Policy beveiligingsincidenten en gegevenslekken

Wie	Versie	Datum	Omschrijving
IVC Stad Aarschot	1.0	20230622	Beschrijving proces lokaal bestuur Aarschot: Stad Aarschot OCMW Aarschot AGB Aarschot

1 Inleiding

Lokale besturen moeten zich bewustzijn van hun verantwoordelijkheden als het gaat om de bescherming van de informatie ten behoeve van hun burgers en ketenpartners.

Alle medewerkers zijn verantwoordelijk voor informatiebeveiliging en dienen een incident te herkennen en weten waar ze dat moeten melden.

Afhankelijk van de impact en de urgentie van het incident dient er een prioritering aan gehangen te worden. Het eerste uur na ontdekking van een incident kan cruciaal zijn, er moet zo min mogelijk impact zijn van het incident zonder dat er informatie verloren gaat. Dit is namelijk nodig om later een goed onderzoek te kunnen doen naar de oorzaak van het incident.
Als het gaat om inbreuk op de beveiliging van of verlies van persoonsgegevens is de Meldplicht Gegevenslekken van toepassing als onderdeel van de Algemene Verordening Gegevensbescherming (AVG) (art. 33 en 34).

Als een beveiligingsincident betrekking heeft op persoonsgegevens, moet er binnen de 72 uur melding worden gemaakt aan de GBA (en de VTC) (art. 33, lid 1 AVG).

De meldplicht is eveneens van toepassing als het gegevenslek bij een derde is ontstaan, bijvoorbeeld een verwerker. Een verwerker moet zonder onredelijke vertraging een gegevenslek melden bij de verwerkingsverantwoordelijke (art. 33, lid 2 AVG).

Met de Meldplicht Gegevenslekken wil de Europese wetgever de gevolgen van een gegevenslek voor de betrokkenen zoveel mogelijk beperken en hiermee een bijdrage leveren aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens. Indien er sprake is van een ernstig gegevenslek, waarbij er kans is op verlies of onrechtmatige verwerking van persoonsgegevens, moet de verantwoordelijke het gegevenslek melden aan de Gegevensbeschermingsautoriteit (GBA) of de Vlaamse Toezichtcommissie voor de verwerking ven persoonsgegevens (VTC).

Elke Vlaamse instantie zoals vermeld in het Bestuursdecreet van 7/12/2018 (bv. art. II.115 §2 ev.) heeft de VTC als toezichthoudende autoriteit. Zowel steden, gemeenten alsook OCMW 's zijn Vlaamse instanties.

In een aantal gevallen moet het gegevenslek ook gemeld worden aan de betrokkenen.

Als er ten onrechte geen melding wordt gemaakt van een gegevenslek kan dit gesanctioneerd worden door de VTC en GBA.

In de AVG zelf wordt niet gesproken over een gegevenslek, maar over een inbreuk in verband met persoonsgegevens ('Inbreuk') (art. 4 (12) AVG).

De AVG stelt strenge eisen aan de eigen documentatie en registratie van de inbreuken die zich binnen een organisatie hebben voorgedaan (art. 33 lid 5 AVG). Hiermee kan de GBA controleren of een organisatie aan de meldplicht heeft voldaan (art. 5 lid 2 AVG).

De GBA vraagt om een adequate procedure te voorzien om gegevenslekken op te sporen, te rapporteren en te onderzoeken. De onderstaande procedure kan daarvoor behulpzaam zijn (art. 33 en 34 AVG en overweging 86 t/m 88AVG).

100% beveiligen bestaat niet en los daarvan: niet alle incidenten zijn te voorkomen. Het is niet de vraag óf er iets gaat gebeuren maar wanneer.

De belangrijkste te verwachte incidenten kunnen van te voren bedacht worden en de bijpassende reactie en escalatieprocedure kan dus ook van te voren uitgewerkt en geoefend worden.

1.1 Doel

Deze procedure is bedoeld voor het snel oplossen van beveiligingsincidenten en, indien nodig, het tijdig melden van gegevenslekken.

Het doel van deze procedure is eveneens om vast te leggen welke stappen genomen moeten worden door de verwerkingsverantwoordelijke bij het vermoeden van of kennisnemen van een incident dat (mogelijks) een gegevenslek is. Het volgende resultaat wordt hiermee nagestreefd:

- volgen van een eenduidige procedure;
- zorgvuldig waarborgen van de belangen van de verwerkingsverantwoordelijke, de betrokkene en/of een derde die betrokken is bij het incident, dat (mogelijks) een gegevenslek is;
- op zorgvuldige en systematische wijze analyseren van een incident, dat (mogelijks) een gegevenslek is, zodat aanwezige risico's in het proces zichtbaar worden. Centraal staat hierbij het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijks) hebben kunnen leiden tot het incident;
- bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen van deze verbetermaatregelen;
- realiseren van een voldoende en eenduidige interne en op verzoek externe verantwoording over de afhandeling van een incident, zijnde (mogelijk) gegevenslek.

Deze procedure legt eveneens de taken, verantwoordelijkheden en bevoegdheden met betrekking tot beveiligingsincidenten / gegevenslekken vast.

Een incident moet behalve intern opgelost soms ook extern geëscaleerd worden zodat anderen gewaarschuwd kunnen worden en daarmee de impact van het incident zo klein als mogelijk gehouden kan worden.

Bijlage 1 bevat een uitgebreide lijst van mogelijke incidenten die moeten gemeld worden.

1.2 Waarom deze procedure?

Beveiligingsincidenten kunnen leiden tot informatie en/of gegevens die verloren gaan of onbedoeld gewijzigd worden. Dit kan gevolgen hebben voor de kwaliteit en continuïteit van de werking en de dienstverlening van een organisatie.

Daarnaast kunnen vertrouwelijke gegevens door beveiligingsincidenten lekken of in verkeerde handen vallen. Voor de verwerking van persoonsgegevens zijn regels vastgelegd in de AVG. Het niet-zorgvuldig omgaan met vertrouwelijke gegevens kan leiden tot stopzettingen van verwerkingen van persoonsgegevens en imagoschade.

