

PROTOCOL MELDPLICHT DATALEKKEN

Provincie Limburg



INHOUDSOPGAVE PROTOCOL MELDPLICHT DATALEKKEN

1.	Inleiding	3
2.	Worden er persoonsgegevens verwerkt waarvoor de Provincie verantwoordelijk is?	3
3.	Is er sprake van een datalek?	5
4.	Moet dit datalek worden gemeld aan de AP?	7
5.	Wanneer en hoe moet het datalek worden gemeld aan de AP?	8
6.	In welke gevallen dient het datalek te worden gemeld aan de betrokkene?	9
7.	Wat moet worden meegedeeld aan betrokkene?	12
8.	Wanneer moet het datalek worden gemeld aan de betrokkene?	12
9.	Welke gegevens over een datalek moeten worden vastgelegd in...?	13
10.	Interne processen bij een datalek	15
11.	SE rekenmethode	15

Revisietabel	
Versie 1.0	12 november 2019
Versie 1.1	27 november 2019
Versie 1.2	18 december 2019
Versie 1.3	21 januari 2020
Versie 2.0	27 februari 2024

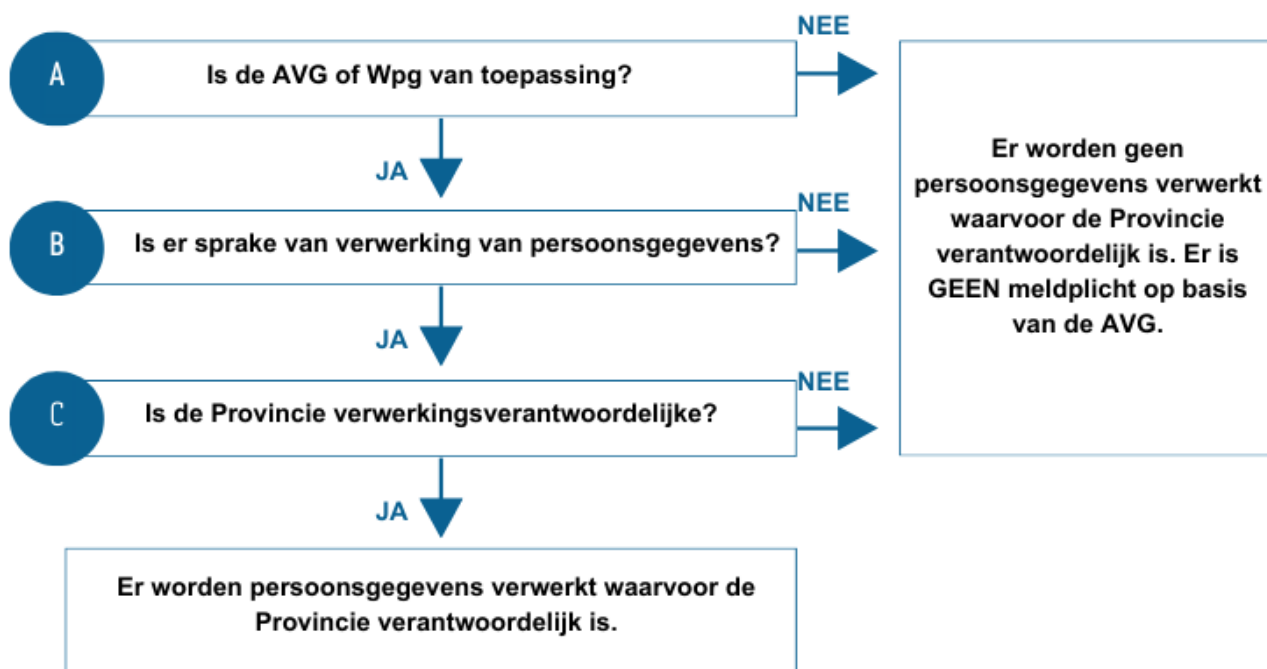
1. Inleiding

In de Algemene verordening gegevensbescherming (hierna: 'AVG') is een meldplicht opgenomen voor *inbreuken in verband met persoonsgegevens* (hierna: 'datalek'). Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) in bepaalde gevallen een melding moeten doen bij de Autoriteit Persoonsgegevens (hierna: 'AP') zodra zij een datalek hebben. In een aantal van deze gevallen moet het datalek ook medegedeeld worden aan de betrokkenen (de personen van wie de persoonsgegevens zijn gelekt).

Op grond van de Wet Politiegegevens (hierna: 'Wpg') geldt dezelfde meldingsplicht voor inbreuken in verband met politiegegevens.

Bij de beslissing of de Provincie Limburg (hierna: 'de Provincie')¹ een gebeurtenis die zich heeft voorgedaan moet melden aan de AP, en eventueel daarnaast ook aan de betrokkene(n), moeten een aantal afwegingen worden gemaakt. Dit protocol is gebaseerd op de *Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679(WP250 rev.01)* en de Wpg en helpt de provinciale medewerkers bij het maken van deze afwegingen.

2. Worden er persoonsgegevens verwerkt waarvoor de Provincie verantwoordelijk is?



¹ Waar de Provincie genoemd wordt, worden de volgende organen van de Provincie Limburg aangeduid: de Commissaris van de Koning en zijn kabinet, het college van Gedeputeerde Staten en Provinciale Staten.

A. Is de AVG of Wpg van toepassing?

AVG

De meldplicht van een datalek aan de AP ontstaat slechts, indien er sprake is van een inbreuk op de verwerking van persoonsgegevens als bedoeld in de AVG. Artikel 2 AVG stelt dat de AVG van toepassing is als er sprake is van (1) een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens of (2) een verwerking van persoonsgegevens die in een bestand zijn opgenomen of daarin opgenomen zullen worden. De AVG is niet van toepassing als de verwerking van persoonsgegevens uitsluitend persoonlijke of huishoudelijke doeleinden dient of als deze plaatsvindt in het kader van het onderzoek van strafbare feiten of de bescherming van de openbare veiligheid. Een voorbeeld van een verwerking die op de Provincie zou kunnen plaatsvinden, maar die slechts de huishoudelijke sfeer betreft is het printen van de adreslijst voor je kerstkaarten of het privé bijhouden van een lijst van oud-collega's. Meestal is de AVG echter van toepassing.

Wpg

De meldplicht van een datalek aan de AP ontstaat slechts, indien er sprake is van een inbreuk op de verwerking van politiegegevens als bedoeld in de Wpg. Artikel 2 Wpg stelt dat de Wpg van toepassing is op de verwerking van politiegegevens die door een bevoegde autoriteit in een bestand zijn opgenomen of bestemd zijn daarin te worden opgenomen. De Wpg is niet van toepassing op de verwerking van politiegegevens (1) ten behoeve van activiteiten met uitsluitend persoonlijke doeleinden of (2) ten behoeve van de interne bedrijfsvoering.

B. Is er sprake van een verwerking van persoonsgegevens?

Indien er geen sprake is van verwerking van persoonsgegevens of politiegegevens, dan kan er ook geen sprake zijn van een inbreuk op de verwerking van persoonsgegevens en is er dus ook geen datalek. Let op! Er is dan waarschijnlijk wel sprake van een beveiligingsincident dat via de Helpdesk moet worden opgenomen in het incidentenregister.

