaccounts stellen wij voor per gebruiker een e-mail te sturen naar onze contactpersoon met daarin de loginnaam en een tijdelijk wachtwoord van betreffende gebruiker. Wij vragen de contactpersoon deze mails dan door te sturen naar betreffende gebruiker. Deze gebruiker kan dan met de verstuurde informatie een nieuw wachtwoord instellen.

Mocht u zich wel hebben aangemeld als contactpersoon voor deze nieuwsupdates, maar niet de aangewezen persoon zijn voor het doorsturen van de gebruikersgegevens aan uw collega's, dan wil ik u vragen via info@go2cit.nl de contactgegevens (e-mail en telefoonnummer) van de daarvoor aangewezen persoon binnen uw organisatie aan ons door te geven.

Wij beseffen ons goed hoe vervelend deze situatie voor u is en doen er alles aan om de situatie zo snel als mogelijk weer volledig te herstellen en u te informeren over de stand van zaken en de uitkomsten van ons onderzoek. Ook willen wij u hartelijk danken voor het getoonde begrip.

Met vriendelijke groet,

Namens alle collega's van Cit,

art.5.1-2e

CIT
Collections Information Technology

W: www.go2cit.nl

Niet beschikbaar op woensdag
Not available at Wednesday

Personen en instellingen:

- bruikleen contactgegevens museum of historische vereniging
  hoeveel: paar honderd
  algemene contactgegevens, ook elders openbaar< of naam conservator museum x e-mail telefoonr, postadres werkmail
  enkele particulieren naw
  vaak al overleden want collectie overgedragen na dood
  mevr bakker ouddorp + zeer telefoonnr <10 Deze gegevens worden niet op website gepubliceerd (“particulier”)
  Opgravingsbedrijven ADC worden wel genoemd.
  Overleden: Collectie Bakker.

  Opgravinsdocs jaren 60 soms gevoelig burgemeester jansen kwam langs.

art.5.1-2e

Van: art.5.1-2e
Verzonden: 13:14
Aan: art.5.1-2e
CC: art.5.1-2e privacy
Onderwerp: RE: Datalek Eas on duidelijkheid toega.ng enkele PZH medewerkers tot BSN nummers - advies; WEL datalek NIET melden

Beste art.5.1-2e

Dank voor je reactie. Wij weten op dit moment ook niet of de relatie tussen de autorisatiematrix en de processen wel 1 op 1 zijn ingeregeld en of het hier mis kan gaan. We zullen dit punt uitzoeken en je daarover informeren als we meer weten.

Met vriendelijke groet,

art.5.1-2e
Privacy jurist
Eenheid Privacy

provincie Zuid-Holland

M art.5.1-2e
E art.5.1-2e @pzh.nl
www.zuid-holland.nl/contact

Krachtig Zuid-Holland

Van: art.5.1-2e < art.5.1-2e @p zh.nl>
Verzonden: vrijdag 8 september 2023 08:54
Aan: art.5.1-2e < art.5.1-2e @pzh.nl>
CC: Frank Rijkaart <f.rijkaart@pzh.nl>; art.5.1-2e < art.5.1-2e @pzh. nl>; privacy <privacy@pzh.nl>
Onderwerp: FW: Datalek Easyfunders - onduidelijkheid toega.ng enkele PZH medewerkers tot BSN nummers - advies; WEL datalek NIET melden

Dag art.5.1-2e
Dankjewel. Ik volg je advies.
Het brengt me wel op een ander (?) punt. Ik ben natuurlijk geen deskundige, maar het roept bij mij de vraag op of de relatie tussen de autorisatiematrix en de processen wel 1 op 1 zijn ingeregeld. Ik mag toch aannemen dat de autorisaties in de matrix 1 op 1 zijn vertaald naar alle (werk)processen? Of kan het daar mis gaan?
Hartelijke groet, art.5.1-2e

Van: art.5.1-2e < art.5.1-2e @pzh.nl>
Verzonden: donderdag 7 september 2023 16:21
Aan: art.5.1-2e < art.5.1-2e @p zh.nl>

CC: Frank Rijkaart <f.rijkaart@pzh.nl>; art.5.1-2e <art.5.1-2e @pzh. nl>; privacy <privacy@pzh.nl>
Onderwerp: Datalek Easyfunders - onduidelijkheid toegang enkele PZH medewerkers tot BSN nummers - advies; WEL datalek NIET melden

Beste art.5.1-2e

We hebben een melding beoordeeld over het subsidiesysteem Easyfunders. Een subsisieadviseur heeft aangegeven dat er (bij doorklikken) toegang is tot volledige BSN nummers, maar dit voor de uitvoering van de werkzaamheden niet nodig is. Uit onderzoek blijkt dat de interne autorisatiematrix wel aangeeft dat hoofd Subsidies en subsidieadviseurs toegang mogen hebben. Andere rollen zijn afgeschermd. Of de rol van functioneel beheerder recht geeft op inzage in het BSN is nog niet duidelijk geworden. Inzage is in ieder geval beperkt tot enkele medewerkers van PZH en geeft daarom geen hoog risico. Het voorstel is om dit datalek niet te melden bij de AP, maar de beschrijving van inrichting van het systeem, autorisaties en eventuele maatregelen aan te vullen en te beoordelen in de DPIA die al gestart is.

