VERSLAG VAN DE RAAD VOOR MAATSCHAPPELIJK WELZIJN VAN HAMME IN ZITTING VAN 11/09/2019 AANSLUITEND OP DE GEMEENTERAAD

Aanwezig: Jan Laceur, raadsvoorzitter
Herman Vijt, burgemeester
Luk De Mey, Ann Verschelden, Koen Mettepenningen, Mieke De Keyser, Lien De Vos, Kurt De Graef, Jan Ketels, An Geerinck, Lotte Peeters, Jan De Graef, Kim Peelman, André Raemdonck, Tom Vermeire, Jan Rosschaert, Tom Waterschoot, Henri Peelman, Evelien D'hooghe, Agnes Onghena, Mustafa Tokgoz, Gülcan Unan, Leo Van der Vorst, Mario Michils, Christel Vanhoyweghen, leden raad voor maatschappelijk welzijn
André Reuse, algemeen directeur

Verontschuldigd: Frans Van Gaeveren, Nadia Dhooghe, leden raad voor maatschappelijk welzijn

---

OPENBAAR

O.1 <u>Proces-verbaal van de vorige zitting dd. 19 juni 2019 - goedkeuring</u>

De raad voor maatschappelijk welzijn,

In openbare zitting vergaderd,

Keurt het proces-verbaal van 19 juni 2019 met algemene instemming goed.

O.2 <u>Jaarverslag 2018 - akteneming</u>

De raad voor maatschappelijk welzijn,

In openbare zitting vergaderd,

REGELGEVING:

- Het huidige Decreet Lokaal Bestuur van 22 december 2017 bevat geen expliciete verplichting meer voor het lokaal bestuur om een "Jaarverslag" te maken en voor te leggen aan de raad voor maatschappelijk welzijn.
- Art. 260, tweede lid van het DLB stelt dat de jaarrekening bestaat uit een beleidsevaluatie, een financiële nota en een toelichting; art.261 DLB specifieert verder wat de "beleidsevaluatie" inhoudt.

OVERWEGINGEN:

- Het Jaarverslag over de werking van het OCMW wordt jaarlijks binnen de diensten van het OCMW opgesteld en bevat een overzicht van de activiteiten binnen het OCMW aan de hand van cijfergegevens over de prestaties van de verschillende OCMW diensten: sociale dienst, WZC Meulenbroek, poetsdienst, Kinderopvang, … In die zin geeft het een goed beeld weer van wat er gebeurt aan dienstverlening binnen het OCMW. Het wordt dus best samen gelezen met het "financieel rapport", de jaarrekening.
- Tevens wordt een overzicht opgenomen van de belangrijkste beslissingen van het OCMW gedurende het afgelopen jaar.

AKTENAME:

De raad voor maatschappelijk welzijn neemt akte van het jaarverslag 2018 over de werking van het OCMW.

O.3 Informatieveiligheidsbeleid - vaststelling - besluit

De raad voor maatschappelijk welzijn,

In openbare zitting vergaderd,

REGELGEVING:

- Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen.
- Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid.
- Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
- Besluit van de Vlaamse Regering van 15 mei 2009 houdende de uitvoering van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
- Besluit van de Vlaamse Regering van 29 november 2013 tot uitvoering van het decreet van 13 juli 2012 houdende de oprichting en organisatie van een Vlaamse dienstenintegrator
- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming AVG; ook gekend als General Data Protection Regulation GDPR), in het bijzonder:
    - Artikel 24, 2°: '(…) de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen [treft] om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. (…) Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde

maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.'
    - Artikel 39, 1°, b) dat stelt dat de functionaris voor gegevensbescherming onder andere toeziet 'op naleving van deze verordening, van andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens (…)'.
- Besluit van de Vlaamse Regering van 23 november 2018 betreffende de functionarissen voor gegevensbescherming (vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer), in het bijzonder artikel 7, 1°:
    - In het kader van zijn taken bevordert en ziet de functionaris voor de gegevensbescherming overeenkomstig artikel 39, lid 1, b), van de algemene verordening gegevensbescherming toe op de naleving van de voorschriften voor de gegevensbescherming, opgelegd door de algemene verordening gegevensbescherming, de regelgeving over de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens en het beleid van de verwerkingsverantwoordelijke over de bescherming van persoonsgegevens.
- Vanuit de Gegevensbeschermingsautoriteit (GBA): richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens in steden en gemeenten; vanuit de Kruispuntbank van de sociale zekerheid (KSZ): minimale normen informatieveiligheid en privacy waarbij het volgende wordt bepaald: 'Elke organisatie moet over een formeel, geactualiseerd en door het hoogste beslissingsorgaan van uw organisatie goedgekeurd informatiebeveiligingsbeleid beschikken dat op regelmatige basis naar alle relevante partijen gecommuniceerd wordt.'
- Decreet van 22 december 2017 over het lokaal bestuur.
- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.
- Besluit van de Vlaamse Regering van 23 november 2018 betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
- Bestuursdecreet van 7 december 2018.