Verwerking van persoonsgegevens of politiegegevens betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens (artikel 4 sub 2 AVG of artikel 1 sub c Wpg). Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Een verwerking kan ook geheel geautomatiseerd verlopen.

Een **persoonsgegeven** is elk gegeven betreffende een geïdentificeerde of identificeerbaar natuurlijk persoon (artikel 4 sub 1 AVG). Een rechtspersoon is identificeerbaar als zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Er is al snel sprake van identificeerbaarheid. Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten (**anonymisering**). Het verwijderen van de direct identificerende persoonsgegevens biedt op zichzelf niet altijd voldoende garantie dat er geen sprake meer is van persoonsgegevens. Door middel van spontane herkenning, vergelijking van (persoons)gegevens en/of koppeling aan (persoons)gegevens uit een andere bron, kan immers identificatie tot stand worden gebracht. Verder moet bij anonimisering rekening worden gehouden met de stand van de techniek. Wat bij een bepaalde stand van de techniek als anoniem kan worden beschouwd, aangezien het gegeven niet redelijkerwijs tot een persoon te herleiden is, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding. Een andere techniek is **pseudonimisering** (artikel 4 sub 5 AVG). Dit houdt in dat persoonsgegevens op een dusdanige wijze worden verwerkt dat zij niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er gebruik wordt gemaakt van aanvullende gegevens. Let ook hier weer op de kans dat men persoonsgegevens kunnen vergelijken

en/of koppelen waardoor een betrokkene geïdentificeerd zou kunnen worden.

Een **politiegegeven** is elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaken, bedoeld in de artikelen 3 en 4 van de Politiewet 2022, met uitzondering van (1) de uitvoering van wettelijke voorschriften anders dan de Wet administratiefrechtelijke handhaving verkeersvoorschriften of (2) de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 1, eerste lid, onderdeel i, onder 1° en artikel 4, eerste lid, onderdeel f, van de Politiewet 2012.

C. Is de Provincie de verwerkingsverantwoordelijke?

De meldplicht van een datalek is gericht de verantwoordelijke voor de verwerking van persoonsgegevens of politiegegevens. Bij de Provincie Limburg is dat meestal het college van Gedeputeerde Staten.

De **verwerkingsverantwoordelijke** is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 sub 7 AVG). Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking van persoonsgegevens er plaatsvindt en waarom. Ook is van belang wie er beslist over de middelen voor die verwerking; op welke manier zal de gegevensverwerking plaatsvinden? Deze bevoegdheden worden soms door verschillende mensen uitgeoefend. In dat geval is er sprake van gezamenlijke verantwoordelijkheid (artikel 26 AVG).

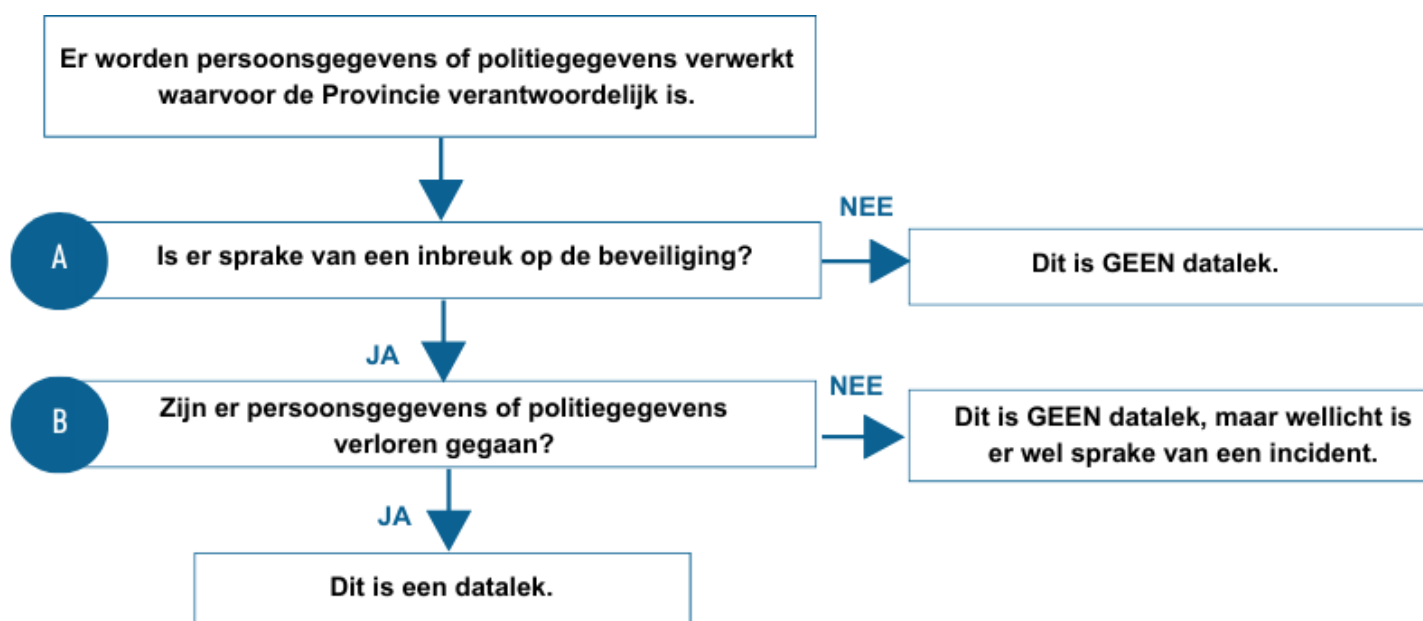
De werkgever van de buitengewoon opsporingsambtenaar (hierna: 'boa') is de verwerkingsverantwoordelijke van de persoonsgegevens die door de boa worden verwerkt, ook als dit politiegegevens zijn. Dit is bepaald in artikel 1, aanhef en onder c van het Besluit politiegegevens buitengewoon opsporingsambtenaren.

Verwerker is degene die ten behoeve van de verwerkingsverantwoordelijke de persoonsgegevens verwerkt (artikel 4 sub 8 AVG of artikel 1 sub 1 Wpg). Deze heeft op grond van artikel 33 lid 2 AVG of artikel 6c, vijfde lid Wpg een meldingsplicht van een datalek aan de verwerkingsverantwoordelijke. De verwerker moet een datalek dus zo snel mogelijk melden aan de verwerkingsverantwoordelijke.

3. Is er sprake van een datalek?

Een “**inbreuk in verband met persoonsgegevens**”, beter bekend als een **datalek** is in artikel 4 lid 12 AVG gedefinieerd als ‘*een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens*’. In artikel 1 sub q Wpg is een datalek gedefinieerd als ‘*een inbreuk op de beveiliging met de vernietiging, het verlies, de wijziging, de bekendmaking of de ter beschikkingstelling van of de geoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte politiegegevens tot gevolg*’. De definities uit de AVG en Wpg komen nagenoeg overeen. Om na te gaan of er sprake is van een datalek zijn er dus drie vragen die gesteld moeten worden:

- A. Is er sprake van een inbreuk op de beveiliging?
- B. Zijn er als gevolg van deze inbreuk persoonsgegevens of politiegegevens verloren gegaan?
- C. Kan worden uitgesloten dat persoonsgegevens of politiegegevens onrechtmatig zijn verwerkt?



