AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

[redacted]
Aangeboden per e-mail[redacted]

Datum
6 juni 2024

Ons kenmerk
[redacted]

Uw Woo-verzoek van
4 oktober 2023

Contactpersoon
[redacted]
070 8888 500

Onderwerp
Woo-besluit

Geachte[redacted]

Op 4 oktober 2023 heeft u de Autoriteit Persoonsgegevens (AP), met een beroep op de Wet open overheid (Woo), verzocht om informatie en documenten. Uw verzoek ziet, samengevat, op de openbaarmaking van alle publieke informatie over datalekken in de periode van 1 januari 2019 tot heden.

Op 25 oktober 2023 is de ontvangst van het Woo-verzoek per e-mail aan u bevestigd. Vanwege de gecompliceerdheid van uw verzoek, en de beperkte personele capaciteit, verdaagden wij de beslistermijn met twee weken. Dit hebben wij gedaan met toepassing van artikel 4.4, tweede lid, van de Woo.

Ondanks onze inspanningen is het ons helaas niet gelukt om binnen de wettelijke termijn te beslissen op uw verzoek, waarvoor onze excuses.

Besluit
De AP besluit de door u opgevraagde en door ons aangetroffen informatie gedeeltelijk openbaar te maken. U kunt de informatie in het bijgesloten document vinden.

Hieronder licht de AP dit besluit aan u toe.

Uw Woo-verzoek
Uw verzoek ziet op de volgende documenten:

"1. Documenten ten aanzien van procedures en beleid ten aanzien van datalekken;
2. Documenten ten aanzien van de behandeling en afhandeling van meldingen van (mogelijke) datalekken;

3. *Documenten ten aanzien van de vastlegging van afstemming van (mogelijke) datalekken, waaronder ook adviezen;*
4. *Reglementen, handboeken, draaiboeken en procedures ten aanzien van datalekken;*
5. *Maatregelen die zijn genomen naar aanleiding van eerdere (vermeende) datalekken (in het kader van het zelflerend vermogen van de organisatie);*
6. *Audits ter voorkoming van datalekken."*

In de toelichting bij uw verzoek heeft u het volgende aangegeven: "Technische wetenswaardigheden die kwaadwillenden in de gelegenheid stellen schade aan te brengen aan de systemen van uw organisatie, mogen worden weggelakt. Persoonsgegevens mogen worden weggelakt, behalve voor zover die zien op politieke ambtsdragers." De informatie zoals aangegeven in uw toelichting heeft de AP daarom in acht genomen bij het beoordelen en weglakken van de in de documenten aangetroffen informatie. Op de inventarislijst staat bij deze documenten aangegeven: 'BR' (Buiten Reikwijdte).

Wettelijk kader
De AP behandelt uw verzoek als een verzoek om openbaarmaking van informatie op grond van de Wet open overheid. Een Woo-verzoek wordt ingewilligd (artikel 4.1, zevende lid, van de Woo), voor zover de AP over de informatie beschikt, de informatie niet al openbaar is en de uitzonderingsgronden van hoofdstuk 5 van de Woo hieraan niet in de weg staan.

Hieronder legt de AP uit wat dit betekent voor uw Woo-verzoek.

Zoekslag
Op basis van uw verzoek en door het uitvoeren van de zoekslag zijn zeven documenten aangetroffen.

Reeds openbare documenten
De Woo is niet van toepassing op documenten die al openbaar zijn. Een aantal documenten is reeds openbaar en staat op de inventarislijst als zodanig aangemerkt. Op de inventarislijst staat ook aangegeven waar u deze documenten online kunt vinden.

Motivering bij gedeeltelijke openbaarmaking
Ingevolge artikel 4.1, zevende lid, van de Woo wordt een verzoek om informatie ingewilligd met inachtneming van het bepaalde in hoofdstuk 5 van de Woo. Het recht op openbaarmaking op grond van de Woo dient uitsluitend het publieke belang van een goede en democratische bestuursvoering en komt iedere burger in gelijke mate toe. Daarom kan ten aanzien van de openbaarheid geen onderscheid worden gemaakt naar gelang de persoon of de bedoeling of belangen van de verzoeker. Bij de belangenafweging worden daarom het algemene belang van openbaarmaking en de te beschermen belangen door de weigeringsgronden betrokken. Het specifieke belang van de verzoeker wordt hierbij niet betrokken. Verder wordt de informatie die aan u openbaar wordt gemaakt ook aan eenieder openbaar gemaakt. In dit licht vinden de onderstaande belangenafwegingen dan ook plaats.

<u>De eerbiediging van de persoonlijke levenssfeer (artikel 5.1, tweede lid, onder e, van de Woo)</u>
In de documenten die gedeeltelijk openbaar worden gemaakt, staan persoonsgegevens. Dit

zijn gegevens die, al dan niet in samenhang met andere gegevens, herleidbaar zijn tot een persoon, zoals persoonsnamen, telefoonnummers, e-mailadressen, handtekeningen, initialen en zaaknummers (aangemaakt door de AP). Voor zaaknummers geldt daarbij dat openbaarmaking het risico zou vergroten dat (persoons)gegevens uit dossiers van de AP terecht kunnen komen bij onbevoegden.

Openbaarmaking van de genoemde (persoons)gegevens zou een inbreuk op de persoonlijke levenssfeer van de betrokkenen maken. Onder de betrokkenen behoren ook ambtenaren. Wij wegen het belang van eerbiediging van de persoonlijke levenssfeer zwaarder dan het belang van openbaarmaking. Deze informatie wordt dan ook niet openbaar gemaakt.