OVERWEGINGEN:

- In raadszitting van 18 juni 2014 werd de samenwerkingsovereenkomst tussen gemeente Hamme en provincie Oost-Vlaanderen met betrekking tot informatieveiligheid afgesloten waarop het OCMW ook instapte zoals besproken in de raadszitting van 22 juni 2017.
- Het huidige informatieveiligheidsbeleid, waarover een bestuur dient te beschikken conform de weergegeven regelgeving, werd goedgekeurd in gemeenteraadszitting van 22 februari 2017 en is o.a. door de gewijzigde regelgeving (AVG/GDPR) aan een update toe.
- Met de besluiten van het college van burgemeester en schepenen en het vast bureau van respectievelijk 5 maart 2019 en 12 maart 2019 werd Victor De Meulemeester aangewezen als functionaris voor gegevensbescherming voor de gemeente Hamme.
- De geactualiseerde samenstelling van de informatieveiligheidscel zoals besproken in het college van burgemeester en schepenen van 14 mei 2019.
- De besprekingen van het informatieveiligheidsbeleid in de informatieveiligheidscel.

BESLUIT met algemene instemming:

Enig artikel: Het informatieveiligheidsbeleid voor het OCMW wordt goedgekeurd.

INFORMATIEVEILIGHEIDSBELEID GEMEENTE EN OCMW HAMME

1. Inleiding

1.1 Missie van de organisatie

Refererend aan artikel 2 van het Decreet van 22 december 2017 over het lokaal bestuur is de missie van gemeente en OCMW Hamme:

- *De gemeenten en de openbare centra voor maatschappelijk welzijn beogen om op het lokale niveau duurzaam bij te dragen aan het welzijn van de burgers en verzekeren een burgernabije, democratische, transparante en doelmatige uitoefening van hun bevoegdheden. Ze betrekken de inwoners zo veel mogelijk bij het beleid en zorgen voor openheid van bestuur.*
- *De gemeenten zijn overeenkomstig artikel 41 van de Grondwet bevoegd voor de aangelegenheden van gemeentelijk belang. Voor de verwezenlijking daarvan kunnen ze alle initiatieven nemen. Ze beogen om bij te dragen aan de duurzame ontwikkeling van het gemeentelijk gebied.*
- *De openbare centra voor maatschappelijk welzijn oefenen de opdrachten, vermeld in artikel 1 en 57 van de organieke wet van 8 juli 1976 betreffende de openbare centra voor maatschappelijk welzijn, uit, alsook de andere aangelegenheden die hen door of krachtens een wet of een decreet worden opgelegd.*

Gemeente en OCMW Hamme beschikken uit hoofde van hun missie over veel informatie: zelf gegenereerd of verkregen van andere besturen. Het is evident dat niet al deze informatie openbaar is (vanwege bv. bedrijfsgeheimen, of gevoeligheden omwille van de persoonlijke levenssfeer), en dat derhalve deze informatie beveiligd dient te worden, in het bijzonder tegen oneigenlijk gebruik.

1.2 Definitie informatieveiligheid en doelstelling

Onder informatieveiligheid wordt het proces verstaan van het vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen. Het gaat om de beveiliging van informatie, die over het algemeen is opgeslagen in informatiesystemen (digitale dragers), maar ook opgeslagen kan zijn in papieren dossiers (fysieke dragers).

- Met vertrouwelijkheid wordt bedoeld: de mate waarin de toegang tot informatie of functionaliteit beperkt is tot diegenen die hiertoe zijn geautoriseerd;
- Met beschikbaarheid wordt bedoeld: de mate waarin geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot de informatie;
- Met integriteit wordt bedoeld: de mate van correctheid en volledigheid van de informatie.

Het informatieveiligheidsbeleid is erop gericht om, op basis van risicomanagement, te verzekeren dat de informatie van gemeente en OCMW Hamme correct en volledig is en tijdig toegankelijk voor de geautoriseerde personen.

1.3 Toepassingsgebied

Het informatieveiligheidsbeleid is bindend voor alle onderdelen van gemeente en OCMW Hamme.

Het informatieveiligheidsbeleid is van toepassing op het gehele proces van informatievoorziening en geldt gedurende de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

Het terrein van de informatieveiligheid beperkt zich niet tot bepaalde functies of functionarissen, maar geldt voor al degenen die toegang kunnen nemen tot de informatie van de organisatie (medewerkers, bezoekers, leveranciers) en voor alle (mondelinge en schriftelijke) informatie. Met dit laatste wordt de gecontroleerde informatie (die door de organisatie zelf is gegenereerd, opgehaald en wordt beheerd) alsook niet-gecontroleerde informatie (bv. uitspraken, persoonlijke websites of zakelijke personal pages, waarop de organisatie kan worden aangesproken) bedoeld. Met externe organisaties (vzw's, leveranciers, ...) die toegang kunnen nemen tot de infrastructuur van de organisatie dienen de nodige afspraken gemaakt te worden (bv. via een verwerkersovereenkomst).

