VERGADERING RAAD VOOR MAATSCHAPPELIJK WELZIJN 08.02.2024

VERSLAG

<u>Aanwezig :</u> 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
<u>Verontschuldigd :</u> Gwendolyn Rutten, Thomas Salaets, Dries Van Horebeek, leden van de raad voor maatschappelijk welzijn

OPENBAAR

<u>AGENDAPUNTEN MEEGEDEELD DOOR HET VAST BUREAU</u>

<u>O.2 FINANCIËLE DIENST</u>

Onderwerp: Rapportering door de financieel directeur over de voorafgaande krediet- en wetmatigheidscontrole van de voorgenomen financiële verbintenissen (VISUM) - Periode 01.07.2023 tot en met 31.12.2023

Regelgeving

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

Feiten, context en motivering
Gelet op het rapport - in bijlage - opgesteld door de financieel directeur over de voorafgaande krediet- en wetmatigheidscontrole van de voorgenomen financiële verbintenissen (VISUM) voor de periode 01.07.2023 tot en met 31.12.2023.

BESLUIT :
<u>Enig artikel</u>
De raad voor maatschappelijk welzijn neemt kennis van de rapportering - in bijlage - door de financieel directeur over de voorafgaande krediet- en wetmatigheidscontrole van de voorgenomen financiële verbintenissen (VISUM) voor de periode 01.07.2023 tot en met 31.12.2023.

<u>O.6 PERSONEEL EN ORGANISATIE</u>

Onderwerp: Vaststelling van de bijlage aan het arbeidsreglement inzake alcohol- en drugsbeleid

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;
- 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;
- de Codex over het welzijn op het werk;
- 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;

Feiten, context en motivering
In zitting van 14.05.2018 keurde de gemeenteraad de aanpassingen aan de rechtspositieregeling en het arbeidsreglement voor het gemeentepersoneel goed inzake alcohol- en drugsbeleid (toevoeging bijlage 13).
In het kader van de beslissing van het college van burgemeester en schepenen dd. 03.04.2017 houdende de uitwerking van een alcohol- en drugsbeleid en de bepalingen opgenomen in ons arbeidsreglement, in het bijzonder deze van artikel 456 inzake alcohol en drugs en voetnoot 47 waarin bepaald wordt dat 'de *concrete uitwerking van het alcohol- en drugbeleid voorzien wordt in het licht van de bepalingen van CAO 100 (collectieve arbeidsovereenkomst betreffende een preventief alcohol- en drugbeleid in de onderneming) die reeds van toepassing zijn voor de privé-sector (en eventuele latere wijzigingen),* werd een werkgroep 'alcohol -en drugsbeleid' samengesteld, belast met de uitwerking van het alcohol- en drugsbeleid en bestaande uit de preventieadviseur psychosociale aspecten van de arbeidsgeneeskundige dienst (PREMED), afgevaardigden van de representatieve vakbonden en medewerkers van de stad. Tijdens diverse bijeenkomsten in de periode oktober 2017-januari 2018 werd een voorstel terzake uitgewerkt.
Voorliggend voorstel is een actualisatie van dit alcohol- en drugsbeleid dat ook toepasbaar wordt voor het OCMW personeel.
Het voorstel werd goedgekeurd door het vast bureau in zitting van 31.03.2023 en door de vakbonden tijdens de vergadering van het syndicaal overleg- en onderhandelingscomité van 17.04.2023 waarvan het protocol wordt toegevoegd in bijlage.
Aan de raad voor maatschappelijk welzijn wordt dan ook voorgesteld om hiermee in te stemmen.

Stemming
Goedgekeurd met eenparigheid van stemmen.

BESLUIT :
Artikel 1
Bijgevoegde bijlage inzake alcohol- en drugsbeleid wordt goedgekeurd. Dit document wordt toegevoegd aan het arbeidsreglement voor het OCMW personeel.

Artikel 2
Dit besluit wordt ter kennis gebracht van het OCMW personeel. De leidinggevenden worden gelast met de verdere communicatie en informatie hieromtrent naar hun medewerkers toe.

Onderwerp: Bijlage bij het arbeidsreglement: ICT-richtlijn

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 plaatsvond op maandagnamiddag 23.10.2023, waarop de voorliggende ICT richtlijn werd besproken en waarvan het verslag wordt toegevoegd in bijlage aan deze beslissing;
- op vrijdag 15.12.2023 werd, rekening houdend met de opmerkingen van de vakbonden, het aangepaste document ICT richtlijn doorgestuurd naar de vakorganisaties ter goedkeuring. Er werden geen bijkomende opmerkingen gegeven door de vakbonden.

Stemming
Goedgekeurd met eenparigheid van stemmen.

BESLUIT :
Artikel 1
De raad voor maatschappelijk welzijn keurt onderstaande de ICT-richtlijn goed.

1 Inleiding
De stad Aarschot, OCMW Aarschot en AGB Aarschot *(hierna: het lokale bestuur)* stellen heel wat ICT-middelen ter beschikking voor de dagelijkse werking van de verschillende diensten. Het gebruik hiervan wordt sterk aangemoedigd als ondersteuning en optimalisering van de kernactiviteiten. Het gebruik van ICT-middelen is volledig ingebed in de dagelijkse werking van het lokale bestuur. Defecten, hindernissen of uitval zijn nefast voor de dagelijkse werking. Het lokale bestuur heeft wettelijke en morele verplichtingen om veiligheidsmaatregelen te nemen met betrekking tot deze ICT-middelen en de informatie die via deze ICT-middelen verloopt.
Het doel van dit document is om een richtlijn voor ethisch en veilig gebruik van de ter beschikking gestelde middelen te zijn. Daarmee wordt een kader gecreëerd waarbinnen medewerkers van het lokale bestuur kunnen werken.
Wanneer er iets niet duidelijk is, is het de verantwoordelijkheid van de gebruiker om uitleg te vragen aan de ICT-dienst.