<u>Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen (artikel 5.1, tweede lid, onder i, van de Woo)</u>
Het belang van het goed functioneren van de AP als bestuursorgaan weegt naar het oordeel van de AP zwaarder dan het algemene belang van openbaarheid. Op grond van artikel 5.1, tweede lid, aanhef en onder i, van de Woo kan de AP geen informatie openbaar maken wanneer dit het goed functioneren van de Staat of andere overheden schaadt en dit belang zwaarder weegt dan het belang van openbaarheid. In één document staat informatie die het functioneren van de AP (als toezichthouder) in gevaar zou kunnen brengen. Het gaat om een intern e-mailadres van een afdeling. Bij het algemeen bekend worden van dit e-mailadres bestaat een aantoonbaar groot risico dat de e-mailbox vol zal lopen met spam, grote hoeveelheden e-mails met als bedoeling de overheid te frustreren of e-mails die naar een ander e-mailadres gezonden behoren te worden ten einde een vlotte en goede afhandeling te kunnen garanderen. Dit schaadt het goed functioneren van (die afdeling binnen) de AP. Wij vinden dat dit belang zwaarder moet wegen dan het belang van openbaarheid. Deze informatie wordt dan ook niet openbaar gemaakt.

Publicatie
Dit besluit, de inventarislijst en de te openbaren documenten, zal de AP geanonimiseerd publiceren op haar website.

Bezwaar
Wilt u een toelichting op het besluit? Neem dan contact op met de contactpersoon bovenaan de brief. Deze contactpersoon neemt dan samen met u het besluit door. Indien u het niet eens bent met dit besluit, kunt u bezwaar maken. Meer informatie over de bezwaarprocedure vindt u in de bijlage die bij deze brief is gevoegd.

Hoogachtend,
Autoriteit Persoonsgegevens,
Namens deze

[redacted]

Datum
6 juni 2024

Ons kenmerk
[redacted]

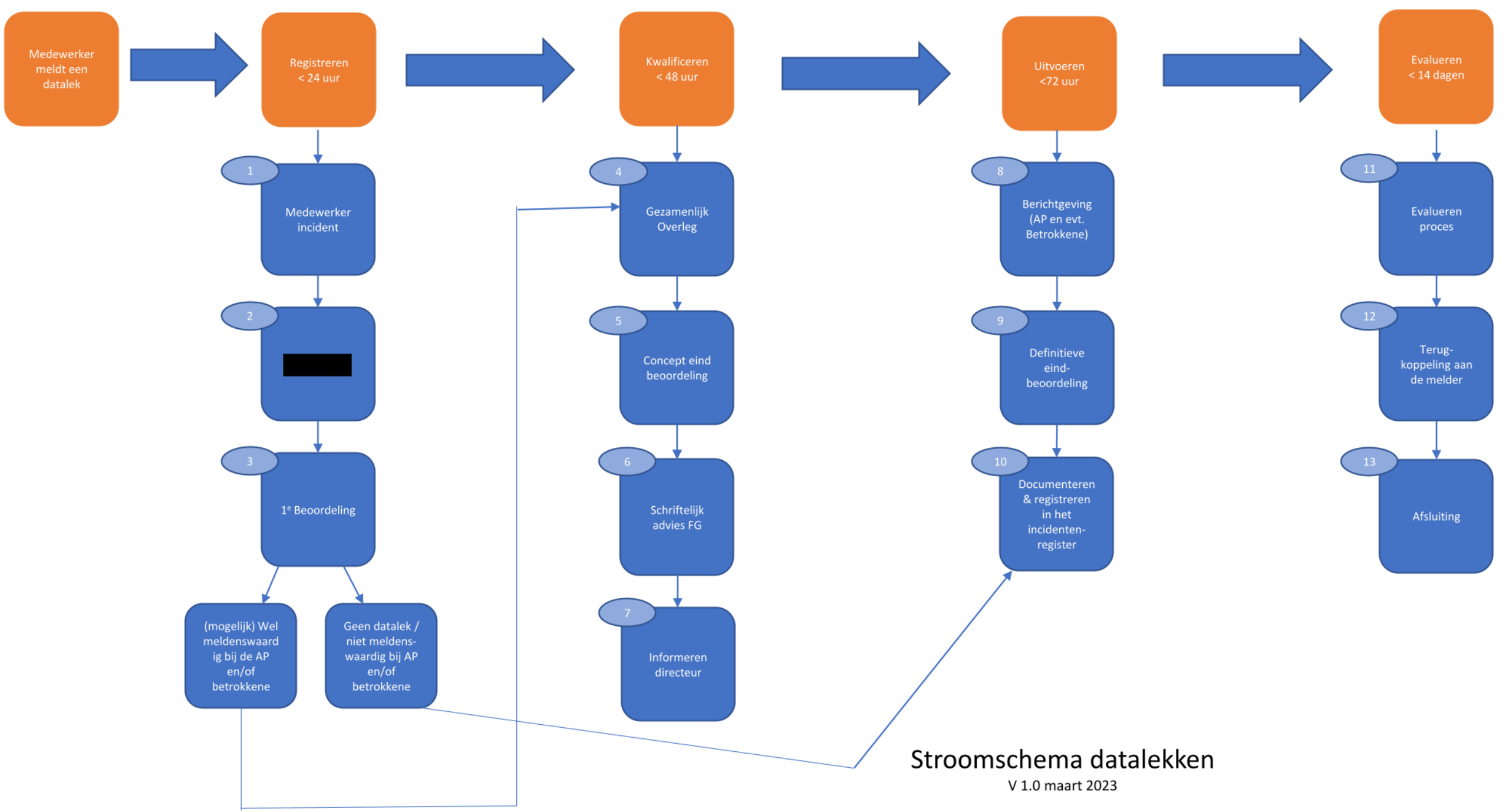
Rechtsmiddelenclausule
Bent u het niet eens met de inhoud van dit besluit? Dan kunt u binnen zes weken na de verzenddatum van dit besluit digitaal of schriftelijk bezwaar indienen. Op autoriteitpersoonsgegevens.nl/bezwaar-maken leest u hoe u dit doet.

Op autoriteitpersoonsgegevens.nl/bezwaar-maken vindt u het digitale formulier waarmee u uw bezwaar indient.