A. Is er sprake van een inbreuk op de beveiliging?

Het is voor de kwalificatie ‘inbreuk in verband met persoonsgegevens’ niet relevant dat er opzet in het spel is. Een datalek houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. De aard van het beveiligingsincident is niet relevant voor de vraag of er al dan niet sprake is van een datalek. Een “inbreuk op de beveiliging van persoonsgegevens of politiegegevens” moet ruim worden geduid. Het is niet van belang of we passende technische of organisatorische maatregelen hebben getroffen of niet. Een datalek kan zich in beide situaties voordoen.

Belangrijk bij een datalek is dat het daadwerkelijk gebeurd moet zijn. 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 eventuele preventieve maatregelen waren niet toereikend om dit te voorkomen.

Voorbeelden van beveiligingsincidenten waar sprake kan zijn van een inbreuk op de beveiliging van persoonsgegevens zijn:

- een kwijtgeraakte/gestolen telefoon, laptop, USB-stick;
- een verkeerd verstuurd email;

- een poststuk geopend retour ontvangen;
- een inbraak door een hacker;
- per ongeluk persoonsgegevens of politiegegevens publiceren.

B. Zijn er persoonsgegevens of politiegegevens verloren gegaan?

Een tweede kenmerk van een datalek is dat er daadwerkelijk gevolgen zijn voor de persoonsgegevens of politiegegevens die de Provincie verwerkt. Dit kan enerzijds zijn dat er persoonsgegevens of politiegegevens verloren zijn gegaan of anderzijds dat het niet kan worden uitgesloten dat persoonsgegevens of politiegegevens onrechtmatig zijn verwerkt.

Verlies houdt in dat de Provincie de persoonsgegevens of politiegegevens niet meer heeft. Dit is ook het geval bij een tijdelijk verlies. Als bij een beveiligingsincident persoonsgegevens of politiegegevens verloren zijn gegaan als gevolg van een calamiteit en de meest recente reservekopie niet beschikbaar is, is er ook sprake van een datalek.

C. Kan worden uitgesloten dat persoonsgegevens of politiegegevens onrechtmatig verwerkt zijn?

Onder onrechtmatige vormen van verwerking vallen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging of ongeoorloofde verstrekking daarvan (zie de definitie van artikel 4 sub 12 AVG). Onder onrechtmatige vormen van verwerking van politiegegevens valt hetzelfde. Als de Provincie niet kan uitsluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet de inbreuk worden gekwalificeerd als een datalek.

Bij een malware-besmetting moeten we ervan uitgaan dat er sprake kan zijn van een datalek. Bepaalde typen malware doorzoeken de besmette apparatuur op waardevolle persoonsgegevens of politiegegevens, om deze vervolgens weg te sluizen naar een server die in handen is van de aanvaller. Een dergelijke malware-besmetting stelt de getroffen persoonsgegevens of politiegegevens dus bloot aan onbevoegde kennisname en andere vormen van onrechtmatige verwerking. Andere typen malware maken bestanden ontoegankelijk voor de rechtmatige eigenaar door ze te blokkeren ('ransomware') of te versleutelen ('cryptoware'). Door deze vormen van malware worden de getroffen persoonsgegevens of politiegegevens dus blootgesteld aan onbevoegde aantasting of wijziging.

Voorbeeld wel/geen datalek (onrechtmatige verwerking van persoonsgegevens)

Een medewerker geeft aan een derde de gebruikersnaam en het wachtwoord die toegang geven tot de personeelsadministratie van de Provincie. Na ontdekking van het gebeurde [REDACTED] zodat de derde geen toegang meer heeft tot de personeelsadministratie.

Daarna onderzoekt O&I of de derde daadwerkelijk toegang heeft gezocht tot de persoonsgegevens.

Als op basis van de logbestanden nagenoeg kan worden uitgesloten dat er door middel van het betreffende account toegang is verkregen tot de personeelsadministratie dan is er uitsluitend sprake van een beveiligingslek en niet van een datalek.

4. Moet dit datalek worden gemeld aan de AP?



Houdt dit datalek een risico in voor de rechten en vrijheden van natuurlijke personen?

In artikel 33 lid 1 AVG en artikel 33a lid 1 Wpg wordt gesteld dat een inbreuk in verband met persoonsgegevens of politiegegevens, een datalek, moet worden gemeld, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Een voorbeeld van een risico voor de rechten en vrijheden van natuurlijke persoon is als een ziekenhuis tijdelijk niet bij de medische dossiers van patiënten kan komen, waardoor behandelingen stil komen te liggen.

In de *Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679* wordt gesteld dat bij de beoordeling van de risico's in het algemeen rekening gehouden moet worden met zowel de waarschijnlijkheid als de ernst van het risico voor de rechten en vrijheden van betrokkenen. In de richtsnoer wordt vermeld dat de focus bij het bepalen van de risico's na een inbreuk ligt op de risico's die voortvloeien uit het effect van de inbreuk. Er moet dan rekening worden gehouden met de specifieke omstandigheden van de inbreuk, inclusief de ernst van het mogelijke effect en de waarschijnlijkheid dat dit gaat gebeuren. De EDPB formuleert daarom 8 criteria waar op gelet moet worden bij de vaststelling van de risico's voor de rechten en vrijheden van natuurlijke personen na een datalek:

1. De aard van de inbreuk; is informatie verloren gegaan of is deze verspreid?
2. De aard, gevoeligheid en omvang van de persoonsgegevens; hierbij moet men ook rekening houden met de personen die toegang hebben gekregen tot de persoonsgegevens en wat de waarde voor hen kan zijn.
3. Het gemak waarmee personen kunnen worden geïdentificeerd; hierbij is ook van belang of de gegevens versleuteld waren en of er gebruik is gemaakt van pseudonimisering.

4. De ernst van de gevolgen voor personen; fysiek of psychisch leed of materiële of immateriële schade.
5. Bijzondere kenmerken van de persoon; als de persoonsgegevens van een kwetsbare groep aangetast worden is het risico groter.
6. Bijzondere kenmerken van de verwerkingsverantwoordelijke; de rol van de verwerkingsverantwoordelijke en zijn (vertrouwens)positie kan van invloed zijn op het risico.
7. Het aantal getroffen personen
8. Algemene punten; bij alle punten moet rekening worden gehouden met de waarschijnlijkheid dat het plaats gaat vinden.

Daarnaast verwijst de EDPB ook naar de '*Recommendations for a methodology of the assessment of severity of personal data breaches*'. Deze zijn opgesteld door de ENISA (Europese Unie voor netwerk- en informatiebeveiliging) en bevat aanbevelingen om de ernst van een datalek te beoordelen. De methode om de SE score vast te stellen, is in paragraaf 11 opgenomen.

SE < 2	Laag
2 ≤ SE < 3	Medium
3 ≤ SE < 4	Hoog Melden AP
SE ≥ 4	Erg hoog Melden Betrokkenen

Indien de hierin vervatte methode leidt tot een score hoger dan 3 wordt het datalek gemeld aan de AP. Voor de Wpg wordt hierbij aangesloten.

5. Wanneer en hoe moet het datalek worden gemeld aan de AP?

De verwerkingsverantwoordelijke moet binnen 72 uur nadat hij op de hoogte is van een datalek een melding maken bij de AP (artikel 33 lid 1 AVG en artikel 33a lid 1). De verwerkingsverantwoordelijke wordt geacht op de hoogte te zijn van een datalek als er een redelijke mate van zekerheid bestaat over het plaatsvinden van een veiligheidsincident dat tot de compromittering van persoonsgegevens heeft geleid. Indien de Provincie het incident later dan 72 uur na ontdekking aan de AP meldt, moet de vertraging gemotiveerd worden (artikel 33 lid 1 AVG en artikel 33a lid 1 Wpg).

