STAD MECHELEN
Gemeenteraad – Uittreksel uit de notulen
Vergadering van 1 maart 2021 - Openbare zitting

Aanwezig:

Fabienne Blavier, voorzitter
Alexander Vandersmissen, burgemeester wd.
Patrick Princen, Greet Geypen, Marina De Bie, Koen Anciaux, Björn Siffer, Abdrahman Labsir, Vicky Vanmarcke, Gabriella De Francesco, schepenen
Bart Somers, Frank Creyelman, Marc Hendrickx, Stefaan Deleus, Catherine François, Karel Geys, Hamid Riffi, Kristof Calvo, Zineb El Boussaadani, Farid Bennasser, Jan Verbergt, Tine Van den Brande, Kerstin Hopf, Freya Perdaens, Anne Delvoye, Ingrid Kluppels, Bert Delanoeije, Pia Indigne, Klaas Delrue, Arthur Orlians, Faysal El Morabet, Mats Walschaers, Charles Leclef, Rina Rabau, Maxine Willemsen, Elisabet Okmen, Dirk Tuypens, Yves Selleslagh, Kenzo Van den Bosch, Thijs Verbeurgt, Zohra Hadnan, Shanna Jacops, gemeenteraadsleden
Jan Bal, adjunct-algemeendirecteur

18. INFORMATIEVEILIGHEIDSBELEID. Goedkeuring beleidsnota 'Informatieveiligheid & Gegevensbescherming voor stad en OCMW Mechelen'.

De beslissing wordt genomen met 38 stemmen voor (Fabienne Blavier, Alexander Vandersmissen, Patrick Princen, Greet Geypen, Marina De Bie, Koen Anciaux, Björn Siffer, Abdrahman Labsir, Vicky Vanmarcke, Gabriella De Francesco, Bart Somers, Marc Hendrickx, Stefaan Deleus, Karel Geys, Hamid Riffi, Kristof Calvo, Zineb El Boussaadani, Farid Bennasser, Jan Verbergt, Tine Van den Brande, Kerstin Hopf, Freya Perdaens, Anne Delvoye, Bert Delanoeije, Pia Indigne, Klaas Delrue, Arthur Orlians, Faysal El Morabet, Mats Walschaers, Charles Leclef, Rina Rabau, Maxine Willemsen, Elisabet Okmen, Dirk Tuypens, Yves Selleslagh, Thijs Verbeurgt, Zohra Hadnan, Shanna Jacops) en 4 onthoudingen (Frank Creyelman, Catherine François, Ingrid Kluppels, Kenzo Van den Bosch)

Motivering

Voorgeschiedenis

Beleidsnota (versie 2.0) m.b.t. Informatieveiligheid werd goedgekeurd op
- 2 maart 2018 door College Burgemeester en Schepenen
- 5 maart 2018 door Vast Bureau
- 19 maart 2018 door Raad voor Maatschappelijk Welzijn
- 27 maart 2018 - punt 9 door Gemeenteraad

De nieuwe beleidsnota (versie 3.0) m.b.t. Informatieveiligheid & Gegevensbescherming werd goedgekeurd op
- 3 december 2020 door het M-team
- 25 januari 2021 – agendapunt 28 door College van burgemeester en schepenen + verwijzing naar de gemeenteraad.

Feiten en argumentatie

Informatieveiligheid is een continu verbeterproces. Het informatieveiligheidsbeleid dient regelmatig herzien te worden zodat het in lijn blijft met veranderende omstandigheden op allerlei vlakken. Zo groeien stad en OCMW naar steeds meer conformiteit met de nieuwe wet- en regelgevingen en richtlijnen.

Het beleid en zijn management spelen een cruciale rol om Informatieveiligheid & Gegevensbescherming te borgen binnen de organisatie. Zij dienen te demonstreren dat zij Informatieveiligheid & Gegevensbescherming ondersteunen en zich hierbij betrokken voelen, door het uitbrengen en handhaven van een beleid van en voor het hele lokale bestuur.