Als u schriftelijk bezwaar wilt maken, dan moet u uw brief binnen zes weken na de verzenddatum van dit besluit sturen naar het bovenaan deze brief genoemde postadres. Vermeld op de envelop 'Awb-bezwaar' en zet 'bezwaarschrift' in de titel van uw brief. Neem in uw bezwaar ten minste op:

- *uw naam en adres;*
- *de datum van uw bezwaar;*
- *de reden(en) waarom u het niet eens bent met dit besluit;*
- *uw handtekening;*
- *het bovenaan deze brief genoemde kenmerk of een kopie van dit besluit.*

Document nummer	Bestandsnaam	Weigeringsgrond	Tags	Vindplaats:
1	20230406-Stroomschema-Datalekken	5.1.2.e	Deels openbaar	
2	Toelichting-Datalekken-2023-1.0	5.1.2.e, 5.1.2.i, BR	Deels openbaar	
3	Werkafspraken bij datalekken versie 1.0	5.1.2.e, BR	Deels openbaar	
4	Jaarrapportage meldplicht datalekken 2019		Reeds openbaar	https://www.autoriteitpersoonsgegevens.nl/documenten/jaarrapportage-meldplicht-datalekken-2019
5	Jaarrapportage meldplicht datalekken 2020		Reeds openbaar	https://www.autoriteitpersoonsgegevens.nl/documenten/jaarrapportage-meldplicht-datalekken-2020
6	Jaarrapportage meldplicht datalekken 2021		Reeds openbaar	https://www.autoriteitpersoonsgegevens.nl/documenten/jaarrapportage-meldplicht-datalekken-2021
7	Jaarrapportage meldplicht datalekken 2022		Reeds openbaar	https://www.autoriteitpersoonsgegevens.nl/documenten/jaarrapportage-meldplicht-datalekken-2022



Stroomschema datalekken

V 1.0 maart 2023

Toelichting stroomschema datalekken

Proces datalekken bestaat uit de volgende documenten:[1]

1. Stroomschema;
2. Toelichting stroomschema datalekken.

Het stroomschema en de toelichting zijn van toepassing op alle incidenten waarbij persoonsgegevens zijn betrokken. De [redacted] is regiehouder, zodat overzicht gedurende het proces blijft. De [redacted] is tevens degene die alle documenten bewaart. De [redacted] en [redacted] zullen in gezamenlijkheid de verschillende beoordelingen doen en daarmee continu met elkaar in contact staan. De medewerker die meldt is alleen verantwoordelijk voor het melden van het incident en het aanleveren van alle relevante informatie (pro actief en op verzoek).

Versiebeheer

Versie	Datum	Opsteller
V0.1	December 2022	[redacted]
V0.2	Januari 2023	
V0.3	Januari 2023	
V0.4	Februari 2023	
V0.5	Maart 2023	
V1.0	Maart 2023	

De [redacted] draagt zorg voor het actualiseren van het document. Jaarlijks controleert de [redacted] of het document herzien dient te worden. De [redacted] zal alle documenten met betrekking tot incidenten op de [redacted] bewaren.

[1] Om de verschillende documenten samen te stellen zijn de volgende bronnen gebruikt: Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679. Goedgekeurd op 3 oktober 2017 en laatstelijk herzien en goedgekeurd op 6 februari 2018. Recommendations for a methodology of the assessment of severity of personal data breaches. Enisa working document, v1.0, december 2013

Inhoudsopgave

Stappen beoordeling incident

Registratie <24 uur

1. Medewerker incident
   De medewerker die een (mogelijk) incident ontdekt of zelf heeft veroorzaakt neemt contact op met de [redacted] en de [redacted] door een e-mail te sturen naar:
   - [redacted]@autoriteitpersoonsgegevens.nl;
   - In het geval van hoge urgentie, wordt telefonisch contact opgenomen met de [redacted] en/of [redacted];
   - In de berichtgeving aan de [redacted] en/of [redacted] wordt door de medewerker die het incident meldt zoveel mogelijk relevante informatie verstrekt.

   Bij afwezigheid van de [redacted] en/of [redacted] worden deze waargenomen door:

functie	Waarnemer
[redacted]	[redacted]

2. [redacted]
   Door: [redacted]
   - De [redacted] en/of [redacted] neemt contact op met de medewerker die het incident heeft gemeld om de situatie te verhelderen;
   - De [redacted] en/of [redacted] gebruikt hiervoor *bijlage A* van dit document;
   - Indien van toepassing vraagt de [redacted] aan de dossiereigenaar de contactgegevens op van de verwerker;
   - De [redacted] en/of [redacted] documenteert de relevante informatie.

3. 1e Beoordeling
   Door: [redacted] & [redacted]
   De eerste beoordeling geeft antwoord op:
   - Is er sprake van een datalek? Zo nee, dan wordt er meteen naar stap 10 gegaan en kan de evaluatie (stap 11) overgeslagen worden.
   - Inschatting van de ernst;
     Zie bijlage B :
     - Meldingsplicht bij de AP?
     - Meldingsplicht bij de betrokkene?
     - Directe mitigerende maatregelen noodzakelijk in het kader van incident management t.b.v. isolatie, analyse en herstel van het datalek? >>>>>**Actie uitzetten!**
   - De [redacted] informeert de directeur van de betreffende afdeling (indien relevant de melder) - en waar relevant wordt ook het bestuur door de [redacted] geïnformeerd - en de [redacted]

Kwalificeren < 48 uur

4. Gezamenlijk Overleg
   Door: [redacted]
   De [redacted] initieert een overleg dat plaatsvindt tussen [redacted] melder van het incident en (optioneel) een communicatiemedewerker.

5. Concept eindbeoordeling
   Door: [redacted]
   Zie bijlage B

   - Is er sprake van een datalek (art. 33 AVG)?
   - Dient het datalek gemeld te worden bij de AP?
   - Dient de betrokkene geïnformeerd te worden over het datalek? (zie bijlage C).
   - Zijn er mitigerende maatregelen nodig en/of zijn de genomen mitigerende maatregelen voldoende/treffend? De [redacted] doet tevens schriftelijk verslag aan de [redacted] van diens overwegingen en conclusies. Hiermee wordt voldaan aan het accountabilityvereiste;
   - Dient over het datalek intern en/of extern gecommuniceerd te worden? En wat dient er gecommuniceerd te worden?[2] De [redacted] en afdeling Communicatie overleggen of, en zo ja wat er gecommuniceerd wordt intern en/of extern.
   - Eigen aansprakelijkheid van de AP en/of aansprakelijkheid van derden (controleer de verwerkersovereenkomst). De [redacted] houdt de regie. De dossiereigenaar is verantwoordelijk;
   - Het al dan niet doen van aangifte bij de politie. Het doen van aangifte wordt gedaan in overleg met stafzaken.