2 Toepassingsgebied
2.1 Wat zijn ICT-middelen?
Het lokale bestuur beheert informatie- en communicatietechnologieën voor de uitoefening van de dagelijkse werking, veralgemeend onder de noemer 'ICT-middelen'. Deze technologieën kunnen worden opgesplitst in:
- **netwerkapparatuur (network hardware)**
  alle toestellen, kasten en bekabeling die nodig zijn om het netwerk te maken en te beheren;
- **systeemapparatuur (system hardware)**
  alle toestellen, kasten en bekabeling die nodig zijn voor het lokaal faciliteren van software, opslag en back-ups;
- **apparatuur op gebruikersniveau (client hardware)**
  alle toestellen die gebruikt worden door medewerkers, zoals: laptops/computers, randapparatuur (printers, USB-sticks, badgelezers, …), telefoons of
  gsm-toestellen (lijst is niet exhaustief);
- **informatie op de apparatuur (data)**
  alle data die verstuurd, opgeslagen, ontvangen of geïnstalleerd is op de hierboven opgesomde apparatuur, onafhankelijk van de bron, o.a.:
  - metadata van bestanden;
  - inhoud van bestanden;
  - login gegevens (gebruikersnamen en wachtwoorden);
  - e-mails;
  - gedownloade en geüploade gegevens;
  - software of geïnstalleerde programmatuur.

Wanneer in dit document wordt verwezen naar 'ICT-middelen' dan gaat het, tenzij anders gespecifieerd, over alle hierboven beschreven technologieën.

2.2 Op wie is deze richtlijn van toepassing?

Deze ICT-richtlijn is van toepassing op alle categorieën van gebruikers die toegang hebben tot de ICT-middelen van het lokale bestuur waaronder: personeelsleden, mandatarissen, externe medewerkers, consultants, stagiairs, vrijwilligers.
In dit document wordt een onderscheid gemaakt tussen drie groepen medewerkers:

- **Gebruikers:**

Deze groep omvat iedereen die toegang heeft tot ICT-middelen.
Toegang wordt hier gebruikt in de breedste zin van het woord. Zodra er mogelijkheid is om ICT-middelen aan te raken, te gebruiken of te beïnvloeden is er sprake van toegang, zelfs al is het gebruik van de middelen niet verbonden aan de job inhoud.

- **Leidinggevenden:**

Deze groep omvat uitsluitend de diensthoofden, de departementshoofden, de leidinggevenden, de decretale graden.

- **ICT-dienst:**

Deze groep omvat uitsluitend iedereen die werkt bij of voor de ICT-dienst.

3 Gebruik

3.1 Ingebruikname

Voor het gebruik van de middelen beschreven in het toepassingsgebied moet elke gebruiker een gebruiksovereenkomst ondertekenen. Deze overeenkomst tussen de gebruiker en het lokale bestuur beschrijft de ontvangen middelen en hun staat op het moment van ingebruikname.
De middelen die door het lokale bestuur ter beschikking worden gesteld blijven eigendom van het lokale bestuur.

3.2 Teruggave

De verkregen middelen moeten onder volgende omstandigheden terug worden overgemaakt aan het lokale bestuur:

- bij het beëindigen van de werkrelatie en uiterlijk op de laatste werkdag maakt de gebruiker op eigen initiatief een afspraak met de ICT-dienst voor het inleveren van de verkregen middelen;
- op vraag van de algemeen directeur.

Op het moment van teruggave worden de verkregen middelen vergeleken met de beschreven staat in bijlage 1 van de gebruiksovereenkomst. Hierbij wordt rekening gehouden met normale sporen van gebruik. Van elke gebruiker verwachten we dat hij/zij zorgvuldig omgaat met de verkregen middelen en bereid is verantwoording af te leggen over het gebruik van deze bedrijfsmiddelen. Inbreuken kunnen leiden tot sancties zoals bepaald in de rechtspositieregeling of het arbeidsreglement.

3.3 Accountblokkering

De verkregen toegangsrechten worden standaard in de volgende gevallen stopgezet:

- bij het beëindigen werkrelatie;
- in geval van langdurige ziekte;
- bij vermoeden van problemen in verband met veiligheid of misbruik;
- bij langdurig niet inloggen of niet aanpassen van wachtwoord;
- en/of langdurige afwezigheid.

Uitzonderingen op deze blokkering kunnen worden verleend door de algemeen directeur.

4 Verantwoordelijkheden

Alle gebruikers hebben de verantwoordelijkheid om te werken in overeenstemming met de regels en principes van deze ICT-richtlijn. De risico's rond het beveiligen van de ICT-middelen kunnen alleen tot een minimum herleid worden wanneer iedereen zich houdt aan de richtlijn. De verantwoordelijkheid om de ICT-middelen veilig te houden is een zaak van elke gebruiker (gebruikers, leidinggevenden, ICT-dienst).
Alleen de ICT-dienst of aangestelde derden mogen ICT-middelen installeren, demonteren, verplaatsen of wijzigen. Er mag geen ander materiaal gebruikt worden dan de ICT-middelen die door de ICT-dienst en door erkende leveranciers ter beschikking werden gesteld.
Enkel de software die rechtmatig aangekocht werd, mag gebruikt worden. Het gebruik van deze software moet toegelaten zijn met het oog op het specifieke karakter van de opdrachten en goedgekeurd zijn door de ICT-dienst.
Aansluitingen op externe netwerken zoals het internet, die niet toegelaten zijn, of die geïnstalleerd noch geconfigureerd zijn door de ICT-dienst, zijn verboden.

4.1 Gebruikers

4.1.1 Veiligheid van de ICT-middelen

4.1.1.1 Bewustzijn

Verantwoord gebruik van ICT-middelen begint bij een bewustzijn van de verschillende soorten gevaren en van de afgesproken procedures.
Daarom is het belangrijk dat de gebruiker de:

- ICT-richtlijn en -procedures goed volgt;
- de gevaren inziet die het onverantwoord omspringen met data en login-gegevens met zich meebrengt;
- de kwetsbaarheden inziet die het delen van ICT-middelen met zich meebrengt;
- een kritische blik heeft op ontvangen communicatie of verkregen hardware van onbekende bronnen.

In het kader van dit bewustzijn kan de ICT-dienst beslissen om onaangekondigde campagnes te voeren waarbij gebruikers getest worden op kennis en alertheid met focus op veiligheid.