Het beleid strekt zich zowel uit over de strategische en de tactische als de operationele organisatieniveaus. Tot slot heeft het informatieveiligheidsbeleid ook betrekking op ketens van informatiesystemen die zich kunnen uitstrekken tot buiten gemeente en OCMW Hamme en de externe partijen waarmee gemeente en OCMW Hamme samenwerken (ook met deze externe partijen zullen overeenkomsten inzage informatiebeveiliging opgesteld moeten worden).

1.4 Beheer van het beleidsdocument

Het informatieveiligheidsbeleid wordt minimaal elke zes jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Bij deze actualisatie worden nieuwe ontwikkelingen op het terrein van de bedrijfsvoering en op het terrein van informatieveiligheid en privacy meegenomen. Waar het bestuur verantwoordelijk is voor de goedkeuring en uitvoering van het beleid, beheert de functionaris voor gegevensbescherming het informatieveiligheidsbeleid: hij draagt zorg voor het bijstellen en actueel houden van het document.

De functionaris voor gegevensbescherming onderhoudt contact met relevante partijen, waaronder:

- Andere overheidsinstellingen
- Expertisegroepen
- ICT-leveranciers

De functionaris voor gegevensbescherming gebruikt deze contacten om informatieveiligheid te verbeteren en zo nodig te vertalen naar nieuw beleid. Het informatieveiligheidsbeleid wordt van kracht na validatie door de gemeenteraad en de raad voor maatschappelijk welzijn. Bij het van kracht worden van dit document worden vorige versies van het informatieveiligheidsbeleid ingetrokken.

Het geactualiseerde informatieveiligheidsbeleid wordt gepubliceerd en ter beschikking gehouden van de medewerkers van gemeente en OCMW Hamme.

2. Strategische uitgangspunten

2.1 Uitgangspunten informatieveiligheidsbeleid

Onze filosofie is dat we een open organisatie zijn, waar veel mogelijk is. De benadering van ICT en beveiliging is echter minder open. Er wordt van medewerkers en mandatarissen verwacht dat ze zich qua techniek en ook qua houding 'fatsoenlijk' gedragen (eigen verantwoordelijkheid). Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Het is om deze reden dat er gedragscodes (deontologische codes) zijn geformuleerd en geïmplementeerd.

De volgende uitgangspunten worden gehanteerd om de doelstelling van informatieveiligheid binnen gemeente en OCMW Hamme te verwezenlijken:

- Informatiebeveiliging is een lijnverantwoordelijkheid: dat betekent dat de diensthoofden de primaire verantwoordelijkheid dragen voor een goede informatiebeveiliging op hun diensten.

- Informatiebeveiliging is de verantwoordelijkheid van iedereen. Van medewerkers, mandatarissen en derden wordt er verwacht dat ze actief bijdragen aan de veiligheid van geautomatiseerde en analoge systemen en de daarin opgeslagen informatie.
- Informatiebeveiliging is een continu proces. Regelmatige herijking van beleid en audits: technologische en organisatorische ontwikkelingen binnen en buiten de organisatie maken het noodzakelijk om periodiek te reflecteren of men nog wel op de juiste wijze bezig is de beveiliging te waarborgen. Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op hun effectiviteit (controleerbaarheid).
- De organisatie is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd, tenzij dit anders is overeengekomen (bijvoorbeeld voor onderzoek). Medewerkers dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie.
- Waardering van informatie: iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Classificatie is hierbij een behulpzaam instrument.
- Bij projecten, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, dient vanaf de start rekening gehouden te worden met informatiebeveiliging.
- Het informatieveiligheidsbeleid voldoet aan de Europese en Belgische wet -en regelgeving, inzonderheid de privacywetgeving. Als leidraad worden de volgende normen gehanteerd:
    - De minimale normen van de Kruispuntbank Sociale Zekerheid (KSZ) ten aanzien van informatieveiligheid (https://www.ksz-bcss.fgov.be/nl/gegevensbescherming/informatieveiligheidsbeleid). Deze zijn gebaseerd op de ISO 27002 norm.
    - Richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens van de GBA (https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Steden%20en%2_0gemeenten v%203.0 0.pdf). Deze zijn gebaseerd op de ISO 27002 norm.

Zowel de minimale normen van de KSZ als de richtsnoeren van de GBA zijn op de internationale standaard voor informatiebeveiliging (ISO 27000) gebaseerd. Deze standaard dient dan ook als een belangrijke leidraad voor het inrichten en onderhouden van de informatiebeveiliging.

2.2 De toepassingsdomeinen met de doelstellingen

In dit onderdeel worden de toepassingsdomeinen beschreven waarbinnen maatregelen worden gedefinieerd om de beoogde doelstelling te verwezenlijken. Per titel wordt telkens verwezen naar de relevante hoofdstukken in de ISO 27002 norm (de praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging).