   De eindbeoordeling wordt schriftelijke vastgelegd incl. overwegingen en onderbouwingen daarvan door de [redacted] De [redacted] zet - indien noodzakelijk - de vervolgacties uit en is aanspreekpunt en houdt regie over het proces.

6. Schriftelijk advies [redacted]
   Door: [redacted]
   De [redacted] wordt geïnformeerd en gevraagd om een schriftelijk advies ten aanzien van de concept eindbeoordeling. De [redacted] stuurt deze in ieder geval aan de [redacted].

7. Informeren directeur van de betreffende afdeling
   Door: [redacted]
   - De concept eindbeoordeling en het advies van de [redacted] wordt gedeeld met de directeur van de betreffende afdeling en indien relevant met het bestuur. De directeur (of indien van toepassing het bestuur) neemt een besluit over de te volgen stappen. Dit kunnen stappen zijn die geadviseerd zijn door de [redacted] maar ook door de

[2] Denk aan berichtgeving binnen de organisatie of media.

directeur of onder verantwoordelijkheid van de directeur bedachte stappen om risico's te mitigeren en een nieuw datalek te voorkomen;
- Concept communicatie wordt gedeeld en overhandigd aan de betreffende directeur (indien van toepassing). De concept communicatie kan toezien op communicatie intern, de betrokkene(n) of extern.

Uitvoeren < 72 uur

8. Berichtgeving (AP en evt. Betrokkene)
   Door: [redacted], directeur en afdeling Communicatie
   - De [redacted] doet een melding bij de AP. *Zie bijlage C*;
   - De directeur van de betreffende afdeling doet de berichtgeving aan de betrokkene(n) en indien noodzakelijk in overleg met de afdeling communicatie aan andere(n) intern/extern. Berichtgeving aan de media gebeurt altijd door afdeling communicatie;
     Voor een conceptbrief aan de betrokkene(n) zie *bijlage D en E*.
   - De directeur zorgt dat de te volgen stappen worden uitgevoerd.

9. Definitieve eindbeoordeling
   Door: [redacted] en [redacted]
   De [redacted] en [redacted] komen- nadat alle relevante informatie beschikbaar is - tot een definitieve beoordeling van het incident. De definitieve beoordeling wordt schriftelijk vastgelegd. De [redacted] bewaart de documenten.

10. Registreren in het incidentenregister
    Door: [redacted]
    De [redacted] zal het incident registeren in het incidentenregister, zodat een overzicht van alle incidenten en datalekken beschikbaar is.

Evalueren < 14 dagen

11. Evalueren proces
    Door: [redacted] en directeur[3]
    - De bovengenoemde gremia evalueren het proces en de genomen maatregelen;
    - De [redacted] legt de conclusies schriftelijke vast.

12. Terugkoppeling aan de melder
    Door: [redacted]
    De [redacted] doet een terugkoppeling aan de melder van het incident.

13. Afsluiting
    Door: [redacted]

[3] Een directeur kan zich ook laten vervangen door een betrokken medewerker of deze er bij betrekken.

Verslagen en bevindingen worden gedocumenteerd en verstrekt aan de [redacted] en de betreffende directeur.

Incidentenregister

Alle incidenten dienen geregistreerd te worden. Dit doet de AP in het incidentenregister. Alle beschikbare informatie van een incident of datalek wordt bewaard. De [redacted] is de regiehouder van het datalekproces waardoor deze alle documenten tot diens beschikking heeft en deze op een juiste wijze kan bewaren. Daarnaast houdt de [redacted] het incidentenregister actueel.

Het incidentenregister is toegankelijk voor de [redacted]

BIJLAGE A VRAGEN MELDING INCIDENT

Om het invullen zo efficiënt mogelijk te laten verlopen, worden de relevante gegevens tijdens de procedure reeds geregistreerd. De onderstaande vragen dienen als hulpmiddel om het incident zo snel mogelijk duidelijk te maken.

	Vraag	Antwoord
1	Contactgegevens van de melder van het incident.	
2	Omschrijving van het incident.	
3	Wanneer werd het incident ontdekt? Datum en tijdstip van binnenkomst van de melding noteren.	
4	Wanneer heeft het incident daadwerkelijk plaatsgevonden?	
5	Kwalificeert het incident als datalek?	
6	Zijn er andere organisaties bij betrokken? Contactgegevens vastleggen.	
7	Duurt de inbreuk nog voort?	
8	Wordt het datalek gemeld bij de AP + onderbouwing?	
9	Wat is de aard van de inbreuk?	
10	Is er specifieke categorie betrokkenen dat wordt getroffen?	
11	Inschatting aantal betrokkenen bij het incident?	
12	Welke soort (persoons)gegevens zijn getroffen?	
13	Zijn er negatieve gevolgen te verwachten voor de betrokkene(n)?	
14	Zijn er mitigerende maatregelen getroffen om de gevolgen van de het incident te beperken. Zo ja, welke?	
15	Wordt het datalek gemeld aan de betrokkene(n) + onderbouwing?	
16	Waren de persoonsgegevens ontoegankelijk gemaakt voor onbevoegden?	

17	Heeft de inbreuk betrekking op betrokkenen in andere (EU)-landen?	
18	Is het datalek gemeld bij toezichthouders in één of meer andere landen in de EU?	
Onderzoeksrapportage(s)		

BIJLAGE B BEOORDELING INCIDENT

Om te beoordelen of een incident gekwalificeerd wordt als datalek dient aansluiting gevonden te worden met de definitie genoemd in art. 4 lid 12 jo art. 33 en 34 AVG.