4.1.1.2 Cybercriminaliteit

Cybercriminaliteit is zeer winstgevend wat meteen de hoge frequentie van de aanvallen verklaart. De criminelen spelen op het scherpst van de snee en passen zich aan naargelang de beveiliging verandert. Een volledige bescherming tegen aanvallen kan nooit gegarandeerd worden en net daarom is het belangrijk om in te zetten op preventie en informeren. Twee van de meest voorkomende soorten aanvallen zijn:

Malware

Malware is de verzamelnaam voor alle kwaadaardige software zoals virussen, spyware, ransomware, enzovoort. De verspreiding van malware gebeurt via allerlei kanalen zoals e-mail, websites, instant messaging of door middel van fysieke toegang. Onder andere door het downloaden en openen van een bijlage, door het klikken op een link naar een besmette website of door het inpluggen van een onbekende usb-stick kunnen de ICT-middelen van het lokale bestuur besmet worden met deze malware.

Phishing

Phishing is het 'hengelen' naar (vertrouwelijke) informatie van de gebruiker of het lokale bestuur. Criminelen proberen door het nabootsen van vertrouwde websites, e-mails of telefoongesprekken deze informatie te ontvreemden van de gebruiker. Doorgaans gaat dit om login-informatie, bankgegevens of vertrouwelijke documenten.

Om aanvallen van cybercriminelen zo goed mogelijk te voorkomen is het belangrijk dat de gebruiker:

- aandachtig is bij het verwerken van e-mails, goed kijkt naar de afzender en zichzelf de vraag stelt: "Verwacht ik een e-mail of een bestand van deze persoon?";
- niet klikt op links van niet vertrouwde bronnen;
- bestanden van niet vertrouwde bronnen niet opent.

In bovenstaande gevallen en in geval van twijfel is het verplicht de ICT-dienst te verwittigen.

4.1.1.3 Gegevenslekken

Er wordt gesproken over een gegevenslek in situaties waarin persoonsgegevens dreigen ongeoorloofd te worden openbaar gemaakt, verloren te gaan, vernietigd of gewijzigd te worden.

Wat 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 emailadres, een vingerafdruk, een IP-adres,…of het combineren van deze of andere gegevens.
- Het gaat niet alleen over gegevens die te maken hebben met de persoonlijke levenssfeer (privacy) van personen, aar ook over gegevens die te maken hebben met het professionele of openbare leven van een persoon.

Wanneer een gebruiker een gegevenslek vaststelt is het van kritisch belang een melding te maken van het incident via privacy@aarschot.be.

4.1.1.4 Richtlijnen rond wachtwoorden

Het wachtwoord is de eerste beveiliging van een account. Het is dus belangrijk dat er met de hoogste voorzichtigheid wordt omgesprongen met wachtwoorden:

- wachtwoorden zijn persoonlijk, deel ze nooit met anderen;
- zorg dat niemand toekijkt bij het ingeven van je wachtwoord;
- gebruik voor elke account die je aanmaakt (Windows, e-mail, applicaties, online diensten, …) een ander wachtwoord. Gebruik je professionele wachtwoorden niet voor je privé accounts;
- het opslaan van wachtwoorden is slechts toegestaan wanneer dit gebeurt in een versleutelde wachtwoordkluis die is goedgekeurd door de ICT-dienst, gebruik dus niet de functie "wachtwoord onthouden" in je browser;
- het opschrijven of afdrukken van wachtwoorden is niet toegestaan;
- iedere gebruiker is verantwoordelijk en aansprakelijk voor alles wat onder hun loginnaam en wachtwoord gebeurt.

Wachtwoorden van alle gebruikers verlopen automatisch na drie maanden. Na het verlopen kiest de gebruiker een nieuw wachtwoord zonder logische opvolging van het vorige wachtwoord en uniek in vergelijking met andere accounts.

4.1.1.4.1 Toepassingsgebied

De richtlijnen rond wachtwoorden worden afgedwongen op de volgende toepassingsgebieden:

- toegang tot de ICT-middelen (computer, mobiel toestel van het lokale bestuur, de ter beschikking gestelde software);
- toegang tot de Microsoft 365 omgeving.

Het bestuur of een hogere overheid kan er ook voor kiezen om deze richtlijnen af te dwingen op volgende toepassingen::

- alle externe toepassingen (gebruikersbeheer Vlaanderen, Social Security, RRNAdmin, …);
- alle interne toepassingen die gebruikt worden op de verschillende diensten (Alfa, Bravo, Mercurius, Echo, …).

Ook als dit (nog) niet verplicht gesteld is, blijft het ten sterkste aan te raden dit zelf toe te passen op:

- alle externe toepassingen (gebruikersbeheer Vlaanderen, Social Security, RRNAdmin, …);
- alle interne toepassingen die gebruikt worden op de verschillende diensten (Alfa, Bravo, Mercurius, Echo, …);
- alle persoonlijke accounts die niets met het bestuur te maken hebben, dit voor je algemene online veiligheid.

4.1.1.4.2 Kiezen van een wachtwoord

De sterkte van een wachtwoord wordt in de eerste plaats beïnvloed door de lengte, hoe langer een wachtwoord hoe beter. De ICT-dienst raadt aan om een wachtwoordzin te gebruiken in plaats van een moeilijk te onthouden combinatie van letters en tekens.
De volgende vereisten zijn van toepassing:

- een lengte van minimum 12 karakters;
- het gebruik van hoofdletters;
- het gebruik van kleine letters;
- het gebruik van cijfers;
- het gebruik van speciale tekens zoals: ! @ # % ( ];
- gebruik geen voor de hand liggende namen, woorden of getallen. Verwerk je naam, geboortedatum, gebruikersnaam of dienst niet in je wachtwoord.