2.2.1 Informatiebeveiligingsbeleid (H5)

- Aansturing door de directie van de informatiebeveiliging
  Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

2.2.2 Organiseren van informatiebeveiliging (H6)

- Interne organisatie
  Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.
- Mobiele apparatuur en telewerken
  Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.

2.2.3 Veilig personeel (H7)

- Voorafgaand aan het dienstverband
  Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen.
- Tijdens het dienstverband
  Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.
- Beëindiging en wijziging van het dienstverband
  Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.

2.2.4 Beheer van bedrijfsmiddelen (H8)

- Verantwoordelijkheid voor bedrijfsmiddelen
  Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.
- Informatieclassificatie
  Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.
- Behandelen van media
  Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.

2.2.5 Toegangsbeveiliging (H9)

- Bedrijfseisen voor toegangsbeveiliging
  Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken.
- Beheer van toegangsrechten van gebruikers
  Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.
- Verantwoordelijkheden van gebruikers
  Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.
- Toegangsbeveiliging van systeem en toepassing
  Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.

2.2.6 Cryptografie (H10)

- Cryptografische beheersmaatregelen
  Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

2.2.7 Fysieke beveiliging en beveiliging van de omgeving (H11)

- Beveiligde gebieden
  Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.
- Apparatuur
  Doelstelling: Verlies, schade, diefstal of het compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.

2.2.8 Beveiliging bedrijfsvoering (H12)

- Bedieningsprocedures en verantwoordelijkheden
  Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.
- Bescherming tegen malware
  Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.
- Back-up
  Doelstelling: Beschermen tegen het verlies van gegevens.
- Verslaglegging en monitoren
  Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.
- Beheersing van operationele software
  Doelstelling: De integriteit van operationele systemen waarborgen.
- Beheer van technische kwetsbaarheden
  Doelstelling: Benutting van technische kwetsbaarheden voorkomen.
- Overwegingen betreffende audits van informatiesystemen
  Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.

2.2.9 Communicatiebeveiliging (H13)

- Beheer van netwerkbeveiliging
  Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.
- Informatietransport
  Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.

2.2.10 Acquisitie, ontwikkeling en onderhoud van informatiesystemen (H14)

- Beveiligingseisen voor informatiesystemen
  Doelstelling: Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.
- Beveiliging in ontwikkelings- en ondersteunende processen
  Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.
- Testgegevens
  Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.

2.2.11 Leveranciersrelaties (H15)

- Informatiebeveiliging in leveranciersrelaties
  Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.
- Beheer van dienstverlening van leveranciers
  Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.

2.2.12 Beheer van informatiebeveiligingsincidenten (H16)

- Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

2.2.13 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer (H17)

- Informatiebeveiligingscontinuïteit
  Doelstelling: Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.
- Redundante componenten
  Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.

2.2.14 Naleving (H18)

- Naleving van wettelijke en contractuele eisen
  Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.
- Informatiebeveiligingsbeoordelingen
  Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.

2.3 Wettelijke voorschriften

De belangrijkste toepasselijke wet- en regelgeving met betrekking tot informatieveiligheid en gegevensbescherming:

- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming).
- Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen.
- Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid.
- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.
- Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
- Decreet van 22 december 2017 over het lokaal bestuur.
- Bestuursdecreet van 7 december 2018.

- Besluit van de Vlaamse Regering van 15 mei 2009 houdende de uitvoering van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.
- Besluit van de Vlaamse Regering van 29 november 2013 tot uitvoering van het decreet van 13 juli 2012 houdende de oprichting en organisatie van een Vlaamse dienstenintegrator.
- Besluit van de Vlaamse Regering van 23 november 2018 betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

3. Informatieveiligheidsorganisatie

3.1 Rollen binnen Informatieveiligheid

In dit onderdeel worden beknopt de rollen, bevoegdheden en verantwoordelijkheden beschreven voor de informatieveiligheid.

3.1.1 Bestuur

Het hoogste bestuursorgaan is verantwoordelijk voor de verwerking binnen de organisatie. Daardoor is dit de eindverantwoordelijke voor de verwerking van persoonsgegevens en voor het informatieveiligheidsbeleid. Dit bestuursorgaan is doorgaans een gekozen groep van volksvertegenwoordigers. Voor gemeente en OCMW Hamme is dit respectievelijk de gemeenteraad en de raad voor maatschappelijk welzijn. Zij keuren het informatieveiligheidsbeleid goed.

3.1.2 Dagelijks bestuur

Het dagelijks bestuur legt verantwoording af aan het algemeen bestuur, zij heeft een meer uitvoerende taak. De uitvoering van het informatieveiligheidsbeleid via het informatieveiligheidsplan wordt dan ook ter goedkeuring voorgelegd aan dit dagelijks bestuur. Adviezen worden tevens meegedeeld aan het dagelijks bestuur. Het jaarverslag over het informatieveiligheidsbeleid wordt gerapporteerd aan het dagelijks bestuur: het College van Burgemeester en Schepenen (CBS) en het Vast Bureau (VB).

3.1.3 Managementteam (MAT)

Het managementteam vormt de leiding van een organisatie. Alle disciplines (directies/diensten) worden in het managementteam vertegenwoordigd door haar leden. Het managementteam is verantwoordelijk voor de kwaliteitsbewaking en coördinatie van de interne taken.

3.1.4 Directeur informatica

De directeur informatica, ook wel IT-verantwoordelijke of IT-manager, is verantwoordelijk voor het opstellen van de informatiestrategie en voor de informatiecoördinatie (het coördineren en afstemmen tussen diverse beleidsplannen). Daarnaast is hij verantwoordelijk voor het financieel-, capaciteits-, kwaliteits- en contractmanagement van de informatieverwerkende faciliteiten. Idealiter wordt hij bijgestaan door een Chief Information Security Officer (CISO). De CISO neemt dan de verantwoordelijkheid voor de implementatie van en het toezicht op het informatiebeveiligingsbeleid van de organisatie op zich en stelt de betrouwbaarheidseisen en een samenhangend pakket aan beveiligingseisen voor de informatieverwerkende faciliteiten vast, mede gebaseerd op de classificatie van de informatie die door deze faciliteiten worden verwerkt. Binnen gemeente en OCMW Hamme is deze laatste functie momenteel niet ingevuld.

3.1.5 Functionaris voor gegevensbescherming

De taken en bevoegdheden van de functionaris voor gegevensbescherming worden vastgelegd in het besluit van de Vlaamse Regering van 23 november 2018
(https://codex.vlaanderen.be/Zoeken/Document.aspx?DID=1030030&param=inhoud).

De functionaris voor gegevensbescherming werkt onder het rechtstreekse functionele gezag van de verantwoordelijke voor het dagelijks bestuur binnen de instantie, de leidend ambtenaar (algemeen directeur). Hij werkt nauw samen met de andere diensten binnen de instantie die mee instaan voor de gegevensbescherming. Tevens is hij aanspreekpunt voor en werkt hij samen met de toezichthoudende autoriteit(en).

3.1.6 Stuurgroep informatieveiligheid

Een stuurgroep informatieveiligheid (ook wel aangeduid als informatieveiligheidscel, of met soortgelijke term) volgt de uitvoering van het beveiligingsbeleid op dat werd opgemaakt in een informatieveiligheidsplan.

De stuurgroep komt op regelmatige momenten (om de zes weken) samen en heeft een adviserende, stimulerende, documenterende en faciliterende opdracht binnen de organisatie op vlak van informatiebeveiliging. Zij volgt ook de gemelde incidenten en zwakheden inzake informatieveiligheid op, en formuleert naar aanleiding hiervan eventuele acties en beheersmaatregelen.

De leden van de stuurgroep zijn aanspreekpunten inzake informatiebeveiliging voor de organisatie. Zij zijn vanwege hun functie en takenpakket betrokken bij of hebben affiniteit met processen en/of projecten waarin informatieveiligheid van belang is. In functie van de agenda kunnen er ook ad hoc leden worden uitgenodigd.

De functionaris voor gegevensbescherming fungeert als voorzitter van de stuurgroep.

3.1.7 Lijnmanagement

Informatieveiligheid is een lijnverantwoordelijkheid. De departements-/diensthoofden zien toe op de correcte toepassing van het informatieveiligheidsbeleid. Eventuele tekortkomingen en/of inbreuken worden gemeld aan de functionaris voor gegevensbescherming (of aan de stuurgroep).

3.1.8 Medewerkers

Informatiebeveiliging is ieders verantwoordelijkheid. De medewerker is verantwoordelijk voor het zorgvuldig omgaan met (vertrouwelijke) informatie conform het Informatieveiligheidsbeleid. Elk incident met betrekking tot de informatieveiligheid wordt gemeld aan de functionaris voor gegevensbescherming en andere belanghebbenden, conform de procedure inzake informatieveiligheidsincidenten en datalekken.

3.2 RACI-model

Een RACI-model is een schema dat gehanteerd wordt om de rollen en verantwoordelijkheden bij de diverse activiteiten aan te duiden en de communicatiestromen te verduidelijken. De letters RACI staan voor:

- R (Responsible, NL: Verantwoordelijk): De rol die verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de rol ‘accountable’.
- A (Accountable, NL: Eindverantwoordelijk): De rol die (eind)verantwoordelijk, bevoegd is en goedkeuring geeft aan het resultaat.
- C (Consulted, NL: Geraadpleegd): Deze rol geeft (mede) richting aan het resultaat, wordt voorafgaand aan beslissingen of acties (verplicht) geraadpleegd.
- I (Informed, NL: Geïnformeerd): Iemand die geïnformeerd wordt over de beslissingen, over de voortgang, bereikte resultaten enz. Dit is eenrichtingscommunicatie, in tegenstelling tot ‘consulted’.

	GR	CBS/AD	MAT	ICT	FG	IVC	LM	MW

Informatieveiligheidsbeleid	A	R	R	C	C	C	I	I
Wet- en regelgeving	A	R	I	I	C	I	I	I
Richtlijnen	I	AR	C	C	C	C	I	I
Maturiteitsmeting		A	I	C	R	C		
Risicoanalyse		A	I	C	R	C		
Informatieveiligheidsplan		A	I	C	R	C		
Incidentenprocedure	I	A	I	I	R	R	I	I
Controle beheersmaatregelen		A	I	I	R	R		
Verwerkingsregister		A	R	I	C	I	R	I
Jaarverslag		I			AR	C		
Correctieve acties		A	C	R	R	R	I	

Figuur: het beveiligingsproces.

- *GR: Gemeenteraad*
- *CBS: College van burgemeester en schepenen*
- *AD: Algemeen directeur*
- *MAT: Managementteam*
- *ICT: ICT verantwoordelijke*
- *FG: Functionaris gegevensbescherming*
- *IVC: Informatieveiligheidscel*
- *LM: Lijnmanagement*
- *MW: Medewerkers*

4. Informatieveiligheidsproces

In dit hoofdstuk wordt het informatieveiligheidsproces, risicomanagement en het gemeenschappelijk informatieveiligheidsniveau beschreven. Doel van dit hoofdstuk is om inzicht te geven in het proces van informatieveiligheid, de aansturing van dit proces en de samenhang met de bedrijfsprocessen van de organisatie.

4.1 Informatieveiligheidsproces (PDCA-cyclus)

Het informatieveiligheidsproces zelf is, conform de ISO 27000 norm, ingericht op basis van de Plan-Do-Check-Act-cyclus. De PDCA-cyclus zorgt voor periodieke toetsing van de werking en de noodzaak van gekozen beheersmaatregelen zoals voorgesteld in een informatieveiligheidsplan en leidt zo tot continue verbetering van de informatieveiligheid. De maatregelen worden geïmplementeerd op basis van risicomanagement en een bewuste kosten-batenanalyse. Dit zorgt voor een optimale beveiliging tegen een aanvaardbare kost. Hiermee wordt invulling gegeven aan het beleid van gemeente en OCMW Hamme om veilig te faciliteren in plaats van maximaal te beveiligen.

4.2 Aansturing van het proces

Informatieveiligheid gaat om het voortdurend bepalen van risico's, het kunnen reageren op incidenten en het nemen van adequate maatregelen voorgesteld in een informatieveiligheidsplan op basis van risicomanagement. Om de risico's te bewaken en te beheersen is binnen gemeente en OCMW Hamme een informatieveiligheidsproces ingericht. Het beveiligingsproces wordt aangestuurd vanuit het lijnmanagement, omdat daar de verantwoordelijkheid ligt met betrekking tot de informatieveiligheid.

Het lijnmanagement wordt daarbij ondersteund door de functionaris voor gegevensbescherming. Doel van het beveiligingsproces is het inzichtelijk maken van de (rest)risico's voor een bepaalde situatie of informatiesysteem zodat de lijnmanager op basis hiervan tot een weloverwogen besluit kan komen.

Wet- en regelgeving stellen de minimumeisen waaraan informatieveiligheid moet voldoen. Het eerbiedigen ervan is een uitgangspunt voor de inrichting van het beveiligingsproces. Andere organisaties (derden) kunnen eisen stellen aan de informatieveiligheid van gemeente en OCMW Hamme voor de borging van hun bedrijfsprocessen. Andersom zullen gemeente en OCMW Hamme bij het buiten de organisatie brengen van informatie eisen stellen aan de informatieveiligheid van de ontvangende partijen en bij het ontvangen van informatie eisen stellen aan de informatieveiligheid van de leverende partijen.

Om de risico's te verkleinen worden maatregelen getroffen in de bedrijfsprocessen en de daarbinnen gebruikte informatiesystemen. Informatieveiligheidsincidenten kunnen een aanleiding zijn om (aanvullende) maatregelen te nemen en de bestaande maatregelen te evalueren.

Departementen en de ICT-dienst rapporteren over de voortgang, actualiteit en de effectiviteit van de maatregelen. Vanuit het beveiligingsproces kan hierop worden ingegrepen door verbetervoorstellen in te dienen.

Ontwikkelingen op technisch en sociaal gebied zorgen ervoor dat het informatieveiligheidsbeleid veroudert. Om dit te voorkomen dient het beleid periodiek geëvalueerd en herzien te worden.

4.3 Bedrijfscontinuïteitsbeheer (BCP)

Gemeente en OCMW Hamme zullen een BCP uitwerken, testen en onderhouden indien de kritische processen dit vereisen. Dit continuïteitsplan moet gebaseerd zijn op een risicoanalyse om de kritische opdrachten van gemeente en OCMW Hamme te kunnen waarborgen.