2 Definities

Beveiligingsincident :

- elke niet toegelaten toegang tot of verstrekking van informatie (vertrouwelijkheid)
- elke niet toegelaten wijziging of beschadiging van informatie (integriteit)
- elke toevallige, accidentele of ongeoorloofde vernietiging of verlies van informatie (beschikbaarheid)
- elke verwerking van gegevens voor een doel dat niet ondersteund wordt door de wettelijke opdracht of door een andere wettelijke grond (doelgebondenheid)
- elke situatie die tot een van de bovenstaande situaties kan leiden

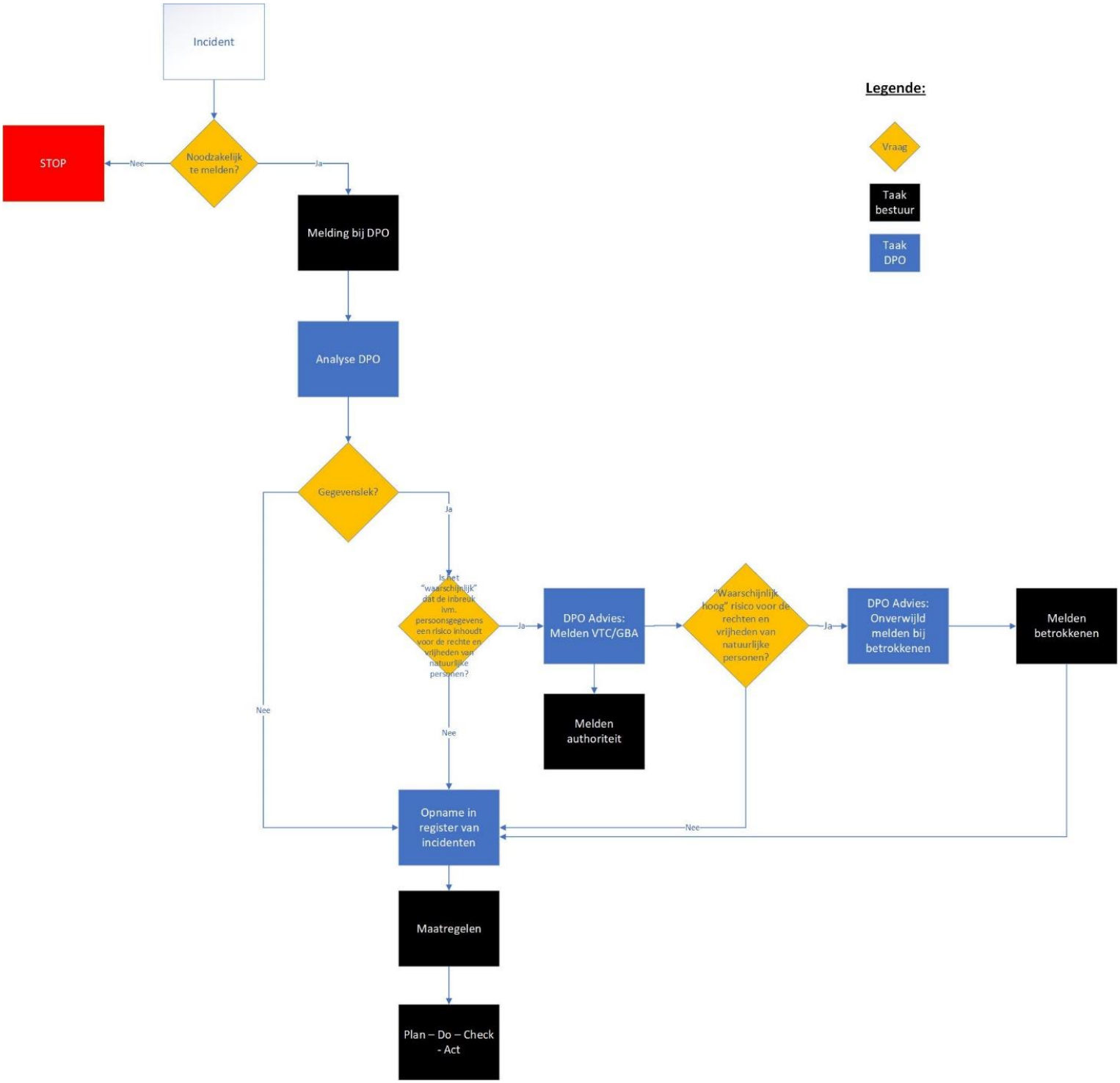
Gegevenslek :

elk beveiligingsincident waarbij persoonsgegevens betrokken zijn

Persoonsgegevens :

- Een persoonsgegeven is iedere informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon (de “betrokkene” genoemd in de AVG).
- Een persoon kan geïdentificeerd worden via de naam, een foto, een telefoonnummer, zelfs een telefoonnummer op het werk, een code, een bankrekeningnummer, een e-mailadres, een vingerafdruk, een IP-adres,…of het combineren van deze of andere gegevens.

3 Procedure


Incident
Noodzakelijk te melden?
Nee
STOP
Ja
Melding bij DPO
Analyse DPO
Gegevenslek?
Ja
Nee
Is het "waarschijnlijk" dat de inbreuk ivm. persoonsgegevens een risico inhoudt voor de rechte en vrijheden van natuurlijke personen?
Ja
Nee
DPO Advies: Melden VTC/GBA
Melden authoriteit
"Waarschijnlijk hoog" risico voor de rechten en vrijheden van natuurlijke personen?
Ja
Nee
DPO Advies: Onverwijld melden bij betrokkenen
Melden betrokkenen
Opname in register van incidenten
Maatregelen
Plan – Do – Check - Act
Legende:
Vraag
Taak bestuur
Taak DPO

3.1 Intern melden van een incident

Alle medewerkers en mandatarissen moeten alle beveiligingsincidenten en datalekken zo snel mogelijk melden.

Werkwijze :

- ⇨ via e-mail: privacy@aarschot.be of privacy@ocmw-aarschot.be;
- ⇨ aan de intern verantwoordelijke;
- ⇨ ICT dienst: helpdesk@aarschot.be; wanneer het incident verband houdt met ICT;
- ⇨ Het eigen diensthoofd.