Voorbeelden van sterke wachtwoorden:

- wEntelteef;57hoplakEE615
- 6504hond,Put-feesttaart!
- Erwaseensaldaareenvlindermetgrotebaard9846&$
- #a9*!F59Hyfe&5cn
- wv@!L$SUXH23!7Br

Voorbeelden van enorm zwakke wachtwoorden:

- 123456
- 123456789
- qwerty
- password
- 3200wachtwoord!
- Login-3200

4.1.1.4.3 Wijzigen van wachtwoorden

Het is verplicht en afgedwongen om het Microsoft-account wachtwoord minstens elke drie maanden te wijzigen. Daarnaast kan de ICT-dienst vragen om onmiddellijk je wachtwoord te wijzigen wanneer er bijvoorbeeld een inbraak of een afwijking van de afspraken wordt vastgesteld. Je kan steeds op eigen initiatief je wachtwoord wijzigen door na het aanmelden op je computer de toetsencombinatie CTRL+ALT+DEL te gebruiken en de optie “Wachtwoord wijzigen” te selecteren, en je bent verplicht dit te doen wanneer je het minste vermoeden hebt dat iemand je wachtwoord kent.

4.1.1.5 Multi Factor Authentication (MFA)

Multi Factor Authentication (MFA) is een beveiligingsmaatregel waarbij gebruikers hun identiteit moeten bevestigen bij het inloggen door middel van een prompt van een smartphone applicatie, of een hardware authenticatie toestel.
Elke gebruiker is verplicht gebruik te maken van MFA en zal zijn/haar identiteit minstens elke week moeten bevestigen via het MFA-systeem.

4.1.1.6 Inbraak

Wanneer een externe persoon of systeem ongeoorloofd toegang krijgt tot de systemen van het lokale bestuur dan spreken we over inbraak. Inbraak in de ICT-middelen kan bijvoorbeeld gebeuren door het verkrijgen van de logingegevens van een gebruiker of door zwakke punten in beveiliging van de systemen te misbruiken.
De gebruiker neemt verplicht minstens de volgende maatregelen om inbraak op de ICT-middelen te voorkomen:

- het vergrendelen van de systemen bij het verlaten van de ruimte (Windows-toets + L);
- het volgen van de afspraken rond wachtwoorden;
- de verkregen ICT-middelen niet door derden laten gebruiken.

4.1.1.7 Diefstal of verlies

Wanneer een malafide persoon permanente fysieke toegang heeft tot de systemen van het lokale bestuur zijn er veel meer mogelijkheden om de systemen aan te vallen. Het is dus van enorm belang om de ontvreemding van ICT-middelen van het lokale bestuur te voorkomen.
De gebruiker neemt verplicht minstens de volgende maatregelen om diefstal van de ICTmiddelen te voorkomen:

- het nooit onbeheerd achterlaten van de toestellen in publieke ruimtes of op kantoor. Berg je laptop steeds op;
- het afsluiten van onbemande ruimtes wanneer er ICT-middelen achterblijven.

In geval van diefstal of verlies dient de gebruiker dit op het moment van vaststelling te melden aan de ICT-dienst. De gebruiker dient diefstal ook onmiddellijk aan te geven bij de politie en het bewijs van aangifte te bezorgen aan de ICT-dienst op het moment van ontvangst.

4.1.1.8 Beschadiging

In geval van beschadiging meldt de gebruiker de schade onmiddellijk na het feit of de vaststelling en ten laatste binnen de 48 uur aan de ICT-dienst en stelt een verklaring op over de omstandigheden van de beschadiging. Het schadebedrag zal ten laste van de medewerker teruggevorderd worden bij herhaling van schade, verlies of diefstal. Bij duidelijk aantoonbare nalatigheid zal het schadebedrag meteen teruggevorderd worden ten laste van de medewerker.

4.1.1.9 Gebruik voor privédoeleinden

De ICT-middelen van het lokale bestuur worden ter beschikking gesteld van de gebruikers om de professionele activiteiten uit te voeren. Gezien het gebruik van deze middelen echter zo alledaags is geworden, is incidenteel gebruik voor privédoeleinden toegestaan wanneer dit redelijk blijft, geen onwettelijk gebruik is en niet in strijd is met deze richtlijn.
Concreet is persoonlijk gebruik enkel toegestaan wanneer:

- dit zelden en van korte duur is;
- dit geen impact heeft op de plichten van de gebruiker;
- dit geen impact heeft op de uitvoering van je taken en de productiviteit van jezelf en die van je collega-medewerkers niet in het gedrang brengt;
- er geen extra kosten zijn voor het lokale bestuur;
- het netwerk niet overbelast wordt door onnodig internetverkeer;
- het gebruik niet in strijd is met de rechtspositieregeling/arbeidsreglement, deze of andere richtlijnen;
- het gebruik niet in strijd is met de GDPR- of andere relevante wetgevingen.

4.1.2 Opslag en versturen van informatie

4.1.2.1 Lokale opslag

De gebruiker is verantwoordelijk voor de juiste en meest veilige opslag van informatie. Dit wil zeggen dat werkgerelateerde bestanden moeten worden opgeslagen op netwerkschijven en in de juiste map. Alleen op die manier kan een back-up gegarandeerd worden.

4.1.2.2 Cloud opslag en versturen van informatie

Het online opslaan en versturen van informatie wordt uitsluitend toegestaan via diensten van Microsoft 365 zoals Teams, OneDrive of Sharepoint. Het gebruik van alternatieven is ten strengste verboden.

4.1.3 Digitale correspondentie

4.1.3.1 E-mail

Mailboxen op de domeinen van het lokale bestuur en op naam van de gebruiker worden als vertrouwelijk behandeld maar blijven eigendom van het lokale bestuur. Het gebruik van de officiële e-mailadressen van het lokale bestuur is enkel toegestaan voor professionele doeleinden voor zover:

- de uitgewisselde informatie ondubbelzinnig gelinkt is aan je taken;
- in de e-mail geen vertrouwelijke informatie wordt meegedeeld waartoe je geen bevoegdheid hebt;
- de geldende stijlregels worden nageleefd.