Art. 4 lid 12 AVG

" 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"

Wat betreft de omstandigheden van de inbreuk gelden de volgende drie elementen:

1. *Inbreuk op de vertrouwelijkheid*
   Verlies van vertrouwelijkheid treedt op wanneer informatie door derden wordt ingezien die niet geautoriseerd zijn of geen legitiem doel hebben om toegang te krijgen. De mate van de inbreuk is afhankelijk van de reikwijdte van de openbaarmaking.
2. *Inbreuk op de integriteit*
   Verlies van de integriteit treedt op wanneer oorspronkelijke informatie wordt gewijzigd en vervangen door gegevens die schadelijk zijn voor de betrokkene.
3. *Inbreuk op de beschikbaarheid*
   Verlies van beschikbaarheid treedt op wanneer de oorspronkelijke gegevens niet toegankelijk zijn terwijl er wel behoefte aan is. De toegankelijk kan tijdelijk of permanent zijn. Daarnaast dient onderzocht te worden of er sprake is van kwaad opzet of dat de inbreuk te wijten was aan een vergissing.

Een inbreuk wordt altijd beschouwd als een inbreuk op de beschikbaarheid als persoonsgegevens permanent verloren of vernietigd zijn.[4]

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.

[4] Zie 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.

MELDEN AAN DE AP

Art. 33 lid 1 AVG bepaalt dat:

"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"

Een datalek dient in de basis altijd gemeld te worden bij de AP, *tenzij* de verwerkingsverantwoordelijke conform het verantwoordingsbeginsel kan aantonen dat het onwaarschijnlijk is dat deze inbreuk risico's – lichamelijke, materiele of immateriële schade - voor de rechten en vrijheden van natuurlijke personen met zich meebrengt. Dit zal mede afhangen zoals de aard en omvang van de verwerkingen.

Een hoog risico zijn in beginsel bijvoorbeeld:

1. Veel gegevens per betrokkene en/of om veel betrokkenen op wie de gegevens betrekking hebben;
2. Bijzondere persoonsgegevens (art. 9 lid 1 AVG);
3. Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (art. 10 AVG);
4. Financieel- economische gegevens (gevoelige persoonsgegevens);
5. Gegevens die kunnen leiden tot stigmatisering of uitsluiting (gokverslaving en prestaties);
6. Gegevens die kunnen leiden tot identiteitsfraude zoals biometrische gegevens en/of identiteitsgegevens en kopieën van identiteitsbewijzen.

Afhankelijk van toegepaste technische en organisatorische beveiligingsmaatregelen dient een datalek niet gemeld te worden bij de AP.[5] Wanneer bijzondere persoonsgegevens in de verwerking voorkomen en deze wordt getroffen, dan is het beleid dat het datalek altijd wordt gemeld bij de AP.[6]

Voor een lijst met voorbeelden die niet gemeld hoeven te worden bij de AP:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2019_voorbeeldlijst_wel_niet_melden_datalek_def.pdf

Wanneer gebruik wordt gemaakt van eerder genoemde lijst, maak dan een screenshot van de lijst. Deze wordt toegevoegd aan de beoordeling. Op deze manier wordt aantoonbaar vastgelegd waarom er geen datalek bij de AP wordt gemeld.

[5] Overwegingen 87 en 88 AVG.

[6] Zie pagina26 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.

Factoren beoordeling risico's

Bij de beoordeling van de risico's dient rekening gehouden te worden met de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen. De risico's dienen bekeken te worden vanuit een objectieve beoordeling. Daarnaast dient vastgesteld te worden of er sprake is van een risico of een hoog risico.[7]

Als sprake is van een datalek waarbij in het verleden een DPIA is opgesteld, dan kan deze als hulpmiddel dienen om de risico's te bepalen. Het verwerkingenregister kan ook een hulpmiddel zijn om de risico's snel duidelijk te krijgen.

De beoordeling houdt rekening met de volgende criteria:[8]

De aard van de inbreuk

Het type inbreuk kan van invloed zijn op het risico voor de betrokkene(n). Een inbreuk op de vertrouwelijkheid heeft andere gevolgen dan het verloren en niet meer beschikbaar zijn van de persoonsgegevens.

De aard, gevoeligheid en omvang van de persoonsgegevens

Hoe gevoeliger de persoonsgegevens hoe groter het risico op de schade voor de betrokkene(n). Een aandachtspunt zijn de gegevens die bekend zijn. Door een combinatie van die gegevens kan de schade hoger of lager zijn.

Gemak waarmee betrokkenen kunnen worden geïdentificeerd

Identificatie kan direct of indirect mogelijk zijn op basis van de aantasting van integriteit en/of vertrouwelijkheid (gecompromitteerde gegevens), maar kan ook afhankelijk zijn van de specifieke context en de publieke beschikbaarheid van gerelateerde gegevens.

Ernst van gevolgen voor betrokkenen

Afhankelijk van de aard van de bij een inbreuk betrokken persoonsgegevens, kan de schade voor betrokkenen die daaruit kan voortvloeien zeer ernstig zijn. Dit geldt in het bijzonder als de inbreuk zou kunnen leiden tot identiteitsdiefstal of -fraude, lichamelijk letsel, psychisch leed, vernedering, reputatieschade en de persoonsgegevens van kwetsbare betrokkenen. In de beoordeling is het relevant te kijken naar de intenties van de inbreuk daarnaast kan de verwerkingsverantwoordelijke een mate van zekerheid hebben ten aanzien van de ontvanger, zodat hij redelijkerwijs kan

[7] Overwegingen 75 en 75 AVG.
[8] 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.

verwachten dat de partij de per vergissing verzonden gegevens niet leest of er geen toegang toe heeft, en dat de ontvanger de instructies volgt van de verwerkingsverantwoordelijke.

Bijzondere kenmerken van de betrokkene

Daarbij kan gedacht worden aan de kinderen en andere kwetsbare groepen. Deze lopen in zijn algemeenheid een verhoogd risico op vervelende gevolgen van een inbreuk.

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.