Het informatieveiligheidsbeleid dient goedgekeurd te worden door het College van Burgemeester en Schepenen & de Gemeenteraad voor de Stad Mechelen en door het Vast Bureau & de Raad voor Maatschappelijk Welzijn voor het OCMW Mechelen. Zo wordt het normenkader, samen met de rollen & verantwoordelijkheden, formeel vastgelegd.

Informatieveiligheid & Gegevensbescherming handelt om meer dan enkel ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm, enzoverder) en alle informatie verwerkende systemen (programmatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook om mensen en processen.

Er worden 2 documenten als bijlage toegevoegd:
- '200811_Beleidsnota informatieveiligheid Stad en OCMW Mechelen_definitief_3_0_versie met markering wijzigingen.pdf'
  Hierin zijn de wijzigingen t.o.v. de beleidsnota versie 2.0 aangebracht.
- '200811_Beleidsnota informatieveiligheid Stad en OCMW Mechelen_definitief_3_0_integrale versie.pdf'
  Deze bevat de nieuwe tekst van de volledige beleidsnota (zonder markeringen).

De volledige beleidsnota wordt ter goedkeuring voorgelegd.

Juridische grond

- Europees
  - 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 of General Data Protection Regulation GDPR)
- Federaal
  - 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 (Kruispuntbankwet)
  - Wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten
  - Koninklijk besluit van 16 juli 1992 betreffende het verkrijgen van informatie uit de bevolkingsregisters en uit het vreemdelingenregister.
  - Koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid
  - Koninklijk besluit van 11 juli 2005 tot bepaling van de datum van inwerkingtreding van het koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid, voor wat betreft de openbare centra voor maatschappelijk welzijn
  - Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (organieke wet of WOG)
  - Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (kaderwet of WVG)
  - Wet van 25 november 2018 betreffende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters
  - Wet van 5 september 2018 tot oprichting van het informatieveiligheidscomité wet informatie-veiligheidscomité) en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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 (
  - Gecoördineerde versie van 31 maart 2019 van de algemene onderrichten betreffende het houden van de Bevolkingsregisters
- Vlaams
  - Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (e-govdecreet) zoals gewijzigd bij het AVGdecreet en het bestuursdecreet

- 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 gegevensverkeer
- Decreet van 8 juni 2018 houdende de aanpassing van de decreten aan de 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 (AVG-decreet)
- Decreet van 7 december 2018 Bestuursdecreet

- Gemeenschappelijk normenkader als basis: "richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens in steden en gemeenten, in instellingen die deel uitmaken van het netwerk dat beheerd wordt door de Kruispuntbank van Sociale Zekerheid en bij de integratie OCMW – Gemeente".

Besluit:

Artikel 1
De gemeenteraad keurt de nieuwe beleidsnota met betrekking tot Informatieveiligheid & Gegevensbescherming goed en legt zo het normenkader, samen met de rollen en verantwoordelijkheden, vast.

(bijlage)

Artikel 2
De gemeenteraad beslist tot opheffing van het gemeenteraadsbesluit van 27 maart 2018 – agendapunt 9, houdende goedkeuring van de 'beleidsnota informatieveiligheid en gegevensbescherming'.

Namens de gemeenteraad:

De adjunct-algemeendirecteur
(get.) Jan Bal

De voorzitter
(get.) Fabienne Blavier

Voor eensluidend uittreksel:
NAMENS DE GEMEENTERAAD:

Bij verordening:

Mechelen, 3 maart 2021

STADSBESTUUR VAN MECHELEN - PROV. ANTWERPEN -

Erik Laga
algemeen directeur

Fabienne Blavier
voorzitter

Gegevensbescherming & Informatieveiligheidsbeleid
Stad en OCMW Mechelen

Beleidsnota

Gebaseerd op de Richtsnoeren Informatieveiligheid
versie 3

Inhoudsopgave

0. Versiebeheer

Het beheer van dit document berust bij het informatieveiligheidsteam van stad Mechelen (juridische entiteiten: Stad en OCMW Mechelen).