Het incident wordt onderzocht door degene aan wie de melding gebeurde. Afhankelijk van de aard van het incident, kan de DPO, de ICT-medewerker/dienst ICT en/of het diensthoofd samenwerken en alle informatie opvragen die nuttig wordt geacht.

Er gebeurt een controle of het incident al dan niet ook een datalek is. Zo ja, dan is verder escalatie noodzakelijk.

Een incident moet onmiddellijk worden geëscaleerd naar de DPO als:

- er persoonsgegevens in het incident zijn betrokken
- er meerdere entiteiten (bijv. meerdere steden en gemeenten) bij betrokken zijn of dreigen te worden

er een authentieke bron (bijv. het Rijksregister, de Kruispuntbank van de Sociale Zekerheid, de DIV) bij betrokken is of dreigt te worden.

3.2 Gegevenslekken melden aan de GBA

Bij een datalek dat een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, adviseert de DPO om melding te maken aan de toezichthoudende autoriteit de GBA en de VTC, zonder onredelijke vertraging en indien mogelijk, uiterlijk 72 uur na kennisname. Indien de melding niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

Artikel 33, lid 1 AVG

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.

Het melden van een gegevenslek aan de GBA is niet altijd verplicht. De melding dient alleen te gebeuren wanneer het waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De organisatie dient dit zelf af te wegen aan de hand van *(Checklist Privacy, Berghauser Pont, blz. 56 – 57):*

- De aard, gevoeligheid en hoeveelheid gegevens;
- De moeilijkheidsgraad van identificatie van betrokkene;
- De omvang van de inbreuk en de impact op de betrokkenen, waaronder: specifieke eigenschappen van de betrokkenen (zoals kinderen en ouderen);
- De hoeveelheid betrokkenen;
- Specifieke eigenschappen van de organisatie (bijvoorbeeld een woonzorgcentrum, kinderdagverblijf);
- Overige relevante eigenschappen.

De melding aan de GBA (en de VTC) moet de volgende gegevens bevatten (art 33, lid 3 AVG):

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 de contactgegevens van de DPO;
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.

Indien en voor zover het voor de verwerkingsverantwoordelijke niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt (art. 33 lid 4 AVG).

De verwerkingsverantwoordelijke moet zelf een beredeneerde afweging maken of een informatiebeveiligingsincident dat hen ter kennis komt een gegevenslek is en binnen het bereik van de wettelijke meldplicht valt. Bij twijfel wordt er aangeraden om de gegevenslek te melden aan de GBA.

De richtlijnen om een melding in te dienen bij de GBA kan men terugvinden op hun website via https://www.gegevensbeschermingsautoriteit.be/melding-van-gegevenslekken .

Op basis van huidige uitspraken en ontwikkelingen, wordt ook aangeraden van elke melding die naar de Gegevensbeschermingsautoriteit (GBA) zou worden gedaan, ook door te geven aan de Vlaamse Toezichtcommissie (VTC).

De Vlaamse Toezichtcommissie is als toezichthoudende autoriteit verantwoordelijk voor het toezicht op de toepassing van de Algemene Verordening Gegevensbescherming (AVG of GDPR) door de Vlaamse bestuursinstanties. Al wordt hun bevoegdheid momenteel uitgehold door de uitspraak van het Grondwettelijk Hof nr 26/2023. Er kan evenwel verwacht worden dat melding aan de VTC weer verplicht zal worden voor Vlaamse bestuursinstanties.

De VTC stelt een formulier beschikbaar dat gebruikt dient te worden voor het melden van gegevenslekken:

https://overheid.vlaanderen.be/digitale-overheid/vlaamsetoezichtcommissie/formulier-melden-gegevenslek

Dit moet ingevuld per e-mail verzonden worden naar de VTC op het e-mail adres contact@toezichtcommissie.be

3.3 Gegevenslek melden aan de betrokkene

Artikel 34, lid 1 AVG

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.

Deze mededeling moet een omschrijving bevatten van de aard van het gegevenslek, in passende en eenvoudige taal. Tevens moeten de contactgegevens van de DPO worden bezorgd, de (mogelijke) gevolgen van de inbreuk en de getroffen maatregelen.

De melding aan betrokkenen kan gebeuren via een zelfgekozen communicatiekanaal zoals een brief, een e-mailbericht of SMS.

Onder volgende voorwaarden is een meldplicht alsnog niet vereist (art. 34, lid 3 AVG):

- De verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
- De verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
- De mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

Voor de verwerkingsverantwoordelijke is het doel om zo min mogelijk te hoeven melden aan de GBA.

Dit gebeurt in eerste instantie door het in acht nemen van de noodzakelijke technische en organisatorische maatregelen ter bescherming van de privacy, ten opzichte van het verwerken van persoonsgegevens. Deze zijn er op gericht om de basisbeginselen van de AVG in ere te houden: finaliteit, transparantie en proportionaliteit.

Indien de melding van een gegevenslek nodig is, is het nog belangrijker om het verplicht melden aan de betrokkenen correct uit te voeren.

Het mag echter duidelijk zijn dat in het belang van de verwerkingsverantwoordelijke, vanwege de kans op imago- en financiële schade (als gevolg van publiciteit, nazorg en mogelijke schadeclaims van de betrokkenen), de meldplicht, de communicatieplicht naar betrokkenen en het continu overleg met en betrokkenheid van de DPO een voortdurend aandachtspunt moet zijn.

Om de kans op melding te voorkomen is standaardversleuteling van alle persoonsgegevens op basis van gangbare technieken een serieuze optie (art. 34, lid 3, punt a AVG).

3.4 Welke zijn de risico's voor de betrokkenen?

Overweging 75 (AVG) levert een niet limitatieve voorbeeldlijst van risico's die kunnen voortkomen uit een gegevensverwerking.