Als men 72 uur na het ontdekken van het datalek nog geen volledig overzicht heeft van wat er gebeurd is, moet een melding worden gemaakt van hetgeen wel al bekend is. Deze melding moet zodra er meer duidelijkheid is worden aangevuld (artikel 33 lid 4 AVG en artikel 33 lid 3 Wpg).

Een melding van een datalek moet op zijn minst de volgende onderdelen bevatten (artikel 33 lid 3 AVG en artikel 33a lid 2 Wpg):

- a. De aard van de inbreuk in verband met de persoonsgegevens;
- b. De naam en contactgegevens van de functionaris gegevensbescherming of een ander contactpunt;
- c. De waarschijnlijke gevolgen van het datalek;
- d. De maatregelen die zijn voorgesteld/genomen om het datalek aan te pakken of de schade te beperken.

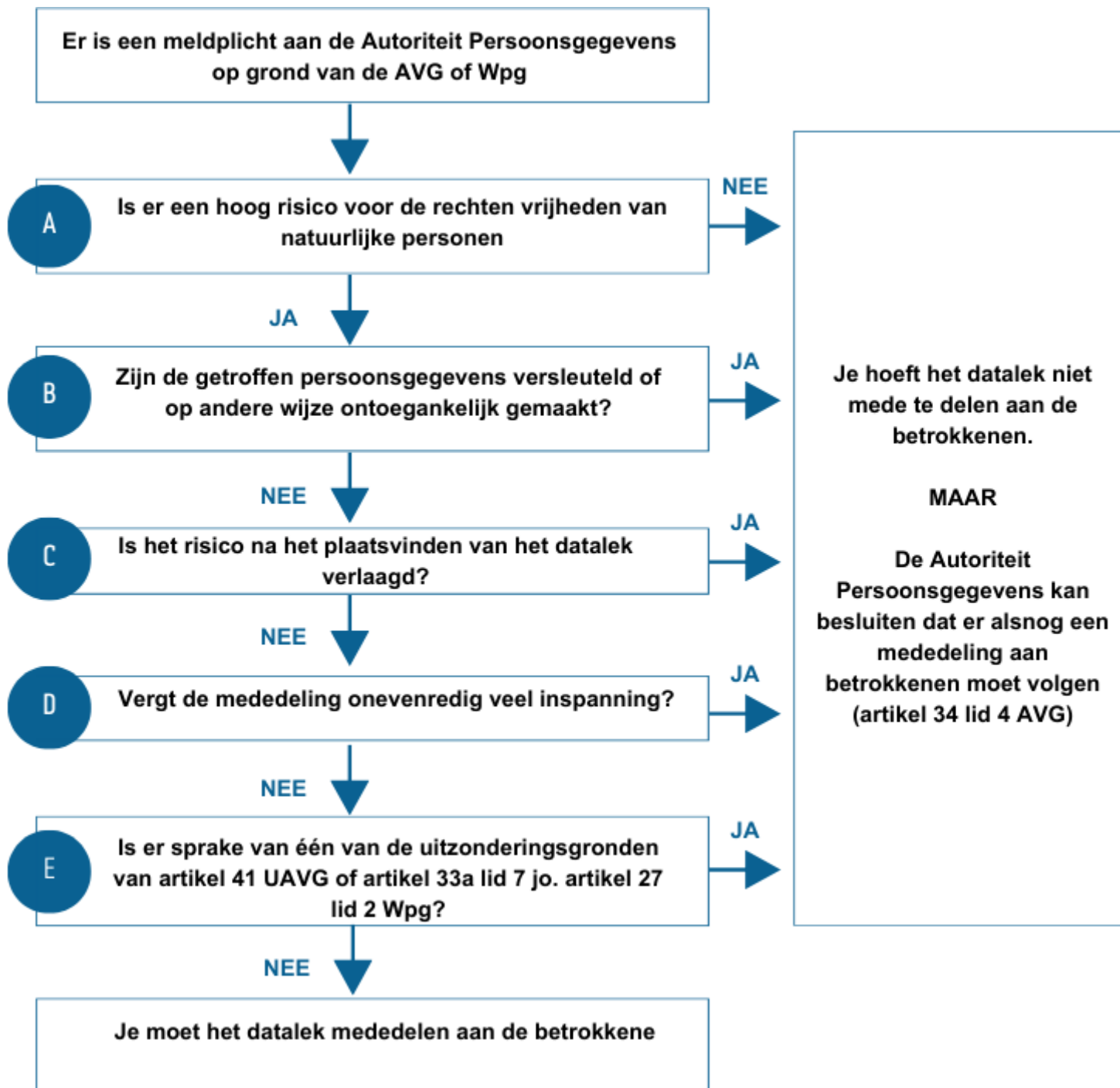
Meldingen van een datalek aan de AP door de Provincie worden door de privacy officer gedaan. Deze raadpleegt allereerst de functionaris gegevensbescherming en besluit tot melding in overleg met de CISO na besluitvorming door de algemeen directeur/provinciesecretaris.

6. Moet ik het datalek meedelen aan de betrokkene?

Als er een datalek is vastgesteld dat op grond van artikel 33 AVG of 33a Wpg gemeld moet worden aan de AP, dan is de volgende vraag of dit datalek ook medegedeeld moet worden aan de betrokkene. Artikel 34 lid 1 AVG of artikel 33a lid 5 Wpg stelt dat een datalek medegedeeld moet worden aan de betrokkenen als er waarschijnlijk een hoog risico is voor de rechten en vrijheden van natuurlijke personen. Er zijn drie uitzonderingsgevallen waarbij een datalek niet medegedeeld hoeft te worden aan een betrokkene ondanks een hoog risico voor de rechten en vrijheden van natuurlijke personen. In artikel 34 lid 3 AVG en artikel 33a lid 6 Wpg staan een drietal uitzonderingen:

- a. Als er passende technische en organisatorische maatregelen zijn getroffen om de persoonsgegevens waarop het datalek betrekking heeft onbegrijpelijk te maken;
- b. Als er achteraf maatregelen zijn getroffen om te voorkomen dat het risico voor de rechten en vrijheden zich niet al voltrekken;
- c. Als de mededeling onevenredige inspanning vraagt.

Daarnaast bevatten artikel 41 Uitvoeringswet AVG en artikel 33a lid 7 jo. artikel 27 lid 2 Wpg ook een aantal uitzonderingen, die later worden vermeld.



A. Is er een hoog risico voor de rechten en vrijheden van natuurlijke personen?

Het datalek moet aan de betrokkene worden gemeld indien de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 34 lid 1 AVG of artikel 33a lid 5 Wpg). De eis voor een mededeling aan de betrokkene is strenger dan de eis voor een melding aan AP, maar ook voor het bepalen van dit risico kan gebruik worden gemaakt van de 8 criteria van de EDPB en van de SE scores.

Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens of politiegegevens in hun belangen worden geschaad. De schade kan van materiële of immateriële aard zijn. Bij dit laatste kan bijvoorbeeld worden gedacht aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie. Identiteitsfraude kan overigens niet alleen leiden tot immateriële gevolgen, maar ook tot materiële gevolgen.