Graag hoor ik of je ons advies volgt.

Met vriendelijke groet,

art.5.1-2e
Privacy jurist
Eenheid Privacy

provincie Zuid-Holland

M art.5.1-2e
E art.5.1-2e @pzh.nl
www.zuid-holland.nl/contact

Krachtig Zuid-Holland

Ontvangstbevestiging van melding inbreuk

AUTORITEIT PERSOONSGEGEVENS

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegeven ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: art.5.1-2e

Melddatum: 06 juli 2023

Meldtijdstip: 15:55

1 Introductie

1.1 De melding van een inbreuk

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

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

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

1.3 Andere toezichthouders

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

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

AUTORITEIT PERSOONSGEGEVENS

KVK-nummer (indien van toepassing)	27375169
Naam van het bedrijf of de organisatie	Provincie Zuid-Holland
Adres	Zuid-Hollandplein 1
Postcode	2596AW
Plaats	Den Haag

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Provincie

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	art.5.1-2e
Functie	Privacy officer
E-mailadres	art.5.1-2e @pzh.nl
Telefoonnummer	art.5.1-2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Ja

Geef aan welke andere organisaties betrokken waren bij de inbreuk?

AUTORITEIT PERSOONSGEGEVENS

Naam	Op welke wijze betrokken	Toelichting (optioneel)
IV-Groep	aannemer (uitvoerend)	in opdracht van Provincie Zuid-Holland
ICT-leverancier van IV-Groep	(sub)verwerker van IV-Groep	

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	1-12-2022
(Mogelijke) einddatum van de inbreuk	31-12-2022
4.2 Wanneer is het incident ontdekt?	4-7-2023
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	De IV-Groep heeft dinsdag 4 juli een melding gedaan aan de Provincie Zuid-Holland. De IV-Groep geeft aan dat door hun deze leverancier het volgende is geconstateerd: - het Azure Storage account waarmee de backups van onze Ftp-server werden gemaakt, was niet voldoende beveiligd, waardoor deze benaderbaar was vanaf internet. Deze back-up service is eind 2022 beëindigd. Dit is door een externe beveiligingsonderzoeker (ethische hacker) , aangesloten bij DIVD, geconstateerd.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

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

[✓] Hacking, malware (bijv. ransomware) en/of phishing

Meerdere opties zijn mogelijk binnen het gearceerde deel.

[✓] Ander type hacking en/of malware

Heeft u (digitaal forensisch) onderzoek uitgevoerd of laten uitvoeren naar de aard en de omvang van het datalek?	Ja, het onderzoek is afgerond

Optioneel: upload hier de rapportage van het onderzoek naar de inbreuk.

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Iv-Groep is een Nederlands ingenieurs bureau en is werkzaam in diverse marktsegmenten (water, infra, industrie, offshore & energy, bouw). Via één van haar werkmaatschappen zijn er werkzaamheden verricht voor de Provincie Zuid-Holland. Voor het uitwisselen van grote hoeveelheid bestanden is er gebruik gemaakt van een zogenaamde Ftp-server. Deze Ftp server wordt beheerd door één van de ICT-dienstverleners van Iv-Groep. Hierop kan via een toegekende gebruikersnaam en wachtwoord toegang tot deze informatie verkregen worden, zowel door Iv-medewerkers als door Provincie Zuid-Holland als opdrachtgever. Door deze ICT-dienstverlener is geconstateerd dat het Azure Storage account waarmee de backups van de Ftp-server werden gemaakt, niet voldoende was beveiligd, waardoor deze benaderbaar was vanaf internet. Dit is geconstateerd door een externe beveiligingsonderzoeker (ethische hacker), aangesloten bij DIVD. Deze back-up service is eind 2022 beëindigd. Er is geen aanwijzing dat er onbevoegde toegang is geweest (anders dan de ethisch hacker). Er is onvoldoende logging beschikbaar om dit met zekerheid vast te stellen.

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

AUTORITEIT PERSOONSGEGEVENS

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Contactgegevens

[✓] Adres en woonplaats

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk

Geef een toelichting op bovengenoemd aantal: Het betreft een adressenlijst met 700 NAW gegevens van bewoners, waarschijnlijk gebruikt voor etikettering van een standaard brief.

7 Getroffen personen

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

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk: aanwonenden van een provinciale weg

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen. aanwonenden van een provinciale weg aan wie een brief moest worden gestuurd.

7.3 Is het exacte aantal betrokkenen bekend? Ja

Het exacte aantal is: 700

8 Maatregelen vooraf

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

9 Gevolgen

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

Meerdere opties zijn mogelijk.

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

Namelijk:	

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Het betreft NAW gegevens die met minimale inspanning ook op andere manieren verkregen kunnen worden.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

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

Van hoeveel personen wilt u de inbreuk gaan melden?	700
Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?	7-8-2023
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Nog niet bekend

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

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

Meerdere opties zijn mogelijk.

[✓] Per brief

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nog niet bekend
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nog niet bekend

11 Verzenden

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

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

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

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

AUTORITEIT PERSOONSGEGEVENS

eef aan wanneer u (uiterlijk) een vervolgmelding
ient
Toelichting

6-9-2023

Nader onderzoek waarbij wij afhankelijk zijn van informatie afkomstig van een derde partij (en de ICT-leverancier van die derde partij) in een vakantieperiode.

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP