OCMW AARSCHOT

UITTREKSEL UIT HET REGISTER VAN BESLUITEN VAN DE RAAD VOOR MAATSCHAPPELIJK WELZIJN VAN 08 februari 2024

Aanwezig: Isabelle Dehond, voorzitter van de Raad voor maatschappelijk welzijn **Bert Van der Auwera, wnd burgemeester** **Nicole Van Emelen, Annick Geyskens, Gerry Vranken, Stef Van Calster, Kurt Lemmens, leden van het vast bureau** **Betty Kiesekoms, Nico Creces, Mattias Paglialunga, Nele Pelgrims, Bart Dehaes, Bart Den Hondt, Leo Janssens, Ronny De Ryck, Koen Nijs, Cindy Symons, Marleen Verhaegen, Wendy De Rijck, Dries Vandenbroeck, Petra Vanlommel, Hannelore Castelein, Martine Verlinden, Hanne Goossens, Gerda Vandegaer, Pieter Schuermans, leden van de raad voor maatschappelijk welzijn** **Christi Van Calster, Algemeen directeur** **Verontschuldigd: Gwendolyn Rutten, Thomas Salaets, Dries Van Horebeek, leden van de raad voor maatschappelijk welzijn**	
Dienst:	**ICT**
Referentie:	**OCMW-raad/2024/007**
Budgethouder:	**OCMW-raad**
Onderwerp: Bijlage bij het arbeidsreglement: Policy beveiligingsincidenten en gegevenslekken	

De Raad,

Regelgeving

- het decreet van 22.12.2017 over het lokaal bestuur, zoals gewijzigd en de bijhorende besluiten en omzendbrieven van de Vlaamse regering;
- de wet van 29.07.1991 betreffende de uitdrukkelijke motivering van bestuurshandelingen;
- de wet van 11.04.1994 betreffende de openbaarheid van bestuur, zoals gewijzigd;
- het bestuursdecreet van 07.12.2018;
- het besluit van de Vlaamse Regering d.d. 30.03.2018 betreffende de beleids- en beheerscyclus van de lokale en provinciale besturen;

Feiten, context en motivering

- de wet van 19.12.1974 betreffende de betrekkingen tussen de overheid en de vakbonden van haar personeel;;
- het koninklijk besluit van 28.09.1984 tot uitvoering van de wet van 19.12.1974 tot regeling van de betrekkingen tussen de overheid en de vakbonden van haar personeel;
- het koninklijk besluit van 29.08.1985 tot aanwijzing van de grondregelingen in de zin van art 2, §1, 1° van de wet van 19.12.1974 tot regeling van de betrekkingen tussen de overheid en de vakbonden van haar personeel;
- de Wet van 04.08.1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk;
- de wet van 28.02.2014 tot aanvulling van de wet van 04.08.1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk wat de preventie van psychosociale risico's op het werk betreft, waaronder inzonderheid geweld, pesterijen en ongewenst seksueel gedrag op het werk;
- de wet van 28.03.2014 tot wijziging van het Gerechtelijk Wetboek en de wet van 04.08.1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk wat de gerechtelijke procedures betreft;
- het besluit van de raad voor maatschappelijk welzijn houdende de vaststelling van het arbeidsreglement voor het OCMW personeel op 24.07.2014, zoals laatst gewijzigd op 10.11.2022 en 15.12.2022;
- de Codex over het welzijn op het werk;
- de vergadering van het syndicaal overleg- en onderhandelingscomité stad/OCMW Aarschot, die heeft plaatsgevonden op maandagnamiddag 23.10.2023, waarop onder meer de policy beveiligingsincidenten en gegevenslekken werd besproken en waarvan het verslag wordt toegevoegd in bijlage aan deze beslissing;
- op 15.12.2023 werd, rekening houdend met de opmerkingen van de vakbonden, het aangepaste document Policy beveiligingsincidenten en gegevenslekken en de samenvatting doorgestuurd naar de vakorganisaties. Er werden geen bijkomende opmerkingen gegeven door de vakbonden.

Stemming

Goedgekeurd met eenparigheid van stemmen.

BESLUIT:

<u>Artikel 1</u>

De raad voor maatschappelijk welzijn keurt de onderstaande policy beveiligingsincidenten en gegevenslekken goed.

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.

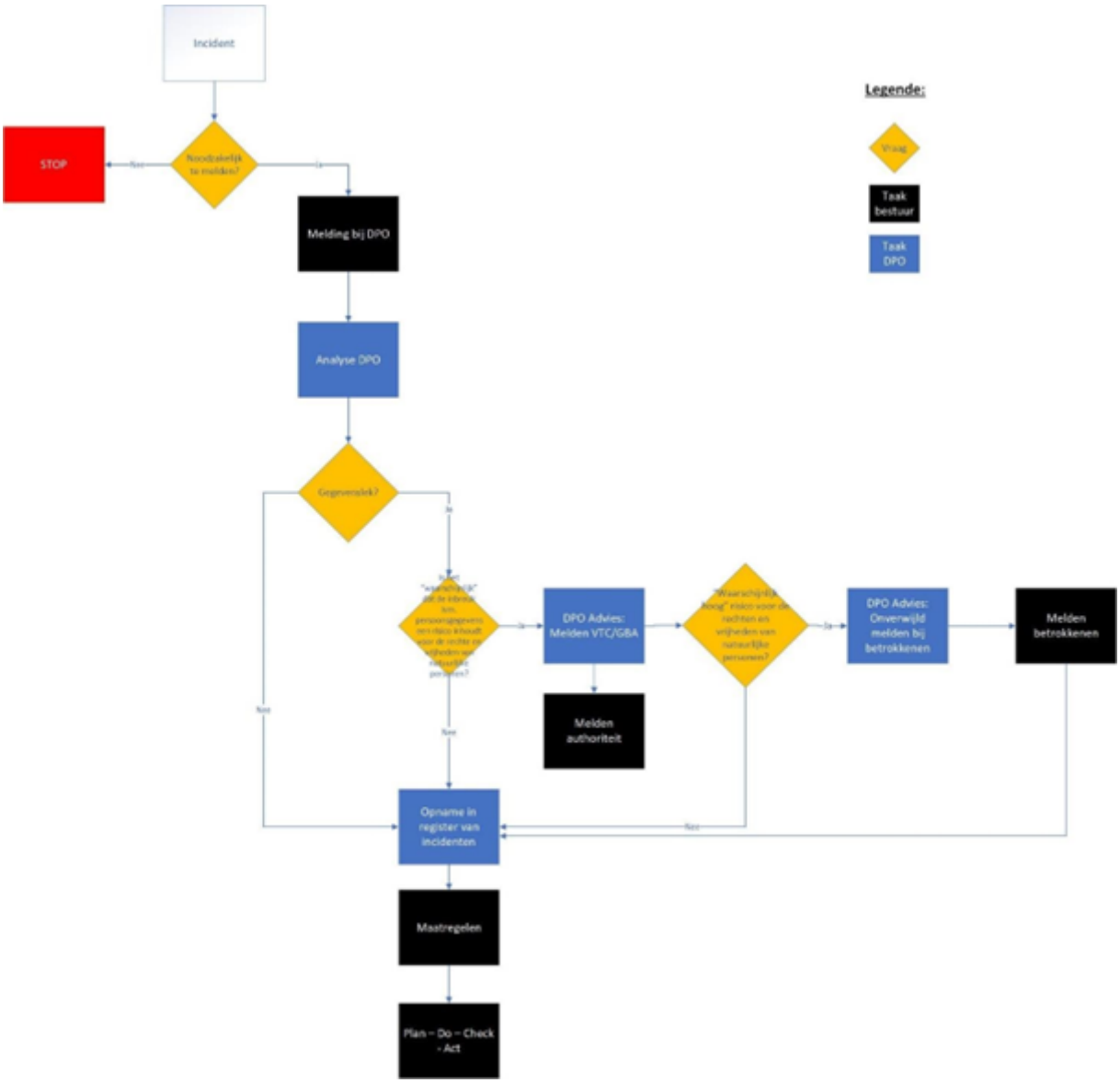
2. Definities

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



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; ð 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 hoeveelheid betrokkenen;
- De omvang van de inbreuk en de impact op de betrokkenen, waaronder: specifieke eigenschappen van de betrokkenen (zoals kinderen en ouderen);
- 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):

1. 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;
2. De naam en de contactgegevens van de DPO;
    1. De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
    2. 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-meldengegevenslek

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, o 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:
   1. onderwerp e-mail: beveiligingsincident
   2. Datum en tijdstip van de inbreuk;
   3. Vaststeller van de inbreuk en de contactgegevens;
   4. 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.

Artikel 2
De bijgaande samenvatting van de Policy beveiligingsincidenten en gegevenslekken wordt toegevoegd aan het arbeidsreglement voor het OCMW-personeel.

Aldus gedaan in zitting datum als hierboven.

De algemeen directeur,
Christi Van Calster

De voorzitter,
Isabelle Dehond