Onderdelen van het BCP:

- Een inventaris van de infrastructuur: hardware, software en netwerk.
- De documentatie van de activiteiten in processen en procedures.
- Het opstellen van een matrix die de verbinding maakt tussen de activiteiten en de infrastructuurelementen.
- Het bepalen van de risico's van en de gewenste minimale dienstverlening voor elke activiteit (o.a. maximale onderbreking).
- Het bepalen van de mogelijke en/of nodige maatregelen om de minimale dienstverlening te garanderen en hun invloed op of nood aan ICT-ondersteuning.
- Het voorzien van redundantie om continuïteit te waarborgen, met inachtname van de bijkomende risico's ten gevolge van redundantie.
- Er worden draaiboeken opgesteld die moeten helpen bij:
    - een IT-incident (het onbeschikbaar worden van (een deel van) de ICT-infrastructuur of connectiviteit),

- een ramp (het onbeschikbaar worden van (een deel van) de ICT-infrastructuur of connectiviteit en van de omgeving).

- Evaluatieprocedures, testmethodes en testplan voor beide scenario's.

4.4 Projecten

In projecten met een ICT-component worden, voorafgaand aan de ontwikkeling of aankoop van nieuwe systemen of belangrijke aanpassingen van bestaande systemen, procedures gehanteerd waarbij door de projectverantwoordelijke rekening wordt gehouden met de veiligheidsvereisten.

De functionaris voor gegevensbescherming wordt bij aanvang van elk project waar het een nieuwe verwerking of wijzigende verwerking van persoonsgegevens betreft geïnformeerd en uitgenodigd om hierover advies te verlenen. Eventueel brengt de functionaris voor gegevensbescherming op eigen initiatief advies uit (zoals bedoeld in artikel 3 van het Besluit van de Vlaamse Regering van 23 november 2018 betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer). Voor alle kritische systemen die privacygevoelige gegevens verwerken wordt bij elke belangrijke aanpassing een externe veiligheidsaudit gedaan.

Ter ondersteuning van projecten is het nuttig een ‘project office’ in te richten. Een dergelijke groep kan administratieve ondersteuning bieden en standaarden ontwikkelen binnen de projectwerking.

4.5 Gegevensbeschermingseffectbeoordeling

Wanneer een gegevensverwerking van gemeente en OCMW Hamme een hoog risico inhoudt met betrekking tot de gegevensbescherming, in het bijzonder door het gebruik van nieuwe technologieën, zal een beoordeling worden gemaakt van het effect daarvan op informatieveiligheid.

Bij het uitvoeren van deze beoordeling wordt het advies van de functionaris voor gegevensbescherming ingewonnen. De beoordeling omvat de maatregelen die genomen moeten worden om de geïdentificeerde risico’s aan te pakken.

4.6 Incident management

Een actuele en betrouwbare registratie van incidenten is een essentiële randvoorwaarde voor een goed beleid. De stuurgroep informatieveiligheid zorgt voor het registreren van incidenten in een incidentenregister. Dit register is de basis voor de afhandeling van informatieveiligheidsincidenten en datalekken, en dient tevens om inzicht te krijgen in trends en ontwikkelingen. Dit dient als input voor de evaluatie en het bijstellen van het informatieveiligheidsbeleid en/of het informatieveiligheidsplan.

4.7 Producten

Het informatieveiligheidsproces levert een aantal producten op die de voortgang van het proces inzichtelijk maken:

4.7.1 Informatieveiligheidsbeleid

Dit document, het beleid, ligt ten grondslag aan de aanpak van informatiebeveiliging binnen de organisatie.

4.7.2 Informatieveiligheidsplan

Het informatieveiligheidsplan is het geheel van voorgestelde acties en beheersmaatregelen die tot doel hebben om binnen de organisatie het gewenste niveau van informatiebeveiliging te kunnen waarborgen. Het veiligheidsplan wordt opgemaakt door de functionaris voor gegevensbescherming en gevalideerd door de werkgroep informatiebeveiliging. Uiteindelijk beslist het dagelijks bestuur (of diens gedelegeerde) inzake de uitvoering van het plan.

4.7.3 Risicoanalyses en audits

Periodieke evaluatie van de risico's van systemen is noodzakelijk om vast te stellen of het gekozen pakket van beheersmaatregelen nog steeds voldoet aan de gewijzigde omstandigheden. Bedreigingen kunnen immers in de loop der tijd veranderen, informatieverwerkende systemen en/of de organisatie kunnen inmiddels zijn aangepast en maatregelen werken wellicht anders uit dan oorspronkelijk bedoeld. De risicoanalyses worden besproken met de systeemeigenaren en de functionaris voor gegevensbescherming en over eventuele te nemen beheersmaatregelen wordt geadviseerd aan het bestuur.

De risicoanalyses en audits worden gemaakt onder verantwoordelijkheid van de functionaris voor gegevensbescherming en in samenwerking met eventuele externe firma's.