Versie	Status	Datum	Auteur(s)	Wijziging(en)	Goedgekeurd
1.0	Definitief	16/03/2016	H. Nys	Voorstelling gemeenschappelijk MAT	n.v.t.
		18/03/2016	H. Nys	Goedkeuring College Burgemeester en Schepenen	Ja
		11/04/2016	H. Nys	Goedkeuring bijzonder comité Algemeen Beleid	Ja
		18/04/2016	H. Nys	Goedkeuring Raad voor Maatschappelijk Welzijn	Ja
		26/04/2016	H. Nys	Goedkeuring Gemeenteraad	Ja
2.0	Definitief	02/03/2018	H. Nys	Goedkeuring College Burgemeester en Schepenen	Ja
		05/03/2018	H. Nys	Vast Bureau	Ja
		19/03/2018	H. Nys	Raad Sociaal Huis	Ja
		27/03/2018	H. Nys	Goedkeuring Gemeenteraad	Ja
2.0	Definitief	17/01/2020	H. Nys	Aanpassen naar nieuwe corporate branding richtlijnen	n.v.t.
3.0.0	Ontwerp versie 3.0	29/05/2020	H. Nys	Actualisatie beleidsnota	n.v.t.
3.0.1	Ontwerp versie 3.0	23/06/2020	H. Nys	Aanpassingen opmerkingen IVT – aanpassen logo	n.v.t.
3.0	Definitief	03/12/2020	H. Nys	Goedkeuring MTeam	Ja
		25/01/2021	H. Nys	Goedkeuring College Burgemeester en Schepenen	Ja
		25/01/2021	H. Nys	Goedkeuring Vast Bureau	Ja
		01/03/2021	H. Nys	Goedkeuring Gemeenteraad	
		01/03/2021	H. Nys	Goedkeuring Raad voor Maatschappelijk Welzijn	

1. Inleiding

1.1 Wat is informatieveiligheid?

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van gebruikte informatiesystemen, processen en de daarin opgeslagen gegevens te beschermen tegen, al dan niet opzettelijk, onheil. Het begrip 'informatieveiligheid' heeft betrekking op:

- **Confidentialiteit**: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- **Integriteit:** het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- **Beschikbaarheid:** het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- **Finaliteit**: het verwerken van informatie vindt plaats met een specifiek en gerechtvaardigd doel;
- **Proportionaliteit**: enkel de relevante, noodzakelijke informatie wordt verwerkt, geen overmatige gegevens;
- **Transparantie**: het is duidelijk welke gegevens, waar en door wie verwerkt worden of werden;

1.2 Risicobenadering

De aanpak van gegevensbescherming en informatieveiligheid is '*risk based*".

Net zoals het preventiebeleid en het beleid inzake organisatiebeheersing (interne controle) is het beleid geschoeid op het regelmatig analyseren van risico's en het evalueren van de effectiviteit en efficiëntie van eerder genomen maatregelen.

1.3 Waarom informatieveiligheid en gegevensbescherming?

Informatie is één van de belangrijkste bedrijfsmiddelen van een lokaal bestuur. Toegankelijke en betrouwbare informatie is essentieel voor een lokaal bestuur, dat zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, dat transparant en proactief verantwoording aflegt aan burgers en raadsleden en dat met minimale middelen maximale resultaten wenst te behalen. De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om draait. Hoe vertrouwelijker de informatie is, hoe meer maatregelen er getroffen moeten worden.

1.4 Reikwijdte en afbakening van informatieveiligheid

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm enzoverder) en alle informatie verwerkende systemen (de programmatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekortschietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn bv: gedragscode veiligheid & privacy, gedragscode e-mail, internet & sociale media, deontologische code, reglement telewerken. Deze handelen over hoe verantwoord om te gaan met gebruik van het internet en e-mail correspondentie.

1.5 Scope

- De scope van dit beleid omvat alle bestuurlijke processen, onderliggende informatiesystemen, informatie en gegevens van het lokaal bestuur, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

- Dit lokaal beleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving mogelijk specifieke (aanvullende) beveiligingseisen.

1.6 Werking

Dit informatieveiligheidsbeleid treedt in werking na goedkeuring en vaststelling door het Vast Bureau (VB) en het College van Burgemeester en Schepenen (CBS).