Bij een geplande afwezigheid moet je steeds je “out-of-office reply” vooraf inschakelen. Je voorziet daarbij een korte afwezigheidsboodschap waarin op een professionele manier de aanvang en het einde van je afwezigheidsperiode vermeld staat. Vermeld daarbij ook het emailadres en/of telefoonnummer van de collega(‘s) van de betrokken dienst die men kan contacteren tijdens jouw afwezigheid.
Bij een onvoorziene afwezigheid is je direct leidinggevende of elke andere door jou aangestelde vertrouwenspersoon ertoe gerechtigd om je mailbox te controleren op inkomende e-mails. Het doel hiervan is de lopende zaken en de continuïteit van de dienstverlening te kunnen garanderen.
Deze toegang is evenwel beperkt tot e-mails die noodzakelijk zijn om de continuïteit van de dienst te waarborgen.
Wanneer je tewerkstelling, mandaat, contract of aanstelling stopt, wordt er van gebruikers verwacht dat ze correspondenten laten weten dat ze de organisatie verlaten met vermelding van de contactgegevens van de dienst of collega’s. Diezelfde informatie dient eventueel in een automatisch afwezigheidsbericht te worden opgenomen en moet ingeschakeld worden vóór vertrek met ingangsdatum na vertrek mits toestemming van het diensthoofd.
Na het vertrek zal de toegang tot de mailboxen voor de gebruiker worden stopgezet en de mailbox verwijderd of kan mits schriftelijke toestemming van de gebruiker toegang worden verleend aan het diensthoofd. Mits toestemming van de gebruiker én het diensthoofd kan ook toegang worden verleend aan een collega voor een maand. Hierna zal de individuele mailbox verwijderd worden. Mits akkoord van de gebruiker kan deze periode verlengd worden tot maximum 3 maanden.
Om continuïteit te garanderen is het de verantwoordelijkheid van de gebruikers en de dienst waar ze tewerkgesteld zijn om vóór het geplande vertrek door de ontvangen e-mails en bestanden te gaan om ze te verwijderen, op te slaan in een gedeelde map of door te sturen naar collega’s.

4.1.3.2 Microsoft 365

Microsoft 365 accounts gekoppeld aan een Microsoft 365 licentie van het lokale bestuur en op naam van de gebruiker worden als vertrouwelijk behandeld maar blijven eigendom van het lokale bestuur. Het is niet toegelaten om Microsoft 365 accounts van het lokale bestuur te gebruiken voor commerciële doeleinden.
Zodra het arbeidscontract of de aanstelling van de gebruiker eindigt zal de toegang tot de Microsoft 365 account voor de gebruiker onmiddellijk worden stopgezet.

4.1.4 Draadloze netwerken

Het lokale bestuur biedt verschillende draadloze Wifi netwerken aan die gebruikt kunnen worden om te verbinden met het bedrijfsnetwerk of het internet. Voor de algemene veiligheid van de middelen is het belangrijk dat het juiste netwerk voor het juiste toestel wordt gebruikt.

Radius

- Rechtstreekse toegang tot het bedrijfsnetwerk en internet.
- Alleen toegelaten voor toestellen in beheer van de ICT-dienst.
- De gebruiker moet toelating vragen om hiermee te kunnen verbinden.

Mobiel

- Alleen toegang tot het internet.
- Alleen toegelaten voor mobiele toestellen van medewerkers.
- Niet toegelaten voor derden, deel het wachtwoord met niemand.

Hotspot (gasten-netwerk)

- Alleen toegang tot het internet
- Toegelaten voor externen

Het is niet toegelaten om data te versturen over netwerken die niet beveiligd zijn, zoals een Wifinetwerk zonder wachtwoord.

4.1.5 Meldplicht

Het is van groot belang om de ICT-dienst op de hoogte te houden van de status van de ICT-middelen. Wanneer er een aanval gebeurt op de systemen van het bestuur is tijd een belangrijk middel om erger te voorkomen, maar ook in geval van schade kan het nodig zijn om snel te handelen in het kader van de garantie. Als je zelf geen contact kan opnemen met de bevoegde dienst moet je de melding maken bij je diensthoofd die de verantwoordelijkheid heeft om de informatie daarna over te maken aan de ICT-dienst.

Het is verplicht om de ICT-dienst onmiddellijk op de hoogte te brengen bij:

- de minste argwaan over een ontvangen e-mail of bijlage;
- het kleinste vermoeden van actieve malware;
- het verliezen of ontvreemd zijn van een ICT-middel;
- de minste schade aan een ICT-middel;
- het vermoeden van een inbreuk op deze richtlijn;
- het besef van een gegevenslek;

4.1.5.1 Meldpunten

Meldingen aan de ICT-dienst dienen te gebeuren op de hieronder in prioritaire vermelde volgorde:

1. via het ICT support portaal;
2. telefonisch via 016 550 325 of 016 550 369 wanneer je niet aan het support portaal kan.

Meldingen in verband met gegevenslekken en inbraken op vlak van privacy dienen te gebeuren via privacy@aarschot.be.

4.2 Leidinggevenden

Alle hierboven beschreven artikels die van toepassing zijn op de gebruiker zijn ook van toepassing op de leidinggevenden. Daarnaast hebben de leidinggevenden de volgende extra verantwoordelijkheden:

4.2.1 Voorbeeldfunctie

De leidinggevende geeft het goede voorbeeld in het gebruik van de middelen en het naleven van deze richtlijn. Als leidinggevende heb je dus een voorbeeldfunctie. Daarnaast kijk je ook toe op het naleven van deze richtlijn door de medewerkers van je team.

4.2.2 Toezicht

Leidinggevenden zijn de eerste lijn in toezicht op de gebruikers. Ze zorgen dat deze richtlijn wordt nageleefd en helpen hun medewerkers om ze correct toe te passen. Het is dus belangrijk dat de problemen die gebruikers hebben, opgevolgd worden en indien nodig besproken worden met de ICT-dienst. Daarnaast is het van belang om inbreuken op deze richtlijn onmiddellijk op te volgen zodat de veiligheid van de systemen gewaarborgd blijft. Wanneer de leidinggevenden een inbreuk vaststellen, melden ze dit bij de ICT-dienst om soortgelijke inbreuken in de toekomst te voorkomen.

4.2.3 Toegangsbeheer

Elke toegangsrecht voor toepassingen en bestanden in gebruik of opgeslagen bij het lokale bestuur moet worden aangevraagd bij de ICT-dienst en worden gemotiveerd door de leidinggevende van de aanvrager.

4.3 ICT-dienst

De ICT-dienst heeft als doel de werking van het lokaal bestuur te ondersteunen en te faciliteren. Concreet wil dit zeggen dat de ICT-dienst naast het zorgen voor passende apparatuur ook instaat voor de beveiliging en de operationele werking van de middelen. De hierboven beschreven afspraken (4.1) vormen de basis voor het verzekeren van de dagelijkse werking.

4.3.1 Bewustmaking en opleidingen

Om de impact van de hierboven beschreven afspraken zo beperkt mogelijk te houden en het bewustzijn van de gebruikers te vergroten, zal de ICT-dienst in de mate van het mogelijke opleidingen voorzien en steekproeven organiseren.

5 Ongeoorloofd gebruik

Het lokaal bestuur laat het gebruik van de ICT-middelen niet toe (lijst is niet exhaustief):

- wanneer het in strijd is met de in hoofdstuk 4 beschreven verantwoordelijkheden;
- om informatie op te slaan of te verspreiden die:om vertrouwelijke informatie door te geven aan personen die niet gerechtigd zijn om deze informatie te ontvangen;
    - het imago, de morele of de economische belangen van het lokale bestuur kan schaden;
    - beledigend, lasterlijk, aanstootgevend of discriminerend is;
    - schade kan toebrengen aan derden;
    - strijdig is met de openbare orde en openbare zeden;
    - gevaar voor verslaving vormt;
    - aanzet tot discriminatie wegens ras, etnische afkomst, geslacht, geloof, enz..
    - om software te installeren of te gebruiken waarvoor de ICT-dienst geen toestemming heeft verleend;
    - om acties te ondernemen die de beveiliging van ICT-middelen in het gedrang kunnen brengen zoals bijvoorbeeld:
        - het omzeilen van systeem- netwerkbeveiliging;

- het ontwerpen of installeren van malware;
- ongeoorloofde toegang forceren;
- het netwerk afluisteren.

- om eigen ICT-middelen aan te sluiten op hardware van het lokale bestuur zoals bijvoorbeeld:
  - smartphones en tablets;
  - laptops;
  - randapparatuur;
  - om intern ontwikkelde programma's te commercialiseren en/of voor persoonlijke doeleinden te gebruiken;
  - USB-sticks.
- in het buitenland zonder voorafgaande toestemming van de leidinggevende en de ICTdienst.

6 Aansprakelijkheid

Gebruikers zijn persoonlijk aansprakelijk voor alle handelingen die worden uitgevoerd met hun verkregen gebruikersaccount. De gebruiker kan te allen tijde om verantwoording worden gevraagd over het gebruik van de ICT-middelen.

7 Toezicht en controle

7.1 Principieel recht op controle

Binnen de wettelijke grenzen kan het lokale bestuur controle uitoefenen op gegevens die een gebruiker opslaat, verstuurt of ontvangt. Dit past binnen de opdracht van het lokale bestuur en haar doelstellingen.

7.2 Toepassingsgebied

De controle is van toepassing op:

- het gebruik van internet;
- het gebruik van e-mail;
- het gebruik van andere professionele communicatiemiddelen zoals Microsoft Teams;
- de informatie en bestanden die gebruikers doorsturen via of publiceren op internet;
- de informatie en bestanden die gebruikers opslaan.

7.3 Doel van de controle

Controle door de ICT-dienst is alleen mogelijk als een van de volgende vijf doelen worden nagestreefd:

1) het voorkomen en vaststellen van ongeoorloofde feiten, lasterlijke feiten of feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden.

Dat zijn feiten als:

- het kraken van computers, waaronder het op illegale manier kennis nemen van persoonsgegevens of vertrouwelijke medische bestanden;
- het raadplegen van sites die
  - zich tegen de grondbeginselen van de democratie en de rechtstaat keren, zoals sites die verband houden met racisme, terrorisme of discriminatie;
  - anderen kunnen kwetsen of beledigen, zoals sites met racistische of seksistische onderwerpen, pornografisch materiaal of schokkende foto's;
  - een gevaar voor verslaving vormen zoals goksites en pornografische sites;
  - het privéleven van iemand aantasten.

2) het beschermen van bepaalde informatie. De algemene regel is 'openbaarheid van bestuur'. Er zijn echter uitzonderingen op die regel, omdat bepaalde informatie niet geschikt is om algemeen gedeeld te worden. Een controle door de werkgever is mogelijk als de te beschermen belangen van het lokale bestuur, zoals bepaald in de vigerende regelgeving rond openbaarheid van bestuur, worden geschaad. De werkgever kan ook controle doen op de praktijken die in strijd zijn met die belangen.

4) het te goeder trouw naleven van deze ICT-richtlijn en andere richtlijnen voor het gebruik van onlinetechnologieën.

5) het verzekeren van de continuïteit van de dienstverlening bij overlijden, onvoorziene afwezigheid of vertrek van een werknemer.

De gegevens die verzameld en verwerkt worden voor een controle met een van de vijf bovenstaande doelen, kunnen niet gebruikt worden voor een controle met andere doeleinden. Als een wettelijke bepaling dat toestaat of oplegt, kan de ICT-dienst de gegevens voor een ander doel gebruiken, inkijken en herleiden tot een bepaald personeelslid.

7.4 Methodologie

De controle wordt uitgevoerd door de ICT-dienst en zal uitsluitend gebeuren met goedkeuring van de algemeen directeur. De ICT-dienst heeft door hun dagelijkse functie de mogelijkheid om toe te zien op het gebruik van (een deel van) de ICT-middelen. Door deze autorisatie zijn ze gebonden aan strikte voorwaarden ten aanzien van de persoonlijke levenssfeer van de werknemers en worden alle acties discreet uitgevoerd. Daarbij moet het recht op een privéleven van de personeelsleden gerespecteerd worden. De controle moet getoetst worden aan:

- het finaliteitsbeginsel: een controle is alleen mogelijk voor het nastreven van gerechtvaardigde doelen;
- het transparantiebeginsel: er wordt open gecommuniceerd over de controles en de doelen en voorwaarden van de controles;

- het proportionaliteitsbeginsel: de controle en het soort controle moeten in verhouding staan tot het doel van de controle.