4.7.4 Incidentregistratie

Er wordt een register opgemaakt van informatieveiligheidsincidenten en datalekken. Het is het resultaat van het incident managementproces (ref. 4.6). Het is vanuit dit register dat een eventuele melding van een inbreuk gedaan wordt aan de bevoegde autoriteit voor de gegevensbescherming (Voor Vlaamse instanties is dit de Vlaamse Toezichtcommissie (VTC)).

4.7.5 Verwerkingsregister

Het verwerkingsregister bevat een overzicht van alle processen (verwerkingsactiviteiten) met betrekking tot persoonsgegevens. De inhoud van dit register wordt gespecificeerd in artikel 30 van de AVG (Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG). Het register dient ook ter beschikking gehouden te worden van de bevoegde autoriteit.

4.7.6 Jaarverslag

De functionaris voor gegevensbescherming maakt elk jaar een verslag op houdende een overzicht van de veiligheidstoestand, uitgevoerde taken, controles, campagnes en genoten opleidingen.

De minimale inhoud van het jaarverslag is vastgelegd in artikel 3 van het Besluit van de Vlaamse Regering van 23 november 2018 (Besluit van de Vlaamse Regering van 23 november 2018 betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer).

Het jaarverslag wordt aangeboden aan het dagelijks bestuur, of diens vertegenwoordiger.

4.8 Evaluatie

Het beleid, de betrouwbaarheidseisen en de maatregelen worden op centraal niveau (door een onafhankelijke deskundige) één keer in de drie jaar geëvalueerd, om vast te stellen of deze leiden tot de gewenste mate van beveiliging. De evaluatie kan aanleiding geven tot het bijstellen van het informatieveiligheidsbeleid, de betrouwbaarheidseisen en/of de maatregelen.

Elke lijnmanager die eigenaar is van een eigen informatiesysteem, heeft de plicht de informatieveiligheid van dit systeem elke drie jaar te (laten) evalueren en actueel te houden (of eerder, bij ingrijpende wijzigingen).

De functionaris voor gegevensbescherming houdt toezicht op de informatieveiligheid door middel van bovengenoemde toetsingsinstrumenten en door middel van de jaarlijkse zelfevaluaties die worden uitgevoerd. De functionaris voor gegevensbescherming draagt zorg voor de (ontwikkeling van de) nodige deskundigheid, mede door intercollegiaal overleg.

5. Bevordering Informatieveiligheidsbewustzijn

5.1 Zwakste schakel

Een goede informatieveiligheid hangt niet alleen af van technische maatregelen maar heeft ook een belangrijke relatie met het gedrag van medewerkers. De beveiligingsketen is zo sterk als de zwakste schakel. Dit blijkt vaak het gedrag van medewerkers te zijn, die zich niet steeds bewust zijn van de risico's van hun handelen. Technische maatregelen kunnen dit vaak niet oplossen.

Daarom is het belangrijk om medewerkers attent te maken op veilig en onveilig gedrag. Medewerkers hebben een eigen verantwoordelijkheid bij het zorgvuldig en integer omgaan met informatie die zij verwerken. Dit betekent niet alleen dat zij vertrouwelijke informatie als zodanig herkenbaar maken voor anderen (classificeren), maar ook dat zij vertrouwelijke informatie alleen delen met anderen die deze informatie nodig hebben voor hun werkzaamheden, vertrouwelijke informatie volgens het vier ogen-principe verwerken, en ervoor zorgen dat onbevoegden geen kennis kunnen nemen van deze informatie (veilig opbergen of *clear desk*-principe, versleuteld verzenden, informatie alleen delen op basis van het *'need to know'* principe in plaats van het *'nice to know'* principe). Medewerkers volgen de classificatierichtlijnen en kennen de regels voor informatieveiligheid.

5.2 Activiteiten om het beveiligingsbewustzijn te vergroten

Het vergroten van het veiligheidsbewustzijn bij medewerkers van de organisatie wordt bereikt door periodiek gerichte activiteiten te organiseren. De functionaris voor gegevensbescherming, samen met de werkgroep informatieveiligheid, initieert en coördineert de periodiek uit te voeren bewustwordingsprogramma's in de vorm van bewustwordingscampagnes, gedragscodes, nieuwsbrieven, presentaties en nieuwsvoorziening via de gebruikelijke kanalen. Informatieveiligheid maakt eveneens een standaard onderdeel uit van de introductieopleiding voor nieuwe medewerkers.

De lijnmanagers verlenen hun medewerking aan en ondersteunen deze activiteiten. Daarnaast is de lijnmanager zelf ook verantwoordelijk voor het vergroten van de bewustwording van zijn/haar medewerkers. Dit kan bijvoorbeeld door informatieveiligheid bespreekbaar te maken in werkoverleggen en in start- en functioneringsgesprekken.

De heer raadsvoorzitter J. Laceur verklaart de zitting gesloten.

Gedaan te Hamme in zitting als ten hoofde.

Namens de raad voor maatschappelijk welzijn:

André Reuse
Algemeen directeur

Jan Laceur
raadsvoorzitter