Het aantal getroffen betrokkenen

Over het algemeen kan een inbreuk grotere gevolgen hebben naarmate er meer betrokken bij betrokken zijn. Een inbreuk kan echter voor één betrokkene ernstige gevolgen hebben. Dit is afhankelijk van de aard van de persoonsgegevens en de context van de inbreuk en situatie.

BIJLAGE C MELDEN DATALEK BIJ DE AP

De [redacted] doet de melding bij de AP. Het formulier is beschikbaar op:
https://datalekken.autoriteitpersoonsgegevens.nl/

BIJLAGE D INFORMEREN VAN DE BETROKKENE

Het informeren van de betrokkene dient plaats te vinden:

*"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"*[9]

De afweging of er sprake is van een hoog risico voor de rechten en vrijheden van de betrokkene is afhankelijk van de omstandigheden van het geval. Daarbij wordt beoordeeld in hoeverre de betrokkene als gevolg van de inbreuk te maken kunnen krijgen met uitsluiting, schade aan gezondheid, financiële schade etc.

De betrokkene hoeft niet geïnformeerd te worden als: [10]

1. De persoonsgegevens versleuteld zijn of op een andere wijze onbegrijpelijk zijn gemaakt;
2. De verwerkingsverantwoordelijke [AP] achteraf maatregelen heeft genomen waardoor het hoge risico voor de rechten en vrijheden van de betrokkene zich waarschijnlijk niet meer zal voordoen,
3. Het een groot aantal betrokken gevallen betreft, waardoor de melding onevenredig veel moeite zou kosten en waarbij een openbare melding kan volstaan,
4. Melding afbreuk zou doen aan een zwaarwegend belang.

De betrokkene wordt geïnformeerd per brief. De inhoud van de berichtgeving is in lijn met de melding van de AP en bevat tenminste de volgende onderdelen:[11]

1. De situatieschets;
2. De mogelijke gevolgen voor de betrokkene;
3. De maatregelen om de schade voor de betrokkene te verkleinen;
4. De maatregelen die betrokkene zelf kan nemen;
5. Contactgegevens van de directeur en [redacted]
6. De mogelijkheid om een klacht in te dienen;
7. Of er wel/geen datalekmelding is gedaan bij de AP.

[9] Art. 34 AVG.
[10] Art. 41 UAVG.
[11] Art. 34 jo art. 33 AVG.

BIJLAGE E MODEL BRIEF AAN DE BETROKKENE

Naam betrokkene

Contact gegevens betrokkene

Den Haag, [datum]

Betreft: informatie over datalek bij de Autoriteit Persoonsgegevens

Geachte [naam betrokkene],

Met deze brief wil ik u informatie geven over een datalek bij de Autoriteit Persoonsgegevens. Daarbij zijn w persoonsgegevens betrokken. Dit kan nadelen hebben voor uw privéleven. Daarom sturen wij u deze brief. In deze brief leest u wat u kunt doen om de schade te beperken. Daarnaast bieden wij onze welgemeende excuses aan.

Wat is er gebeurd?
[omschrijving van het datalek].

[indien van toepassing] Het datalek kan nadelen hebben voor uw privéleven. Om dit te beperken raden wij u aan een aantal maatregelen te nemen. [aanbevolen maatregelen].

Met deze brief hoop ik u voldoende informatie te hebben gegeven over het datalek en de mogelijke gevolgen. *[indien van toepassing: Het datalek is tevens gemeld bij de Autoriteit Persoonsgegevens].* Wij werken steeds aan het verbeteren van de beveiliging. We onderzoeken samen met de [redacted] of onze werkwijze rond het verwerken van persoonsgegevens kan worden verbeterd om herhaling te voorkomen.

Vragen
Mogelijk heeft u nog vragen of wilt u in gesprek. Dat begrijpen wij goed. Neemt u daarover dan gerust contact met mij op. Mocht u na contact niet tevreden zijn over onze handelswijze. Dan kunt u altijd een klacht indienen bij de Autoriteit Persoonsgegevens.

Met vriendelijke groet,

[Naam directeur],
Directeur [afdeling + contactgegevens]

AUTORITEIT
PERSOONSGEGEVENS

Werkafspraken

Datum
3 november 2023

Van
[redacted]

Aan
[redacted]

Onderwerp
Werkafspraken bij het proces datalekken

1. Inleiding en aanleiding
Op 1 april 2023 is het nieuwe proces datalekken gestart. Ten behoeve van het nieuwe proces zijn het Stroomschema datalekken en de Toelichting bij stroomschema datalekken opgesteld. We zien aanleiding voor het maken van werkafspraken voor de uitvoering van het proces datalekken. De behoefte bestaat uit het concretiseren en vastleggen van werkafspraken die niet in het proces datalekken zijn omschreven, zodat het op een eenduidige manier wordt opgepakt en de rolverdeling tussen de taken van de [redacted] en de [redacted] wordt verduidelijkt. Verder is er behoefte aan duidelijkheid rondom het overdragen van taken tijdens verlof. De werkafspraken staan beschreven in dit document en worden ter kennisneming voorgelegd aan het [redacted] en de [redacted]

2. Werkafspraken
2.1 Beveiligingsincidenten
Het proces datalekken is van toepassing op alle beveiligingsincidenten waarbij persoonsgegevens zijn betrokken. De beveiligingsincidenten waarbij géén persoonsgegevens zijn betrokken of waarvan het nog onduidelijk is of er persoonsgegevens bij zijn betrokken worden in eerste instantie buiten dit proces om opgepakt door de [redacted]. De [redacted] heeft daarin geen rol. Als later blijkt dat er toch persoonsgegevens bij zijn betrokken betrekt de [redacted] de [redacted][1] Niet limitatieve voorbeelden van beveiligingsincidenten die éérst worden opgepakt door de [redacted] totdat blijkt dat er persoonsgegevens bij zijn betrokken zijn:

- Het kwijtraken, de diefstal of te laat inleveren van bedrijfsapparatuur (laptop, smartphone of tablet);
- Het kwijtraken van passen ([redacted]);
- ICT storingen (tijdelijk niet kunnen werken / verlopen certificaten);
- Phishing meldingen;
- Besmetting met schadelijke software of false positive meldingen daarvan [redacted];
- Een calamiteit zoals een brand of inbraak in het datacentrum;
- Aanval op de digitale infrastructuur.