Het qua waarschijnlijkheid en ernst uiteenlopende risico voor de rechten en vrijheden van natuurlijke personen kan voortvloeien uit persoonsgegevensverwerking die kan resulteren in:

- Ernstige lichamelijke, materiële of immateriële schade, met name:
  waar de verwerking kan leiden tot :
  - discriminatie,
  - identiteitsdiefstal of -fraude,
  - financiële verliezen,
  - reputatieschade,
  - verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens,
  - ongeoorloofde ongedaanmaking van pseudonimisering,
  - of enig ander aanzienlijk economisch of maatschappelijk nadeel;
- Wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen;
- Wanneer persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt, en bij de verwerking van genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen;
- Wanneer persoonlijke aspecten worden geëvalueerd, om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- Wanneer persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt; of
- Wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

3.5 Gegevenslekken documenteren

De verwerkingsverantwoordelijke houdt een register (hierna het Incidentenregister) bij van alle gegevenslekken waarvan hij kennis heeft genomen (art. 33, lid 5 AVG).

Artikel 33, lid 5 AVG

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.

In het Incidentenregister dienen de volgende gegevens te worden vermeld:

- Wanneer het lek plaatsvond;
- Een korte beschrijving van het lek;
- Wat er gebeurd is met de gegevens;
- Hoeveel gegevens gelekt zijn;
- Van welke categorie personen de gegevens gelekt zijn;
- Welke soort gegevens;
- Gevolgen van de inbreuk;
- Genomen maatregelen (zowel schade beperkend als preventief);
- Wanneer de meldplicht voldaan werd en indien niet, de reden daarvoor.

Het Incidentenregister is een nuttig document om het aantal gegevenslekken te monitoren en daar gevolgen uit te trekken. Daarnaast kan het een handig document zijn om voor te leggen aan de GBA en/of VTC om aan te tonen dat de verwerkingsverantwoordelijke bewust omgaat met gegevenslekken.

4 Meldplicht door de verwerker

De verwerker is verplicht om elke gegevenslek te melden aan de verwerkingsverantwoordelijke (art. 33, lid 2 AVG). Hij dient dit te doen zonder onredelijke vertraging na kennisname van het gegevenslek. Er werd in de AVG geen tijdsperiode voorzien waarin de verwerker de verwerkingsverantwoordelijke op de hoogte moet brengen.

Artikel 33, lid 2 AVG

De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

Het is aangewezen dat de verwerkingsverantwoordelijke in de verwerkersovereenkomst een procedure opneemt waaraan de verwerker moet voldoen bij het vaststellen van een gegevenslek van persoonsgegevens van de verwerkingsverantwoordelijke.

Daarin kan best beschreven worden welke gegevens hij dient mee te delen en binnen welke termijn na kennisname. Dezelfde termijnen zijn hier gangbaar die ook ten aanzien van de verplichting voor de verwerkingsverantwoordelijke gelden vanuit de AVG.

De verwerkingsverantwoordelijke is eveneens verantwoordelijk voor het melden van een gegevenslek indien dit lek is veroorzaakt door een verwerker.

5 Taken, verantwoordelijkheden en bevoegdheden

Echte of vermoede beveiligingsincidenten moeten zo spoedig mogelijk worden gemeld.

Het lokaal bestuur Aarschot: STAD AARSCHOT, OCMW AARSCHOT & AGB AARSCHOT stelt een externe medewerker aan om beveiligingsincidenten af te handelen. Dit is voor het lokaal bestuur Aarschot de externe DPO van VERA.

De intern verantwoordelijke wordt door de algemeen directeur aangeduid.

De medewerkers van het lokaal bestuur Aarschot worden op de hoogte gebracht dat alle beveiligingsincidenten verplicht en onmiddellijk moeten worden gemeld aan de dienstverantwoordelijke, de intern verantwoordelijke en de DPO via e-mail op privacy@aarschot.be of privacy@ocmw-aarschot.be. (zie 2 Definities beveiligingsincident, gegevenslek en/of persoonsgegevens)

Bij dringende zaken gebeurt dit zowel telefonisch op **016/55 03 25** als via e-mail op privacy@aarschot.be of privacy@ocmw-aarschot.be met vermelding van :

- datum en tijdstip,
- vaststeller van de inbreuk en de contactgegevens,
- omschrijving van het beveiligingsincident.

5.1 Procedure

1. Telefonisch contact opnemen met de helpdesk ICT: 016 55 03 25 (enkel bij dringende zaken)
2. Melding per e-mail aan DPO en intern verantwoordelijke via e-mail:
   privacy@aarschot.be (Stad Aarschot & AGB Aarschot)
   privacy@ocmw-aarschot.be (OCMW Aarschot)
3. Melding aan de dienstverantwoordelijke
4. Informatie te vermelden bij een beveiligingsincident:
   onderwerp e-mail: beveiligingsincident
   1. Datum en tijdstip van de inbreuk;
   2. Vaststeller van de inbreuk en de contactgegevens;
   3. Omschrijving van het beveiligingsincident.

Het niet voldoen aan deze interne meldplicht kan leiden tot sancties.

De DPO is verantwoordelijk voor het onderzoeken van het beveiligingsincident. De bij het beveiligingsincident betrokken dienst(en) verlenen zonder verwijl hun volledige medewerking. Hierbij is onder meer aandacht voor de volgende aspecten:

1. Wat is de aard van het beveiligingsincident;
2. Wat is de oorzaak dat dit beveiligingsincident heeft plaatsgevonden;
3. Is er sprake van een gegevenslek;
4. Is er sprake van het niet nakomen of van een tekortkoming in de technische en organisatorische beveiligingsprocedures.

De DPO is verantwoordelijk voor:

- het vastleggen van elk beveiligingsincident in het Incidentenregister,
- het (mee helpen) bepalen van technische en organisatorische maatregelen (niet de beslissing of de uitvoering),
- of er intern/extern moet worden gecommuniceerd en de wijze waarop dit dient te gebeuren.

De Algemeen directeur is verantwoordelijk voor:

- Het goedkeuren van de effectieve melding bij de autoriteiten.

Naargelang de ernst van het beveiligingsincident wordt daarbij het **advies van de IVC (Informatie Veiligheidscomité)** ingewonnen en wordt bepaald wie welke rol dient op te nemen ter uitvoering van de technische en organisatorische en communicatiemaatregelen.

Bij de beslissing van het bestuur bij een beveiligingsincident dat zich heeft voorgedaan dat gemeld moet worden aan de GBA en/of VTC, en eventueel daarnaast ook aan de betrokkenen, moeten er een aantal afwegingen worden gemaakt.

Eventuele aanwijzingen van de GBA en/of VTC worden door de DPO in het Incidentenregister vastgelegd en opgevolgd.

De DPO analyseert de gedurende een jaar ontvangen meldingen en op basis hiervan stelt DPO een verbeterplan of -advies op. Dit plan of advies wordt opgenomen in de jaarlijks uit te brengen managementrapportage en wordt ter goedkeuring (verbeterplan) / aktename (verbeteradvies) voorgelegd aan de bevoegde organen.

Minimaal jaarlijks beoordeelt de DPO of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Als deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden en of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de procedure.

De DPO is verantwoordelijk voor de actualiteit van deze procedure.

6 Inwerkingtreding

De bepalingen en procedure Beveiligingsincidenten en Gegevenslekken treden in werking vanaf goedkeuring door de gemeenteraad en raad voor maatschappelijk welzijn.

De algemeen directeur is verantwoordelijk voor het bepalen van de wijze waarop de kennisgeving aan alle personeelsleden gebeurt binnen de organisatie.

Dit beleid wordt toegevoegd aan het arbeidsreglement.

Wat betreft sanctiemaatregelen igv. het niet-nakomen van de meldingsplicht van een beveiligingsincident voor interne medewerkers moet een vermelding wel verplicht opgenomen worden in het arbeidsreglement.

Voorzitter Gemeenteraad
Voorzitter Raad voor maatschappelijk welzijn
Voorzitter Raad van bestuur AGB Aarschot

Algemeen directeur Stad Aarschot
Algemeen directeur OCMW Aarschot
Secretaris AGB Aarschot
Christi Van Calster

BIJLAGE 1:

Opsomming van situaties die een beveiligingsincident inhouden, en mogelijks een gegevenslek (inbreuk in verband met persoonsgegevens) en die intern moeten gemeld worden

- Verlies of diefstal van een dossier (papier), usb-stick, tablet, laptop of andere gegevensdragers;
    - Een papieren dossier belandt op straat omdat ze “bij het oude papier” worden gezet.
    - Een USB stick met persoonsgegevens (wel of niet geëncrypteerd) wordt verloren
    - Afgevoerde dossiers in een onbeveiligde ruimte gestockeerd
- Inbreuk op fysieke beveiligingsvoorzieningen;
    - Namaken van sleutels
    - Doorgeven van persoonlijke toegangsbadge
    - Verlies van persoonlijke toegangsbadge
- Vergeten papieren op de printer (zeker als die in een publieke ruimte staat) met persoonsgegevens
    - Met loongegevens
- Documenten die niet meer worden teruggevonden (verloren), ook in het gebouw
    - Loonbrieven
- Toegangsovertredingen (digitaal)
    - Inloggen met de account / wachtwoord van iemand anders
    - Onzorgvuldig omgaan met wachtwoorden zodat iemand anders ze te weten kan komen
        - doorgeven van een wachtwoord aan een collega
        - wachtwoorden onbeveiligd opslaan (schriftje, word document, excel document)
    - Je sessie kan overgenomen worden door iemand anders omdat je schermbeveiliging niet opstond bij het verlaten van je werkplek
- Opzettelijk foutief handelen (fraude, diefstal);
    - Oneigenlijk gebruik van admin rechten
    - Oneigenlijk gebruik van de toegang tot het Rijksregister / bevolkingsregister / KSZ gegevens
- Beschadigen of vernielen van (kritische) apparatuur;
- E-mail gebruik
    - Virusbesmetting als gevolg van het aanklikken van een onbetrouwbare bijlage;
    - E-mail met niet versleutelde vertrouwelijke informatie;
        - versturen van onbeveiligde Excels met persoonsgegevens naar een externe organisatie
    - Klikken op een onbetrouwbare link in een e-mail waardoor je malware binnenhaalt
    - Verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden (gebruik van TO of CC ipv BCC)
    - E-mail verzonden naar de verkeerde persoon, zeker als er persoonsgegevens instaan
    - Een e-mail doorsturen naar externen
- Onbevoegd inzien van vertrouwelijke informatie;

- De toekenning van rechten tot informatie is te ruim.
    - Vb. gemeentepersoneel heeft toegang tot informatie van het OCMW zonder formele beslissing dat dit mag
    - Vb. personeel van de sociale dienst heeft toegang tot de mappen van de thuiszorgdiensten
  - Gebruik maken van iemand anders zijn/haar toegangen
- Onbedoelde openbaarmaking van vertrouwelijke informatie;
  - Onvoldoende richtlijnen in het gebruik van de notuleringssoftware
  - Publiceren van vertrouwelijke persoonsgegevens op de website vanuit de notuleringstoepassing
  - Publicatie van persoonsgegevens in besluitenlijsten
  - Niet gebruik van de “vertrouwelijk” knop in de notuleringstoepassing
- Website
  - Onbeveiligde website waar persoonsgegevens wordt gevraagd in webformulier
- Download Illegale software;
- Illegaal kopiëren van gegevens;
- Cyberaanvallen;
- Computerhacking;
- Besmetting met ransomware, met of zonder bruikbare back-up;
- Technisch falen van apparatuur;
  - Uitval internetverbinding door uitgetrokken kabel
- Kwetsbaarheid in een applicatie waardoor persoonsgegevens gelekt worden
- Stroomuitval;
- Wateroverlast;
- …

BIJLAGE 2:

voorbeelden van incidenten en hun beoordeling:

Voorbeeld wel / geen inbreuk in verband met persoonsgegevens:

Een database met persoonsgegevens is vernietigd als gevolg van een menselijke fout van een systeembeheerder. Van de database is een complete, actuele back-up beschikbaar, op basis waarvan de database direct weer wordt opgebouwd. In deze situatie is er geen sprake van een inbreuk in verband met persoonsgegevens. Deze inbreuk wordt in het logboek ingeschreven, maar moet niet gemeld worden.

Voorbeeld wel / geen inbreuk in verband met persoonsgegevens:

Een werknemer geeft aan een derde de gebruikersnaam en het wachtwoord die toegang geven tot alle klantgegevens van alle klanten van het bestuur waar hij werkt.

Na ontdekking van het gebeurde past het bestuur het wachtwoord van het betreffende account aan, zodat de derde geen toegang meer heeft.

Daarna onderzoekt het bestuur of de derde daadwerkelijk toegang heeft gezocht tot de klantgegevens. Bij dit onderzoek maakt het bestuur gebruik van logbestanden, waarin per gebruikersnaam is vastgelegd welke acties er op welk tijdstip zijn uitgevoerd met welke klantgegevens.

Als op basis van de logbestanden redelijkerwijs kan worden uitgesloten dat er door middel van het betreffende account toegang is verkregen tot de klantgegevens, dan is er uitsluitend sprake van een beveiligingslek en niet van een inbreuk in verband met persoonsgegevens. Deze inbreuk wordt in het logboek ingeschreven maar moet niet gemeld worden.

Voorbeelden van inbreuken in verband met persoonsgegevens die moeten worden ingeschreven in het logboek, gemeld aan de Toezichtcommissie en in sommige gevallen aan de betrokkene:

- Intern wordt binnen een ziekenhuis gesignaleerd dat door een haperende beveiliging (technische storing) medische gegevens mogelijks zijn ingezien door onbevoegden;
- Een journalistiek programma confronteert een bestuur met het feit dat als gevolg van een beveiligingslek onder andere persoonlijke gegevens (zoals kopieën van paspoorten of rijbewijzen, bankgegevens en wachtwoorden) van werknemers op de server van het bestuur door onbevoegden zijn ingezien;
- Een medewerker verliest een laptop met onversleutelde klantgegevens;
- Een bestuur krijgt te maken met een hack waarbij klantgegevens en wachtwoorden zijn ontvreemd;
- Een overheidsdatabank met gevoelige persoonsgegevens wordt gehackt waardoor onbevoegden toegang hebben gekregen tot deze gegevens.

- Vier laptops zijn gestolen bij een gezondheidscentrum voor kinderen. De laptops bevatten gevoelige gegevens over gezondheid en welzijn en andere persoonsgegevens van meer dan 2000 kinderen. Gelet op de mogelijke gevolgen van de inbreuk in verband met persoonsgegevens is kennisgeving aan de betrokkenen geboden, evenals melding aan de toezichtcommissie. Daarbij is het wel belangrijk om rekening te houden met de leeftijd en de rijpheid van de betrokkenen. Naast de kennisgeving aan het kind zelf, voor zover deze passend is, kan het in dit geval juister zijn om een ouder of voogd, die al actief betrokken is bij de medische verzorging van het kind, op de hoogte te brengen. Door de kwijtgeraakte gegevens kan de integriteit van de medische dossiers worden aangetast, wat de behandeling van de kinderen kan verstoren. Als de ouders of verzorgers op de hoogte zijn van de inbreuk in verband met persoonsgegevens dan kunnen ze hier alert op zijn, en kunnen ze bij eventuele afwijkingen in de medische zorg voor hun kinderen contact opnemen met de betreffende zorgverlener.
- Bij een levensverzekeraar waren persoonsgegevens ongeoorloofd ingezien als gevolg van een kwetsbaarheid in een webapplicatie. Van 700 personen konden naam, adres en formulieren met medische gegevens worden ingezien. Als de aanvaller buitgemaakte gegevens op internet zet kan dat er bijvoorbeeld toe leiden dat betrokkenen moeilijker een baan kunnen vinden, als gevolg van het bekend worden van informatie over gezondheidsproblemen, zwangerschap, etc. Betrokkenen kunnen ook te maken krijgen met phishing of identiteitsfraude. De inbreuk in verband met persoonsgegevens heeft een hoog risico op negatieve gevolgen voor de betrokkenen, die er daarom ook (= naast de toezichtcommissie) van in kennis moeten worden gesteld.
- Een medewerker van een internetprovider heeft zijn login/wachtwoordgegevens aan een derde partij gegeven die daardoor nagenoeg onbeperkt bij alle klantgegevens (meer dan 100.000) kon komen. Het kan niet redelijkerwijs worden uitgesloten dat er daadwerkelijk persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. De derde partij had onder meer toegang tot betaalgegevens (waaronder creditcardinformatie) en hashwaarden van wachtwoorden van klanten. Misbruik van de betaalgegevens kan financiële gevolgen hebben voor de klanten. Ook is het mogelijk dat de onbevoegde derde op basis van de buitgemaakte hashwaarden de oorspronkelijke wachtwoorden van de klanten kan achterhalen. De inbreuk in verband met persoonsgegevens heeft een hoog risico op negatieve gevolgen voor de betrokkenen, die er daarom van in kennis moeten worden gesteld, evenals de toezichtcommissie. Als de wachtwoorden niet meer veilig zijn, dan moet de verantwoordelijke de klanten op een veilige manier verplichten om een nieuw wachtwoord aan te maken. Hij moet daarbij zorgen dat de nieuwe wachtwoorden worden aangemaakt door legitieme gebruikers, en niet door derden die de inloggegevens hebben bemachtigd. Hij moet daarbij ook aangeven wat de reden is voor de vervanging van het wachtwoord.
- Een envelop met creditcardbetalingsgegevens van 800 personen was per ongeluk niet versnipperd, maar in een vuilnisbak gegooid. Een derde persoon haalde de gegevens uit de vuilniscontainer op straat en verstrekte ze aan andere personen. De inbreuk in verband met persoonsgegevens kan financiële consequenties hebben voor de betrokkenen, als hun kaartgegevens nog geldig zijn en worden misbruikt. De betrokkenen moeten daarom van de inbreuk in verband met persoonsgegevens in kennis worden gesteld, evenals de toezichtcommissie.
- De versleutelde laptop van een financieel adviseur is uit de auto gestolen. Financiële gegevens (hypotheken, salarissen, leningen) van 1000 personen waren betrokken.

Hoewel het wachtwoord van de laptop niet gecompromitteerd is, was er geen back-up voorhanden. Aangezien de verantwoordelijke niet meer beschikt over de persoonsgegevens die op de laptop stonden, zullen deze opnieuw door de betrokkenen moeten worden verstrekt. Op zich heeft dit slechts beperkte negatieve gevolgen voor de betrokkenen: er is hooguit sprake van frustratie en tijdverspilling omdat ze alle informatie nogmaals moeten verzamelen. In sommige gevallen kunnen ook deadlines voor de indiening van documenten of aanvragen worden overschreden, wat kan leiden tot financiële schade voor de betrokkenen. De betrokkenen moeten van de inbreuk in verband met persoonsgegevens in kennis worden gesteld, evenals de toezichtcommissie. In de kennisgeving moet worden aangegeven dat de gegevens opnieuw aan de financieel adviseur moeten worden verstrekt, en moet uitleg worden gegeven over de potentiële consequenties en mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens.

- Op de website van een telefoonbedrijf kunnen klanten inloggen en hun financiële gegevens en belgegevens inzien. Een derde partij heeft toegang gekregen tot de database met inlognamen en bijbehorende hashwaarden van wachtwoorden. Bij het hashen van de wachtwoorden is gebruik gemaakt van een verouderd algoritme dat onvoldoende bescherming biedt tegen kennisname door onbevoegden. Gevolg is dat een derde partij de oorspronkelijke wachtwoorden zonder al te veel moeite zal kunnen achterhalen. De derde partij kan de wachtwoorden van alle abonnees achterhalen. Hij beschikt ook over de inlognamen, en kan zich daardoor toegang verschaffen tot alle accounts. Veel mensen gebruiken voor het inloggen op meerdere websites dezelfde combinatie van inlognaam en wachtwoord. Dit betekent dat de derde zich met de buitgemaakte gegevens mogelijk ook toegang kan verschaffen tot andere accounts van sommige betrokkenen, waaronder mogelijk ook e-mailaccounts. Deze inbreuk in verband met persoonsgegevens heeft een hoog risico op negatieve gevolgen voor de betrokkenen, en kennisgeving is vereist. De Toezichtcommissie en de klanten moeten op de hoogte worden gesteld van de inbreuk in verband met persoonsgegevens, met daarbij het dringende advies om voor alle accounts waar ze hetzelfde wachtwoord gebruiken, dit wachtwoord aan te passen. Ze moeten bij het inloggen op de website in kwestie ook worden gedwongen om hun wachtwoord voor de kwestie aan te passen. Daarbij moet worden gezorgd dat de nieuwe wachtwoorden worden aangemaakt door legitieme gebruikers, en niet door derden die de inloggegevens hebben bemachtigd.
- Een internetprovider biedt de gebruikers de mogelijkheid om details van hun account te zien, zoals onder andere historische zoekgegevens en vaak bezochte websites. Door een fout in de website had eenieder via een simpele truc de mogelijkheid om de accounts van andere gebruikers vrijelijk in te zien. Zonder een sluitende logging is hier niet vast te stellen of dat daadwerkelijk is gebeurd en welke gegevens dan zijn geraadpleegd. De gegevens kunnen worden gebruikt voor het versturen van spam aan de betrokkenen of voor telefonische verkoop of phishing. De buitgemaakte gegevens kunnen mogelijk ook worden gebruikt om profielen van de klanten op te stellen of hun gedragingen in kaart te brengen, wat gevoelige informatie aan het licht zou kunnen brengen. Deze inbreuk in verband met persoonsgegevens heeft een hoog risico op negatieve gevolgen voor de betrokkenen, en moet daarom aan hen en aan de toezichtcommissie worden gemeld.

Voorbeelden van gebeurtenissen die niet onder de meldplicht vallen, maar wel moeten worden ingeschreven in het logboek inbreuken:

- Een brief met daarin persoonsgegevens wordt naar een foutief adres gestuurd, en wordt ongeopend retour gezonden.
- Iemand laat een koffer met daarin persoonsgegevens achter in de trein. De koffer is voorzien van een deugdelijk slot, en komt via 'gevonden voorwerpen' ongeopend terug bij de rechtmatige eigenaar.
- Het zoekraken of hacken van de ledenadministratie van een sportvereniging zal doorgaans leiden tot het nodige ongemak voor verenging en leden, maar zal niet snel aanleiding geven tot een melding bij de betrokkene en/of de toezichtcommissie. Dit kan anders liggen als de sportvereniging zich bijvoorbeeld richt op personen met een specifieke levensovertuiging of seksuele geaardheid, of als er fraudegevoelige gegevens gelekt zijn.
- Als ziekenhuispersoneel gebruik maakt van het wachtwoord van een arts om toegang te krijgen tot medische persoonsgegevens, dan is er niet enkel sprake van een inbreuk in verband met persoonsgegevens, maar vooral ook van schending van interne voorschriften. In eerste instantie liggen dan disciplinaire maatregelen voor de hand.
-

Voorbeeld persoonsgegevens van gevoelige aard bij hack

Een hacker weet op de website van een lokale sportvereniging door middel van SQL-injectie, een veel voorkomende vorm van hacking, een bestand te bemachtigen met daarin de namen en e-mailadressen van een twintigtal abonnees op een nieuwsbrief.

Normaal gesproken gaat het hier niet om persoonsgegevens van gevoelige aard, in dit geval moet de inbreuk enkel ingeschreven worden in het logboek. Dit wordt anders als de sportvereniging of de nieuwsbrief zich richt op mensen met, bijvoorbeeld, een specifieke levensovertuiging, politieke voorkeur of seksuele geaardheid, dan moet de toezichtcommissie en/of betrokkene op de hoogte worden gebracht.