Die drie beginselen hebben als doel het evenwicht te houden tussen:

- het recht van de werkgever op controle van werkmiddelen;
- het recht van de werknemer op zijn privéleven.

De ICT-dienst mag elke controle uitvoeren die inherent is aan het beheer van ICT-middelen, om de goede werking ervan te waarborgen, om overbelasting of veiligheidsproblemen te voorkomen of te verhelpen. Alle medewerkers moeten zich bewust zijn van het bestaan van deze controlemogelijkheid en van het feit dat alle communicatie die zij via het netwerk uitwisselen, hieraan onderworpen kan worden.
Gegevens of communicatie waarvan niet uitdrukkelijk is aangegeven dat het gaat om privéinformatie, kunnen op elk moment door de systeem- en netwerkbeheerders worden ingekeken.

8 Procedure bij incidenten

Een incident is een actie of een feit die de normale werking van het informaticasysteem of het netwerk verstoort.
Voor de toepassing van deze richtlijn wordt een onderscheid gemaakt tussen twee soorten incidenten:

- technische incidenten;
- inbreuken op de gedragsregels.

8.1 Procedure bij technische incidenten

Bij het uitvoeren van hun beheerstaken wordt de ICT-dienst frequent geconfronteerd met technische incidenten. Gebruikers van de ICT-middelen waarvoor ze verantwoordelijk zijn, kunnen bijvoorbeeld het slachtoffer zijn van computervirussen of andere ongewenste fenomenen. Bij het oplossen van deze incidenten kan de ICT-dienst zelfstandig optreden en het netwerkgedrag van gebruikers op individueel niveau opvolgen zolang dit voor de oplossing van het incident noodzakelijk is.
Wanneer het voor de veiligheid en om de goede werking van het netwerk te waarborgen noodzakelijk is, kan de ICT-dienst (sub)netwerken en andere toegangen (zoals bv. e-mailadressen, directories, VPN, …) onmiddellijk en zonder voorafgaandelijke waarschuwing afsluiten.
Wanneer noodzakelijk moet de medewerker op vraag van de systeem- en netwerkbeheerders de ICT-middelen onmiddellijk loskoppelen van de systemen van het lokale bestuur.

8.2 Procedure bij inbreuken op de gedragsregels

Bij inbreuken op de regels van deze richtlijn zijn, naargelang de ernst van de inbreuk, één of meer van de volgende procedurestappen van toepassing.

8.2.1 Meldingen en hun behandeling

Wie een inbreuk op de regels van deze richtlijn vaststelt, meldt dit bij een eerste waarneming aan de betrokken collega-gebruiker en wijst op de correcte manier van werken. Wanneer je herhaaldelijke inbreuken vaststelt, meld je dit aan de ICT-dienst. Meldingen kunnen onder meer afkomstig zijn van gebruikers, diensthoofden, mandatarissen of derden.
Een inbreuk kan ook gemeld worden aan de vertrouwenspersoon.
De ICT-dienst volgt de volgende procedure:

1. Er lijken geen regels van de ICT-richtlijn overtreden te zijn: De ICT-dienst behandelt zelf de melding op informele wijze en legt de afzender van de melding uit waarom geen verdere procedurestappen noodzakelijk zijn. Als de afzender van de melding niet instemt met de uitleg van de ICT-dienst, wordt de volgende procedurestap gevolgd.
2. Eén of meer regels van het ICT-richtlijn lijken (ernstig) overtreden te zijn: De ICT-dienst onderzoekt de gemelde inbreuk naar de effectieve feiten. Hierbij wordt een dossier over de feiten opgesteld.

Indien noodzakelijk neemt de ICT-dienst onmiddellijk (tijdelijke) voorzorgsmaatregelen om verdere onregelmatigheden te voorkomen.
De ICT-dienst bezorgt het dossier aan de algemeen directeur. Afhankelijk van de ernst van de inbreuken en van de schade berokkend aan het lokale bestuur wordt er door de algemeen directeur een vervolgprocedure opgestart. De algemeen directeur oordeelt, eventueel in overleg met het betrokken diensthoofd of anderen, over de te nemen vervolgstappen en/of tuchtmaatregelen in toepassing van de rechtspositieregeling en/of het arbeidsreglement en over eventuele andere maatregelen bijvoorbeeld op gerechtelijk vlak.
Mogelijke vervolgstappen kunnen zijn:

8.2.1.1 Waarschuwingsprocedure

De waarschuwingsprocedure heeft als doel de gebruiker te informeren over de gemelde of vastgestelde inbreuk en verantwoording te vragen over het gebruik van de ter beschikking gestelde ICT-middelen. De gebruiker wordt daarbij op de hoogte gebracht dat zijn/haar netwerkgedrag op individuele wijze gecontroleerd zal worden wanneer een nieuwe onregelmatigheid wordt vastgesteld.
De volgende regels worden hierbij in acht genomen:

- de voor de onregelmatigheid verantwoordelijk geachte gebruiker wordt uitgenodigd voor een gesprek met zijn/haar leidinggevende, een werknemer van de ICT-dienst en eventueel uitgebreid met een werknemer van de personeelsdienst en/of een lid van de leidinggevenden;
- dit gesprek heeft plaats voor iedere beslissing of evaluatie die de gebruiker individueel kan raken;
- de gebruiker krijgt de kans eventuele bezwaren met betrekking tot de voorgenomen beslissing of evaluatie uiteen te zetten. De gebruiker kan zich desgewenst door een vakbondsafgevaardigde laten bijstaan.

8.2.1.2 Maatregelen

Bij vaststelling van veiligheidsrisico's kunnen, naargelang het geval, volgende maatregelen genomen worden om de veiligheid en integriteit van de ICT-middelen te waarborgen:

- de toegangsrechten van de gebruiker kunnen gedurende het onderzoek geschorst of beperkt worden;
- ICT-middelen van de betreffende gebruiker kunnen worden geïnspecteerd en in beslag genomen.

