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, leden 1 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, leden 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

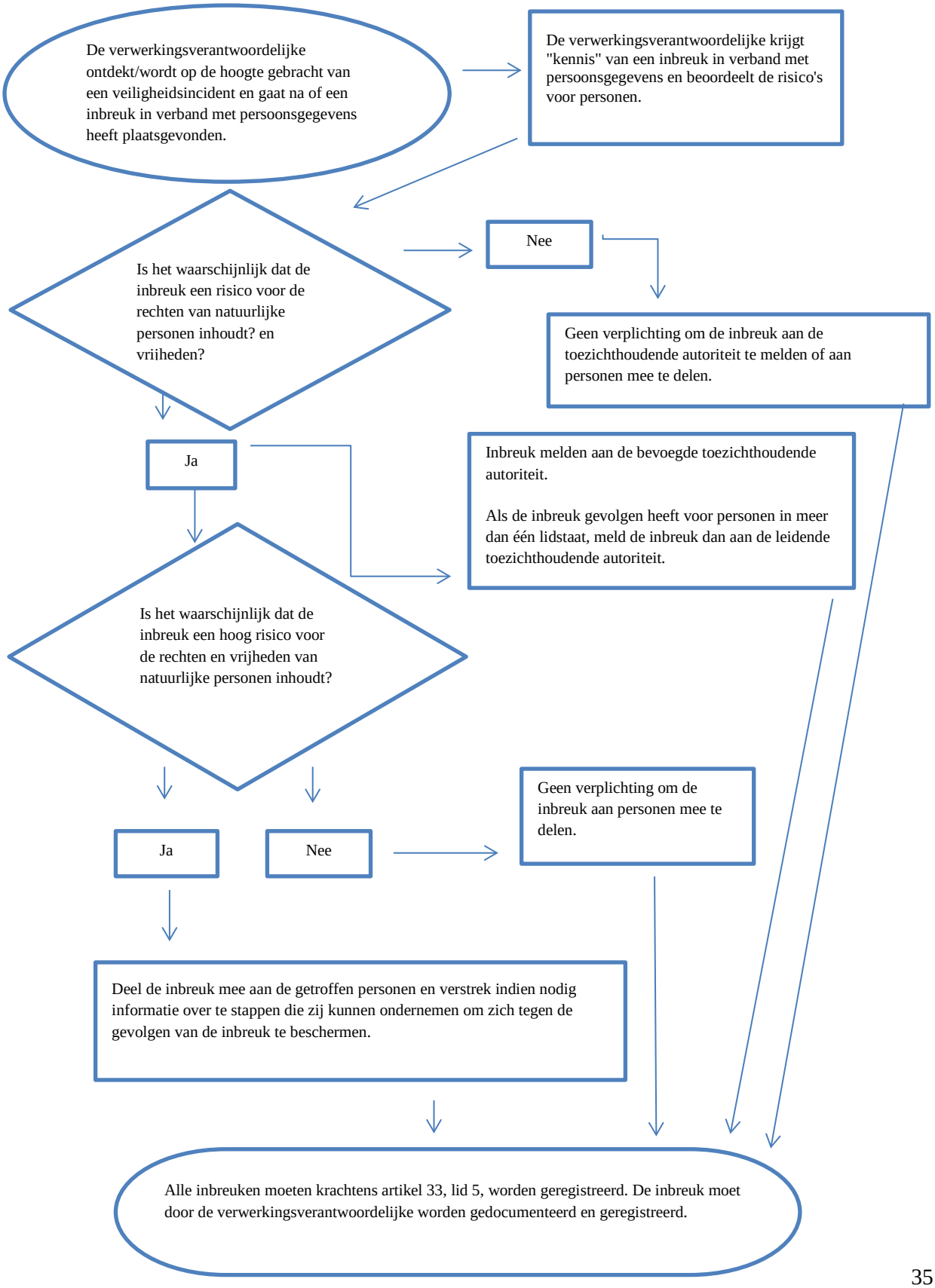
51 Overweging 63: *"In veel gevallen worden persoonsgegevens aangetast als gevolg van incidenten. Daarom moeten de bevoegde autoriteiten en de autoriteiten voor gegevensbescherming samenwerken en informatie over alle relevante zaken uitwisselen om inbreuken in verband met persoonsgegevens als gevolg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