Voorbeeld kwetsbare groepen

Een hacker weet op de website van een buurthuis door middel van SQL-injectie, een veel voorkomende vorm van hacking, een bestand te bemachtigen met daarin de namen en e-mailadressen van een twintigtal abonnees op een elektronische nieuwsbrief. De nieuwsbrief richt zich op buurtbewoners van 65 jaar en ouder die bij het buurthuis een cursus volgen om vertrouwd te raken met het gebruik van computers en het internet. De aard van de doelgroep leidt hier tot extra risico's voor de betrokkenen. Gezien de onervarenheid van de betrokkenen met digitale communicatie bestaat er een aanzienlijk risico dat zij in zullen gaan op pogingen tot phishing. De inbreuk moet worden ingeschreven in het logboek, en gemeld aan de toezichtcommissie en betrokkene.

Voorbeeld persoonsgegevens die niet waren versleuteld op het moment dat de inbreuk plaatsvond:

Op de harde schijf van een laptop staat een bestand met persoonsgegevens. Het bestand zelf is niet versleuteld. De laptop wordt automatisch vergrendeld als deze enige tijd niet wordt gebruikt, en bij de automatische vergrendeling wordt de inhoud van de harde schijf versleuteld. De laptop

is in handen gekomen van een aanvaller die met technische middelen gebruik van het toetsenbord simuleert, en daardoor voorkomt dat de automatische vergrendeling in werking treedt en de gegevens op de harde schijf worden versleuteld. Deze inbreuk moet worden gelogd en gemeld aan de toezichtcommissie en betrokkene.

Voorbeeld waarin niet alle getroffen persoonsgegevens waren versleuteld, en de resterende persoonsgegevens niet waren versleuteld op het moment van de inbreuk:

Een werknemer geeft aan een derde de gebruikersnaam en het wachtwoord dat toegang geeft tot alle klantgegevens van alle klanten van het bestuur waar hij werkt. Het gaat onder meer om namen, adressen, e-mailadressen, telefoonnummers, toegangs- en andere identificatiegegevens (gebruikersnamen, gehashte wachtwoorden en klantnummers) en versleutelde betaalgegevens (waaronder rekeningnummers en creditcardgegevens). Om twee redenen moet de verantwoordelijke deze inbreuk in verband met persoonsgegevens melden aan de betrokkene:

- slechts een deel van de persoonsgegevens is versleuteld (de wachtwoorden en de betaalgegevens);
- de betaalgegevens zijn weliswaar versleuteld opgeslagen, maar als de derde met de verstrekte gegevens inlogt krijgt hij via de gebruikersinterface toegang tot de onversleutelde gegevens.

Tevens moet de inbreuk ingeschreven worden in het logboek en gemeld aan de toezichtcommissie.

Voorbeeld achterwege laten melding betrokkene bij encryptie:

Een laptop, met op de harde schijf een bestand met persoonsgegevens, is gestolen. De verantwoordelijke onderzoekt het incident, en komt tot de conclusie dat hij af mag zien van de melding aan de betrokkene. Zijn overwegingen daarbij zijn:

- bij de versleuteling van het bestand is gebruik gemaakt van combinatie van algoritme en sleutellengte die door het ENISA in een actuele (niet door een recentere publicatie achterhaalde) handreiking wordt beoordeeld als 'toekomst-vast voor de komende 10 tot 50 jaar;
- met betrekking tot het gebruikte algoritme en de implementatie daarvan zijn geen kwetsbaarheden bekend;
- de implementatie is met goed gevolg beoordeeld door een deskundige;
- het bestand zelf was versleuteld, dus de versleuteling was niet afhankelijk van automatische vergrendeling die in het specifieke geval mogelijk niet heeft gewerkt;
- de sleutel is niet gelekt;
- gezien de aard van de inbreuk in verband met persoonsgegevens, de verwerking en de gelekte gegevens is het restrisico acceptabel.

Maar de inbreuk moet wel worden ingeschreven in het logboek en gemeld aan de toezichtcommissie.

Voorbeeld achterwege laten melding i.v.m. bescherming betrokkene:

Er zijn gegevens gelekt over medische en psychosociale hulpvragen die kinderen buiten medeweten van hun ouders hebben gedaan. De verantwoordelijke meldt de inbreuk in verband met persoonsgegevens aan de toezichtcommissie, en beroept zich op de AVG om de mededeling aan de betrokkenen achterwege te kunnen laten. Reden is dat de ouders door de melding op de hoogte zouden kunnen raken van de hulpvraag.

Voorbeeld achterwege laten melding i.v.m. rechten en vrijheden verantwoordelijke:

Een beursgenoteerde onderneming is verwikkeld in een overname op het moment dat zich een grote inbreuk in verband met persoonsgegevens voordoet. De onderneming logt en meldt de inbreuk in verband met persoonsgegevens aan de toezichtcommissie, en beroept zich op de AVG, om de melding aan de betrokkene (voorlopig) achterwege te kunnen laten.

Voorbeeld melding aan de betrokkene en vervolgacties:

Een energieleverancier biedt zijn klanten een online account aan waarop ze kunnen inloggen om recente facturen en verbruiksinformatie te raadplegen. Het bedrijf ontdekt dat een derde zich illegaal toegang heeft verschaft tot de database met gebruikersnamen en wachtwoorden van de website. De wachtwoorden zijn niet adequaat versleuteld.

De energieleverancier onderneemt de volgende acties:

- hij informeert zijn klanten over de inbreuk in verband met persoonsgegevens. Hij beveelt daarbij aan om, voor alle accounts waar de klant hetzelfde wachtwoord gebruikt, dit wachtwoord te wijzigen;
- hij reset alle wachtwoorden en dwingt alle gebruikers om een nieuw wachtwoord op te geven. Hij doet dit op een veilige manier zodat hij zeker weet dat het zijn klanten zijn die een nieuw wachtwoord aanmaken, en niet een onbevoegde derde, en hij geeft hierbij ook aan waarom de klant een nieuw wachtwoord aan moet maken;
- hij past zijn systemen aan, zodat alle gebruikte wachtwoorden op een adequate manier worden versleuteld.

De inbreuk wordt wel gemeld aan de toezichtcommissie en gelogd.