8.2.1.3 Sancties

Sancties kunnen worden genomen in toepassing van de rechtspositieregeling en/ of het arbeidsreglement.
Mogelijke maatregelen en sancties die tegen werknemers kunnen worden genomen bij vaststelling van inbreuken op deze richtlijn en rekening houdend met de ernst van de inbreuken zijn:

- de gebruiker verwittigen van de inbreuk en opleiden om beter om te gaan met de verkregen ICT-middelen;
- ordemaatregelen door de algemeen directeur: de tijdelijke opheffing van een account of tijdelijke beperking van de toegang tot of het gebruik van (delen van) de ICT-middelen waarbij een evenwicht wordt gezocht tussen het belang van de dienst, de bescherming van de systemen en de rechten van de betrokkene;
- maatregelen en sancties zoals voorzien in de toepasselijke regelgeving en de interne reglementen.

8.2.1.4 Gerechtelijk onderzoeken

Iedereen die aan deze richtlijn onderworpen is, dient er zich bewust van te zijn dat het lokale bestuur maximaal zal meewerken aan gerechtelijke onderzoeken en betrokken instanties zal inlichten als de toestand daartoe aanzet.

Artikel 2

Deze ICT richtlijn vervangt bijlage IV van het arbeidsreglement van het OCMW personeel.

Onderwerp: Bijlage bij het arbeidsreglement: Policy beveiligingsincidenten en gegevenslekken

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 :

Artikel 1

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.

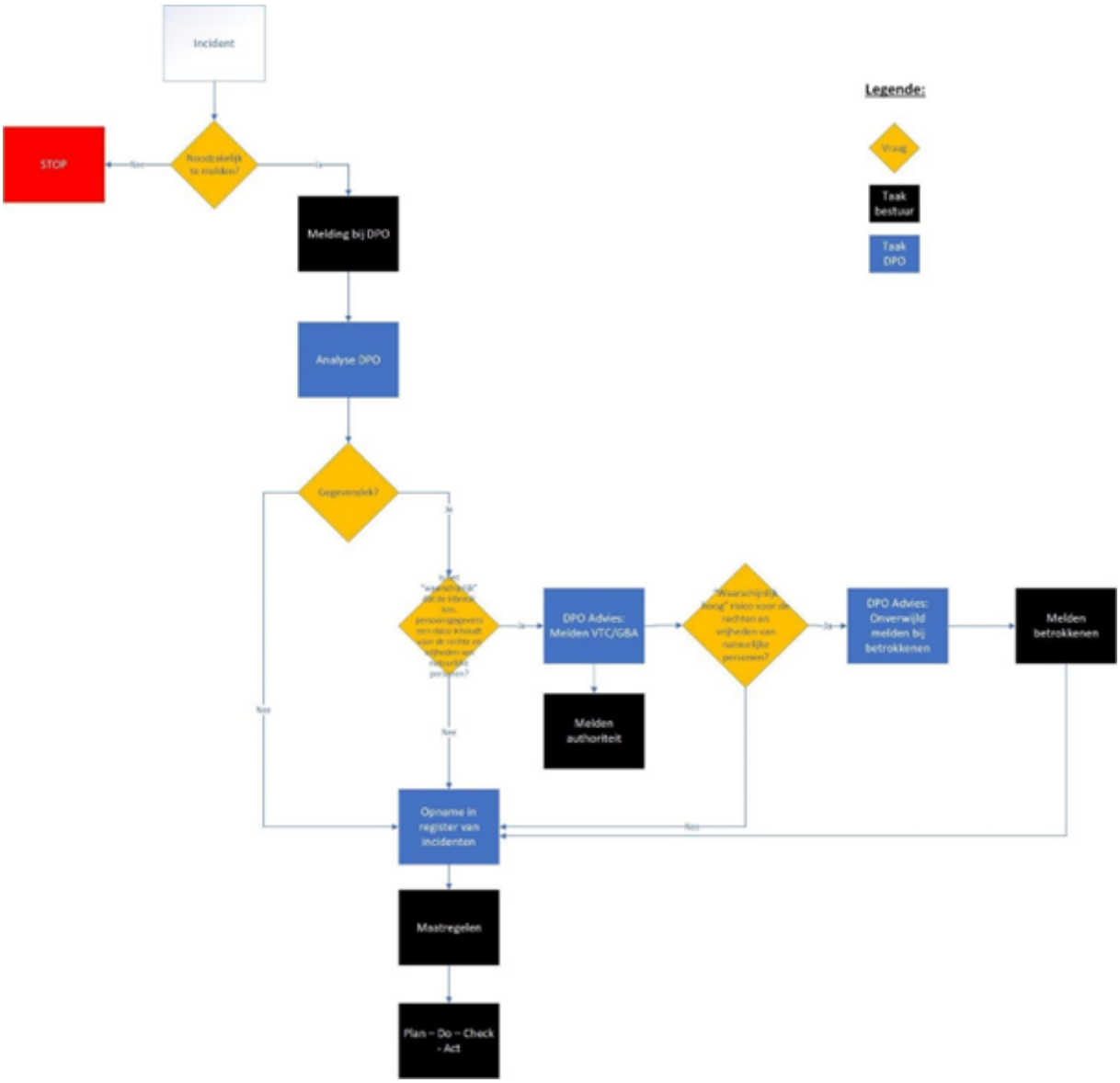
2. Definities

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.

Notulen en zittingsverslag vergadering 11.01.2024
Notulen
Gelet op het huishoudelijk reglement van de raad voor maatschappelijk welzijn, goedgekeurd door de raad van maatschappelijk welzijn in vergadering van 20.01.2022, inzonderheid artikel 29 §3;
Aangezien verder tijdens de vergadering geen bezwaren tegen de notulen van de vergadering van 11.01.2024 werden ingebracht;
zijn de notulen van de vergadering van 11.01.2024 goedgekeurd.
Zittingsverslag
In toepassing van artikel 278 §1 van het decreet over het lokaal bestuur en artikel 28 §2 van het huishoudelijk reglement van de raad voor maatschappelijk welzijn is het zittingsverslag vervangen door de integrale audio-opname van de openbare zitting van de raad voor openbaar welzijn.

De algemeen directeur
Christi Van Calster
[SIG01]

De voorzitter van de raad voor maatschappelijk welzijn,
Isabelle Dehond
[SIG02]