Indien er persoonsgegevens van gevoelige aard, zoals medische gegevens of gegevens omtrent religie of seksualiteit, zijn gelekt, moet er vanuit worden gegaan dat het datalek niet alleen moet worden gemeld aan de AP, maar ook aan de betrokkene. Verlies of onrechtmatige verwerking van dergelijke gegevens kunnen onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of (identiteits-)fraude.

Het informeren van de betrokkene over een opgetreden datalek is met name noodzakelijk in situaties waarin er voor hem of haar daadwerkelijk ongunstige gevolgen voor de persoonlijke levenssfeer te verwachten zijn. Door de kennisgeving is de betrokkene alert op de mogelijke gevolgen van het datalek en kan hij of zij zich, voor zover dat mogelijk is, daartegen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen (zoals vervanging van een wachtwoord).

i. Zijn de getroffen persoonsgegevens of politiegegevens versleuteld of op andere wijze ontoegankelijk gemaakt?

De regel is dat bij een hoog risico voor de rechten en veiligheid van natuurlijke personen, het datalek medegedeeld moet worden aan de betrokkene (artikel 34 lid 1 AVG en artikel 33a lid 5 Wpg). De eerste uitzondering op deze mededelingsplicht is als de verwerkingsverantwoordelijke vooraf beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens of politiegegevens versleuteld of op een andere manier ontoegankelijk zijn (artikel 34 lid 3 sub a AVG of artikel 33a lid 6 sub a Wpg).

Persoonsgegevens of politiegegevens die adequaat zijn versleuteld kunnen bij een datalek nog steeds worden vernietigd en ook aantasting of onbevoegde wijziging is nog steeds mogelijk (bijvoorbeeld door zogenoemde 'cryptoware', die de reeds versleutelde gegevens nogmaals versleutelt met een sleutel die de verantwoordelijke uitsluitend tegen betaling in zijn bezit kan krijgen). Voor beantwoording van de vraag of de toegepaste cryptografie voldoende bescherming biedt om de mededeling aan de betrokkene achterwege te laten, dient contact opgenomen te worden met de specialisten binnen het cluster O&I.

ii. Is het risico na het plaatsvinden van het datalek verlaagd?

De tweede uitzondering is neergelegd in artikel 34 lid 3 sub b AVG en artikel 33a lid 6 sub b Wpg en ziet op situaties waarin de kans op realisatie van de geïdentificeerde risico's na een datalek verkleind is. Een voorbeeld hier van is het op afstand wissen van de persoonsgegevens die op een apparaat staan (*remote wiping*). Door de persoonsgegevens of politiegegevens te wissen worden deze ontoegankelijk voor onbevoegden. Door een tijdige en geslaagde *remote wipe* heeft een eventuele aanvaller nog wel de beschikking over het apparaat waarop de persoonsgegevens of politiegegevens stonden, maar niet meer over de persoonsgegevens of politiegegevens zelf. De kans op verwezenlijking van de risico's voor de rechten en vrijheden van natuurlijke personen zijn hierdoor verkleind, waardoor een mededeling van het datalek aan de betrokkene niet meer nodig is.

iii. Vergt de mededeling onevenredig veel inspanning?

De derde uitzondering van artikel 34 lid 3 AVG en artikel 33a lid 6 sub c Wpg houdt in dat als de mededeling aan de betrokkene onevenredig veel inspanning zou vergen, deze achterwege mag blijven. In plaats van een persoonlijke mededeling van het datalek, dient er een openbare mededeling van het datalek plaats te vinden (artikel 34 lid 3 sub c AVG en artikel 33a lid 6 sub c Wpg).

iv. Is een van de uitzonderingsgronden van artikel 41 Uitvoeringswet AVG of artikel 33a lid 7 jo. artikel 27 lid 2 Wpg van toepassing?

Artikel 41 Uitvoeringswet AVG stelt dat er geen mededeling aan de betrokkene hoeft plaats te vinden als dat noodzakelijk is ter waarborging van een aantal gronden. (Enkel de gronden die voor de Provincie van belang zijn worden genoemd, zie voor een volledig overzicht het artikel)

- Nationale veiligheid;
- Openbare veiligheid;
- Voorkoming, onderzoek, opsporing en vervolging van strafbare feiten.

Artikel 33a lid 7 jo. artikel 27 lid 2 Wpg stelt dat de mededeling aan betrokkene kan worden uitgesteld, beperkt of achterwege gelaten kan worden:

- ter vermindering van belemmering van de gerechtelijke onderzoeken of procedures;
- ter vermindering van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
- ter bescherming van de openbare veiligheid;
- ter bescherming van de rechten en vrijheden van derden;
- ter bescherming van de nationale veiligheid;
- ingeval van een kennelijk ongegrond of buitensporig verzoek, als bedoeld in artikel 24a, vierde lid.

B. Wat moet worden medegedeeld aan betrokkene?

De informatie die bij een mededeling aan betrokkenen moet worden verstrekt stemt grotendeels overeen met de informatie die wordt gemeld aan de AP. De mededeling aan de betrokkene dient in duidelijke en eenvoudige taal te worden gedaan en dient op zijn minst de volgende informatie te bevatten (artikel 34 lid 2 AVG en artikel 33 lid 5 Wpg):

- 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 het datalek; 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.

Belangrijk is dat de betrokkene genoeg informatie heeft om de nodige voorzorgsmaatregelen te treffen. Volgens de eerder genoemde *Richtsnoeren voor de melding van datalekken* moet het bericht van een datalek in een specifiek bericht worden opgenomen en mag het niet samen met andere informatie worden verzonden. Op die manier wordt de communicatie over het datalek duidelijker en transparanter.

C. Wanneer moet het datalek worden gemeld aan de betrokkene?

Het datalek moet onverwijld worden gemeld aan de betrokkene. Onverwijld houdt in: zo snel als redelijkerwijs mogelijk (artikel 34 lid 1 AVG). Zo moeten betrokkenen bijvoorbeeld zonder onevenredige vertraging in kennis worden gesteld wanneer een onmiddellijk risico op schade moet worden beperkt, bijvoorbeeld wanneer creditcardgegevens in verkeerde handen zijn gevallen. Een langere kennisgevingstermijn kan gerechtvaardigd zijn als er passende maatregelen moeten worden genomen tegen aanhoudende of soortgelijke inbreuken in verband met persoonsgegevens (overweging 86 AVG). Hetzelfde geldt voor een datalek op grond van de Wpg.

Net als bij de melding aan de AP kan er eventueel voor worden gekozen om de betrokkene in eerste instantie te informeren op basis van de informatie waarover op dat moment wordt beschikt, zodat deze alvast maatregelen kan gaan treffen om zich te beschermen tegen de gevolgen van het datalek en om deze informatie in tweede instantie op basis van nader onderzoek aan te vullen.

Op de site van de AP waar een datalek gemeld moet worden, moet worden aangegeven of het

datalek al aan de betrokkene is gemeld en, zo niet, wanneer dat wordt gedaan of waarom het niet wordt gedaan. De termijn die in de melding aan de AP wordt vermeld, moet ook worden nagekomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, laat dit dan aan de AP weten door middel van een aanpassing van de melding. Als besloten wordt een datalek niet mee te delen aan de betrokkene, kan de AP daartoe alsnog verplichten (artikel 34 lid 4 AVG). In de Wpg is een dergelijke bepaling niet opgenomen. De melding aan de AP wordt door het cluster AJZ gedaan.