[1] Zie ook paragraaf 2.3 van deze werkafspraken.

Datum
3 november 2023

2.2 Waarnemen tijdens afwezigheid [2]

In het proces datalekken staan afspraken over waarnemen bij afwezigheid, namelijk:

- Bij afwezigheid van de [redacted] is de [redacted] waarnemer.
- Bij afwezigheid van de [redacted] is de [redacted] waarnemer.

Deze afspraken blijven geldig, maar behoeven concretisering.

Het waarnemen behelst het overnemen van alle taken die op naam staan van de [redacted] en/of [redacted] zoals omschreven in het proces datalekken en in dit document met werkafspraken.

Waarneming vindt in ieder geval plaats op de vaste onderstaande momenten:

Functie	Afwezig op	Waarnemer
[redacted]	Woensdag	Tot 12:00 uur [redacted], vanaf 12:00 uur [redacted]
[redacted]	Maandag tot 9:30-13:30 uur, woensdag vanaf 12:00 uur	[redacted]

Bij afwezigheid anders dan het bovenstaande vindt door de afwezige ruim van te voren afstemming plaats met de [redacted], [redacted] en [redacted] De [redacted] en [redacted] zijn zo min mogelijk tegelijk afwezig. En de [redacted] en [redacted] zijn zo min mogelijk tegelijk afwezig. Als de [redacted] en de [redacted] tegelijk afwezig zijn, neemt de [redacted] beiden waar. Als de [redacted] en de [redacted] tegelijk afwezig zijn, maken de [redacted] en de [redacted] vooraf samen afspraken. Bij korte afwezigheid gaat het om een bereikbaarheidsafspraak: de [redacted] of de [redacted] zijn afwezig, maar een van hen is wel bereikbaar en beschikbaar om datalekken op te pakken. Bij langere afwezigheid wordt per keer vooraf bepaalt wie hen vervangt. Bij afwezigheid van de [redacted] van langer dan twee dagen[3] wijst de [redacted] een [redacted] aan waar de [redacted] en/of de [redacted] mee kan overleggen inzake de risicoafweging (wel/niet melden bij de AP en/of de betrokkene). De [redacted] vervangt de [redacted] niet, maar kan worden ingeschakeld als klankbord. De stappen in het proces datalekken worden dus niet door de [redacted] maar door de [redacted] en/of de [redacted] zelf uitgevoerd. In het geval van ongeplande afwezigheid (ziekte) meldt de afwezige dit bij zijn/haar leidinggevende en de [redacted] zodat de aanwezigen in overleg met de leidinggevende vervanging bepalen.

Vóór en ná de afwezigheid vindt in het geval van lopende datalekken door de afwezige een overdracht plaats.[4] Verder worden de actiehouders in [redacted] door de afwezige omgezet naar de waarnemer. De informatie op Plein wordt niet aangepast. Wel verandert de afwezige zijn/haar voicemailbericht + afwezigheidsassistent (zowel voor internen als externen) waarbij wordt aangegeven met wie er contact kan worden opgenomen inclusief het telefoonnummer van diegene.

2.3 Onderzoeken van de root cause[5]

Op dit moment is het onderzoeken van de root cause van datalekken niet opgenomen als stap in de beoordeling. Daardoor vindt er te snel een beoordeling van het datalek plaats terwijl het onderzoek naar de root cause minimaal is. Om passende mitigerende maatregelen te bedenken die getroffen moeten worden na een datalek én om de risicobeoordeling te kunnen maken is het gebruikelijk om de root cause te

[2] Toevoeging aan Stap 1 van het proces datalekken.
[3] I.v.m. meldplicht bij de AP binnen 72 uur.
[4] Op dit moment gebeurt dat tijdens het wekelijks overleg op dinsdag en het bijpraat moment op donderdag.
[5] Toevoeging aan het begin van Stap 2 van het proces datalekken.

achterhalen. Hierbij werken we volgens het BOB-model. De eerste fase is Beeldvorming.[6] Na een grondige beeldvorming volgt de fase van Oordeelsvorming.[7] De laatste fase is de Besluitvorming.[8] Ten behoeve van de eerste fase Beeldvorming wordt aan het proces een nieuwe actie toegevoegd: na het ontvangen van een melding neemt de [redacted] contact op met degene die het datalek heeft gemeld om de root cause te achterhalen. Als de informatie van de melder onvoldoende is om de root cause te achterhalen en daar technische hulp voor nodig is, schakelt de [redacted] relevante partijen in, zoals het cluster Informatievoorziening of J&V. De [redacted] beschrijft naast de root cause de omschrijving van het datalek. Als de [redacted] aanvullende informatie nodig heeft voor de beoordeling – met name over de categorieën persoonsgegevens en betrokkenen – neemt de [redacted] ook contact op met de melder. De beeldvorming van het datalek vindt dus eerst plaats vanuit de [redacted] en wordt later aangevuld door de [redacted] Ook kunnen bewijsstukken worden opgevraagd (denk aan een brief die verkeerd is verstuurd).

In de praktijk wordt Bijlage A niet ingevuld bij ieder datalek, maar wordt gebruik gemaakt van een standaardmail waarin de elementen uit Bijlage A terugkomen. In de toekomst gebeurt dit in [redacted]. De [redacted] en [redacted] zijn bezig met het inregelen daarvan.