D. Welke gegevens over een datalek moeten worden vastgelegd?

De Provincie moet een overzicht bijhouden van alle datalekken/beveiligingsinbreuken die onder de meldplicht vallen. Dit om de AP in staat te stellen toezicht te houden op de naleving van de meldplicht. De Verordening verlangt niet dat deze documentatie openbaar wordt gemaakt, waarmee evenwel niet is uitgesloten dat een bestuursorgaan mogelijk wel op grond van de Wet open overheid gehouden kan zijn om deze documentatie openbaar te maken. Per datalek bevat het overzicht in ieder geval feiten en gegevens omtrent de aard van de inbreuk. Als het datalek is gemeld aan de betrokkene, dan ook de tekst van de kennisgeving aan de betrokkene in het overzicht opnemen. Dit zal hierna verduidelijkt worden.

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 AVG dient de verwerkingsverantwoordelijke bijzonderheden met betrekking tot het datalek te registreren, waaronder:

- de feiten van het datalek;
- de gevolgen van het datalek;
- de genomen corrigerende maatregelen.

In het kader van de Wpg worden dezelfde bijzonderheden met betrekking tot het datalek geregistreerd.

Zowel in de AVG als Wpg is niet bepaald hoelang deze gegevens moet worden bewaard. Indien deze geregistreerde gegevens van de melding van het datalek persoonsgegevens bevatten, is het aan de verwerkingsverantwoordelijke om een passende bewaartermijn te bepalen in overeenstemming met de beginselen voor de verwerking van persoonsgegevens en om te voldoen aan de rechtsgrond voor de verwerking. Als de geregistreerde gegevens geen persoonsgegevens bevatten, is het in de AVG opgenomen beginsel van opslagbeperking uiteraard niet van toepassing.

Naast deze details wordt aanbevolen dat de verwerkingsverantwoordelijke ook zijn motivering voor de besluiten die naar aanleiding van een inbreuk zijn genomen, documenteert. Met name wanneer een inbreuk niet is gemeld of medegedeeld, 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 (overweging 85 AVG). Indien de verwerkingsverantwoordelijke van mening is dat aan een van de voorwaarden van artikel 34 lid 3 AVG of artikel 33a lid 6 Wpg is voldaan, moet hij daarvoor afdoende bewijs kunnen leveren.

Als de verwerkingsverantwoordelijke een inbreuk niet meldt aan de AP, maar de melding uitstelt, moet dit gemotiveerd worden; documentatie waaruit blijkt dat uitstel noodzakelijk is zou kunnen helpen om aan te tonen dat het uitstel gerechtvaardigd en niet buitensporig is.

Indien de verwerkingsverantwoordelijke een inbreuk aan de getroffen personen mededeelt, dient deze 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.

De Provincie houdt een register bij van:



- alle (bekende) datalekken die zich voorgedaan hebben;
- de aan de AP gemelde datalekken;
- de aan betrokkenen medegedeelde datalekken;
- de motivatie waarom datalekken niet aan betrokkenen meegedeeld zijn;
- de motivatie van besluiten die als gevolg van een datalek zijn genomen.

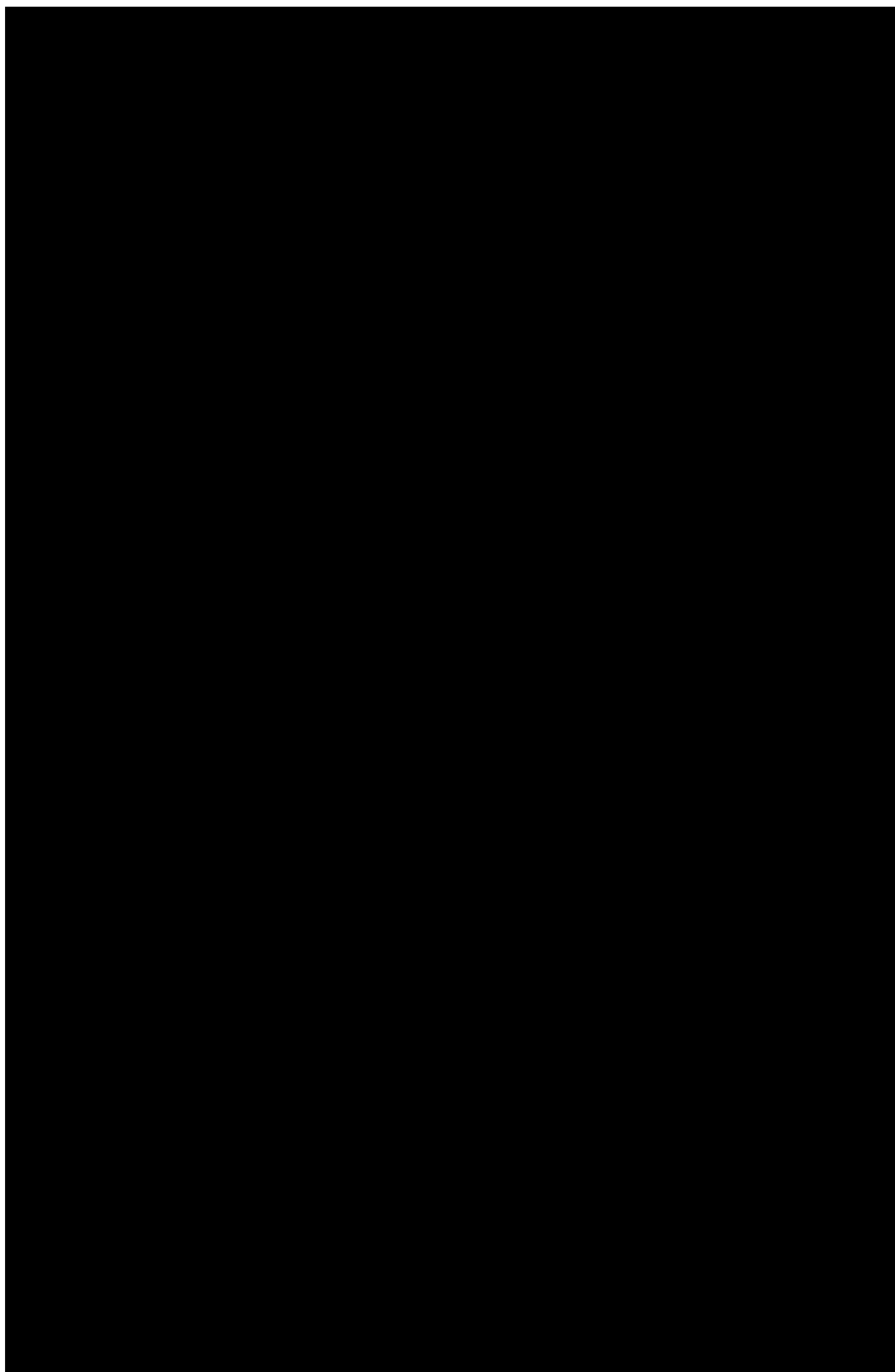
Gegevens die worden opgenomen in het Register Datalekken

1. Nummer
2. Naam incident
3. Omschrijving incident
4. Datum constatering
5. Categorieën betrokkenen
6. Uitvoerend cluster
7. Aantal betrokkenen
8. Type persoonsgegevens/politiegegevens
9. Aantal persoonsgegevens/politiegegevens
10. Aard incident²
11. Maatregelen getroffen
12. Tijdspad
13. Kennisgeving
14. Of er gemeld is aan AP
15. Termijn melding
16. Of betrokkenen zijn geïnformeerd
17. De wijze waarop betrokkenen zijn geïnformeerd

² '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.

10. Interne processen bij een datalek

		provincie limburg 
		Laatste wijziging: 22-jan-2020 9:21:25



Naam

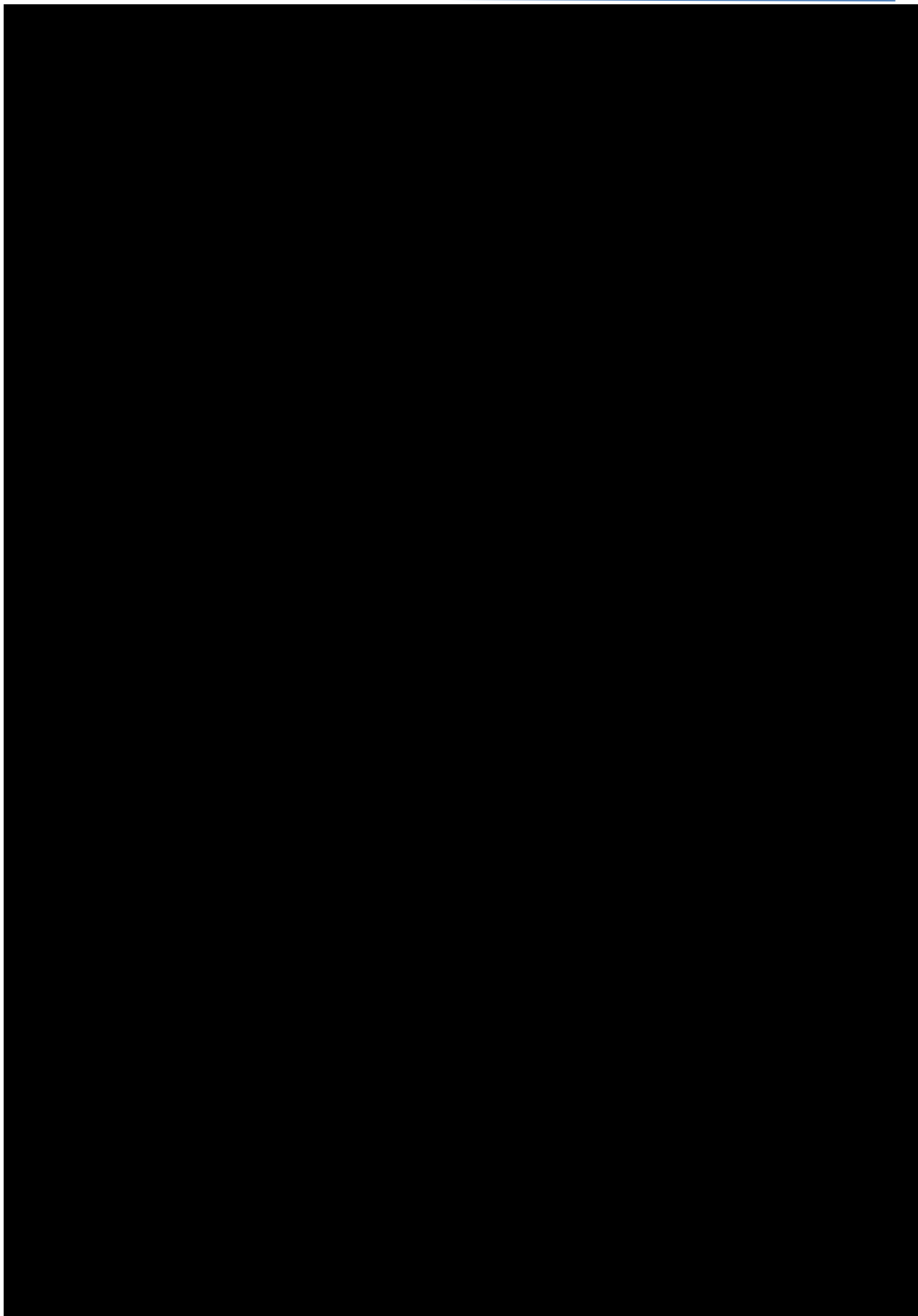
Melding datalek

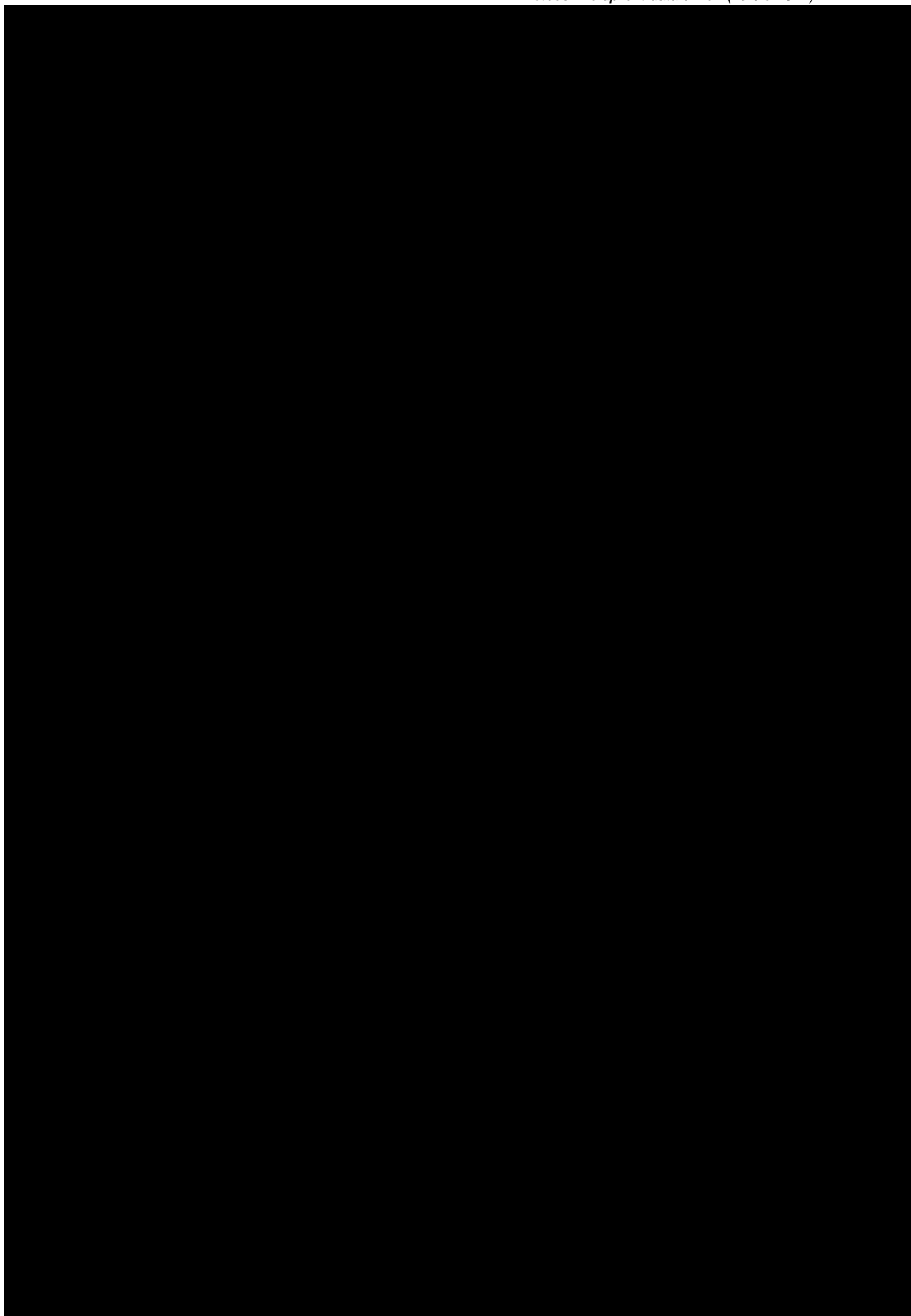
Beschrijving

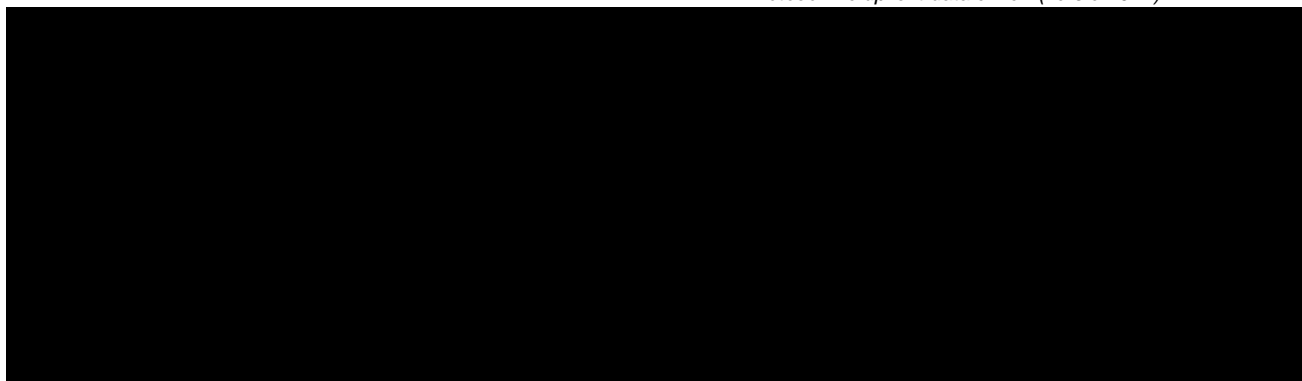
Het proces 'melding datalek' zorgt ervoor dat meldingen van (beveiligings)incidenten die op diverse wijze binnenkomen worden getoetst aan de AVG of Wpg.

Het proces zorgt voor de aanduiding, registratie en verder afhandeling van een datalek.

Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 is de leidraad voor dit proces.







11. SE rekenmethode

SE = DPC x EI + CB		
SE	= Ernst datalek	(Severity)
DPC	= Context data verwerking	(Data Processing Context)
EI	= Identificatierisico: gemak waarmee natuurlijke persoon kan worden geïdentificeerd	(Ease of Identification)
CB	= Omstandigheden datalek	(Circumstances of Breach)

DPC Score (Data Processing Context)

Bepaal het type persoonsgegevens en neem de contextuele factoren in rekening

Basis score	1	Alleen gewone persoonsgegevens zijn gelekt
	1.5	Een groot volume gewone persoonsgegevens gelekt (meerdere betrokkenen)
	2	Een groot aantal gewone persoonsgegevens van een grote groep betrokkenen
	2.5	Als de gelekte persoonsgegevens kunnen leiden tot profilering of conclusies omtrent bijzondere persoonsgegevens
	3	Bijzondere of gevoelige persoonsgegevens ³ zijn gelekt
	3.5	Bijzondere en gevoelige persoonsgegevens zijn gelekt
	4	Een grote hoeveelheid bijzondere en/of gevoelige persoonsgegevens zijn gelekt

Factoren die van invloed kunnen zijn op de hoogte van de DPC score

Verzwarende / Verminderende factoren	Het volume van de gegevens van dezelfde betrokkene
	Specifieke eigenschappen van de verwerker (vb. werkgever of bank)
	Specifieke eigenschappen van de betrokkenen (vb. kwetsbare groep)
	Als het lek slechts intern was
+/- 0.25 per punt (max. 1 punt)	Als de data incorrect is
	Als de data openbaar beschikbaar is
	Specifieke eigenschappen van de data/verwerking
	Als daadwerkelijk misbruik is gebleken