2.4 Beoordeling van het datalek[9]

2.4.1 Bedenken en bewaken van de maatregelen

De beoordeling of het datalek gemeld moet worden aan de AP en/of de betrokkene wordt gedaan door de [redacted] waarbij de [redacted] ondersteunt bijvoorbeeld als het gaat om het inschatten van de kans.
De [redacted] zet directe maatregelen uit om de inbreuk te stoppen en stelt maatregelen op om soortgelijke datalekken in de toekomst te voorkomen en wijst daarbij een actiehouder aan. De [redacted] beoordeelt of getroffen/bedachte[10] maatregelen voldoende/treffend zijn om de inbreuk aan te pakken. De [redacted] bewaakt of alle maatregelen worden getroffen en houdt dat bij in het datalekregister.[11] Verder ondersteunt de [redacted] de [redacted] bij het omschrijven van de maatregelen in het geval van communicatie en bij een melding bij de AP.[12]

2.4.2 Beoordeling van de impact op de organisatie

Bij de beoordeling van het datalek wordt op dit moment met name impact van het datalek op betrokkenen meegenomen. De impact van het datalek op de organisatie zelf ontbreekt in het proces datalekken. In de beoordeling van het datalek neemt de [redacted] mee in hoeverre er bedrijfsgevoelige en/of toezichtsvertrouwelijke informatie bij betrokken is en wat het risico daarvan is (bijvoorbeeld reputatieschade, vroegtijdig naar buiten komen van een onderzoek of inzicht in zwakheden).

2.5 Meenemen van het afdelingshoofd bij informeren directeur[13]

---

[6] Zie Stap 2 van het proces datalekken en paragraaf 2.3 van deze werkafspraken.
[7] Zie Stap 3, Stap 5 en Stap 9 van het proces datalekken en paragraaf 2.4 van deze werkafspraken.
[8] Zie Stap 7 van het proces datalekken.
[9] Toevoeging aan Stap 3, Stap 5 en Stap 9 van het proces datalekken.
[10] In de praktijk bedenken melders / verwerkers zelf ook maatregelen. Daarnaast kan in het proces datalekken de directeur/[redacted] ook stappen bedenken om risico's te mitigeren en een nieuw datalek te voorkomen, zie stap 7.
[11] Toevoeging aan Stap 10 van het proces datalekken.
[12] Toevoeging aan Stap 7 en 8 van het proces datalekken.
[13] Toevoeging aan Stap 3 van het proces datalekken.

Datum
3 november 2023

In het DB is verzocht om de afdelingshoofden meer te betrekken bij datalekken. Met de [redacted] is besproken dat de [redacted] daarom afdelingshoofden in cc meeneemt bij het informeren van de directeuren.

2.6 Evaluatie van datalekken[14]

Onderdeel van het proces datalekken is dat een datalek altijd wordt geëvalueerd met de [redacted] en desbetreffende directeur. Om dit efficiënter en minder tijdsintensief te laten doen verlopen heeft een concretisering op het proces plaatsgevonden. De directeur nodigt na iedere kwartaal de [redacted] uit voor een evaluatie van alle beveiligingsincidenten/datalekken die het afgelopen kwartaal hebben plaatsgevonden binnen de directie met als doel het evalueren van het proces en de genomen maatregelen. Uitzondering hierop zijn de risicovolle datalekken die bij de AP en/of de betrokkenen worden gemeld. Daarvoor geldt dat een evaluatie plaatsvindt binnen twee weken na het ontdekken van het datalek (conform het huidige proces). Deze concretisering is goedgekeurd in het DB van 3 juli 2023. De [redacted] stuurt voorafgaand aan de evaluatie een overzicht van datalekken (afgestemd met de [redacted]) naar de directeur.

3. Bekendmaken van het proces datalekken

Het nieuwe proces datalekken is binnen de organisatie bekend gemaakt in de AP Talk van 20 april 2023 en via Plein. Daarnaast gaan de [redacted] en de [redacted] langs bij alle afdelingen om op een interactieve manier toelichting te geven op het proces datalekken. Het doel is om dat in 2023 af te ronden.

4. Actualiseren van het proces datalekken

In het proces datalekken is opgenomen dat de [redacted] zorgdraagt voor het actualiseren van het document. De [redacted] controleert jaarlijks of het document herzien dient te worden. Dit staat op de planning voor Q2 2024. Daarbij zullen de bovenstaande werkafspraken, het inzetten van [redacted] voor datalekken en de aandachtspunten van het afgelopen jaar worden meegenomen. Aandachtspunten die het afgelopen halfjaar al zijn geconstateerd door de [redacted] zijn:

- Het ontwikkelen van een visie inzake transparantie: volgt de AP strikt de AVG en/of richtlijn AP en/of richtlijn EDPB met betrekking tot het melden aan de AP en het informeren van betrokkenen? Of is de AP strenger (*zie bijv. het proces datalekken waarin staat dat wanneer bijzondere persoonsgegevens in de verwerking voorkomen en deze worden getroffen, dan is het beleid dat het datalek altijd wordt gemeld bij de AP.*)? De AP wil namelijk steeds meer transparant zijn/worden. Waarom vinden we het dan zo spannend om betrokkenen in te lichten die onderdeel waren van het datalek? Daarbij ook de vraag welke betrokkenen worden er allemaal ingelicht?
- Aan wie (IV Beraad, DB, BO, directeuren, [redacted]) en op welke manier willen we rapporteren over datalekken binnen de organisatie?
- Hoe kunnen we alle medewerkers bij de AP meenemen in het leren van datalekken? Met andere woorden: hoe kunnen we in de toekomst wel intern gaan communiceren over datalekken die er hebben plaatsgevonden? Bijvoorbeeld per kwartaal een korte nieuwsflits van soorten datalekken en mitigerende maatregelen? Dit om de awareness bij medewerkers te verhogen.
- We gaan af op informatie die de melder geeft. In hoeverre willen we de stukken die zijn gelekt controleren? Afhankelijk van hoe vaak het voorkomt zullen we daar iets over vastleggen of bepalen we per situatie.

[14] Toevoeging aan Stap 11 van het proces datalekken.

- Bepalen wie verantwoordelijk is voor het nemen van mitigerende maatregelen en dit vastleggen in het proces. In de RASCI, die is goedgekeurd door de stuurgroep van het project AVG-proof en het BO, staat dat dit de dossiereigenaar/lijnmanagement is.
- Hoe vindt de risicoinschatting van een datalek plaats? Is er naast impact voldoende rekening gehouden met de kans?