(deze lijst is niet uitputtend)	Als er snel actie ondernomen is

EI Score (Ease of Identification)

Beoordeel het identificatierisico. Hoe makkelijk is het om de identiteit van de betrokkene te achterhalen met de gelekte persoonsgegevens?

Verwaarloosbaar	0.2	Als er geen aanvullende informatie bekend is om betrokkenen te identificeren
	5	Als de data encrypted is
Gelimiteerd	0.5	Als de informatie op veel personen betrekking kan hebben
		Als er gebruik wordt gemaakt van 2 factor authenticatie

³ Onder gevoelige persoonsgegevens verstaan wij: een nationaal identificatienummer, strafrechtelijke gegevens, bestuursrechtelijke sancties, financiële gegevens, wachtwoorden.

Significant	0.75	Als de informatie iets zegt over betrokkenen (vb. <i>geslacht, adres, duidelijke foto</i>) of als de informatie maar op weinig betrokkenen betrekking kan hebben
Maximaal	1	Als er gebruik wordt gemaakt van 1 factor authenticatie Als betrokkenen makkelijk te identificeren zijn.
CB Score (Circumstances of the Breach) (B+I+V+K) Beoordeel de omstandigheden van het datalek.		
Verlies van beschikbaarheid (B)	0	Data verloren, maar kan snel zonder moeite worden hersteld.
	0.25	Data tijdelijk niet beschikbaar.
	0.5	Data verloren.
Verlies van integriteit (I)	0	Persoonsgegevens gewijzigd zonder enig geïdentificeerd incorrect of illegaal gebruik.
	0.25	Persoonsgegevens mogelijk veranderd/gebruikt op incorrecte of illegale wijze, maar herstel is mogelijk.
	0.5	Persoonsgegevens veranderd en mogelijk gebruikt op een incorrecte of illegale wijze, zonder de mogelijkheid van herstel.
Verlies van vertrouwelijkheid (V)	0	Persoonsgegevens waren mogelijk onderwerp van een inbreuk op de vertrouwelijkheid (zonder bewijs van illegale verwerking).
	0.25	Persoonsgegevens gelekt aan een bekend en beperkt aantal onbevoegden.
	0.5	Persoonsgegevens gelekt aan een onbekend aantal onbevoegden.
Kwaadwillendheid (K)	0.5	De inbreuk was het gevolg van een kwaadwillende daad.

Ernst van het datalek	
SE < 2	Laag
2 ≤ SE < 3	Medium
3 ≤ SE < 4	Hoog Melden AP
SE ≥ 4	Erg hoog Melden Betrokkenen