1.7 Communicatie

Dit informatieveiligheidsbeleid wordt, na goedkeuring, integraal gepubliceerd op de voor “Informatieveiligheid” voorziene pagina op intranet. Op regelmatige basis wordt er via verscheidene kanalen getracht de medewerkers over de gehele organisatie te sensibiliseren om aandacht te besteden aan informatieveiligheid en gegevensbescherming. Bij deze opleidings-, sensibiliserings- of communicatie acties worden een aantal punten uit het beleid uitgelicht, verder uitgewerkt en/of verklaard naar de medewerkers toe.

2. Definities

2.1 Algemene Verordening Gegevensbescherming (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.

Ook wel General Data Protection Regulation of GDPR genoemd.

2.2 Persoonsgegeven(s)

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Als identificeerbaar wordt beschouwd een natuurlijke persoon, die direct of indirect, geïdentificeerd kan worden aan de hand van gegevens zoals naam, identificatienummer, locatiegegevens, online identificator of één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

2.3 Betrokkene

De geïdentificeerde of identificeerbare natuurlijke persoon op wie een Persoonsgegeven betrekking heeft.

2.4 Verwerken/Verwerking

Elke bewerking of geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, alligneren of combineren, afschermen, wissen of vernietigen van gegevens (zoals ook gedefinieerd in artikel 4, 2 AVG).

2.5 Verantwoordelijke voor de verwerking

De natuurlijke persoon of rechtspersoon, overheidsinstelling, dienst of ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen (o.a. budget) voor de verwerking van persoonsgegevens vaststelt.

2.6 Verwerker

De natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of ander orgaan die/dat ten behoeve van de verantwoordelijke voor de verwerking persoonsgegevens verwerkt.

2.7 Verantwoordingsplicht (of Accountability)

Dit beginsel is beter gekend onder zijn Engelse naam: accountability. Het houdt in dat de verantwoordelijke van de verwerking actief verantwoordelijk is opdat de gegevensverwerkingen overeenkomstig de Algemene Verordening Gegevensbescherming zullen geschieden.

2.8 Privacy by Design en (Data) Privacy Impact Assessment

Het Privacy by Design (Gegevensbescherming door Ontwerp) principe zorgt ervoor dat gegevensbescherming standaard ingebouwd wordt in de werking van de organisatie. Dit is een duidelijke wettelijke vereiste van de Algemene Verordening Gegevensbescherming (AVG).

Privacy by Design kan ingebouwd worden door o.a. het maken van een Privacy Impact Analyse. Een Privacy Impact Analyse (PIA) is ook gekend onder de benamingen: (Data) Privacy Impact Assessment (D)PIA of Gegevensbeschermingseffectbeoordeling GEB.

De AVG verplicht het maken van een PIA voor verwerkingen met een waarschijnlijk hoog risico voor de betrokkenen. Dit houdt onder andere in (maar is niet beperkt tot): mogelijke discriminatie, mogelijke identiteitsdiefstal, mogelijkheid dat betrokkenen hun rechten & vrijheden niet kunnen uitoefenen, verwerking van gevoelige of zeer vertrouwelijke persoonsgegevens, evaluatie van persoonlijke aspecten (denk aan bv. automatische profilering).

Het is de bedoeling om risicosituaties op voorhand in te schatten, zodat maatregelen om de risico's te verminderen ingebouwd kunnen worden.

3. Rollen en verantwoordelijkheden

Het lokaal informatieveiligheidsbeleid is bedoeld voor alle interne en externe medewerkers van het lokaal bestuur:

Verantwoordelijke	**Rol m.b.t. Informatieveiligheid & Gegevensbescherming**
Vast Bureau (VB)/College van Burgemeester en Schepenen (CBS)	Integrale verantwoordelijkheid O.a. goedkeuring informatieveiligheidsbeleid en -plan
Raad voor Maatschappelijk Welzijn (RMW) /Gemeenteraad (GR)	Goedkeuring informatieveiligheidsbeleid
Algemeen directeur & adjunct algemeen directeur samen met managementteam	Kaderstelling en implementatie
Directeurs	Kaderstelling en implementatie binnen eigen directie
Betrokken leidinggevende (bv. afdelingshoofd, teamchef, ...)	Sturing op informatieveiligheid en gegevensbescherming Controle op naleving Beoordelen van de risico's Toekennen van de toegangsrechten Invullen en up to date houden register verwerkingsactiviteiten
Gegevenseigenaar (dienst die de gegevens voor de eerste keer binnen de organisatie brengt)	Bepaling van beschermingseisen van informatie aan de hand van dataclassificatie
Functionaris voor Gegevensbescherming of Data Protection Officer (DPO)	Dagelijkse coördinatie (adviseren, stimuleren, documenteren en controleren) van het informatieveiligheidsbeleid en gegevensbescherming Organiseren IVT door o.a. bieden van ondersteuning, verlenen van onafhankelijk advies en uitvoeren van door IVT genomen beslissingen Fungeren als intern en extern aanpreekpunt Adviseren PIA's, overeenkomsten, protocollen en interne procedures Uitbouwen kenniscentrum Auditen werking
Informatieveiligheidsteam (IVT)	Opstellen en implementeren van het informatieveiligheidsbeleid en -plan binnen de organisatie

	Advies vragen aan DPO inzake informatieveiligheid en gegevensbescherming Gemotiveerde beslissingen nemen, waarbij omwille van noodwendigheden kan afgeweken worden van advies DPO Toezien op de gegevensverwerkingen binnen de organisatie Controleren van de naleving van wetgeving m.b.t. gegevensbescherming (o.a. AVG) en de interne regels
Personeelszaken	Arbeidsvoorwaardelijke aspecten
Beheer Gebouwen	Fysieke toegangsbeveiliging
ICT-diensten (en -ontwikkelaars)	Technische beveiliging en gegevensbescherming
Projectmanagers, projecteigenaren, gegevenseigenaren & proceseigenaren	Inbouwen van gegevensbescherming bij ontwerp en uitvoeren van Privacy Impact Analyses (PIA)
Medewerkers	Gedrag en naleving
Leveranciers en ketenpartners	Naleving (compliance)
Auditors	Onafhankelijke toetsing

4. Beleidsverklaring Stad en OCMW Mechelen

Het beleid en management spelen een cruciale rol bij het uitvoeren van dit informatieveiligheidsbeleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor het lokaal bestuur hebben, de risico's die het lokaal bestuur hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatieveiligheid op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

De algemeen directeur en managementteam geven een duidelijke richting aan informatieveiligheid en gegevensbescherming. Door het uitbrengen en handhaven van een informatieveiligheidsbeleid van en voor het hele lokale bestuur demonstreren zij dat zij informatieveiligheid & gegevensbescherming ondersteunen en zich hierbij betrokken voelen. Ze nemen hierbij een voorbeeldfunctie op voor hun medewerkers.

Het informatieveiligheidsbeleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatieveiligheidsbeleid is in lijn met het algemene beleid van het lokaal bestuur en de relevante Europese, Federale en Regionale wet- en regelgeving. Het lokale bestuur is verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid.

Er is toepasselijke wet- en regelgeving op verschillende niveaus, zoals maar niet beperkt tot:
Europees

- 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 of General Data Protection Regulation GDPR)

Federaal

- 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 (Kruispuntbankwet)
- Wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten
- Koninklijk besluit van 16 juli 1992 betreffende het verkrijgen van informatie uit de bevolkingsregisters en uit het vreemdelingenregister.
- Koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid
- Koninklijk besluit van 11 juli 2005 tot bepaling van de datum van inwerkingtreding van het koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid, voor wat betreft de openbare centra voor maatschappelijk welzijn
- Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (organieke wet of WOG)
- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (kaderwet of WVG)
- Wet van 25 november 2018 betreffende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters
- Wet van 5 september 2018 tot oprichting van het informatieveiligheidscomité wet informatieveiligheidscomité) en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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 (
- Gecoördineerde versie van 31 maart 2019 van de algemene onderrichten betreffende het houden van de Bevolkingsregisters

Vlaams

- Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (e-govdecreet) zoals gewijzigd bij het AVGdecreet en het bestuursdecreet
- 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 gegevensverkeer
- Decreet van 8 juni 2018 houdende de aanpassing van de decreten aan de 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 (AVG-decreet)
- Decreet van 7 december 2018 Bestuursdecreet

Daarnaast is er ook een gemeenschappelijk normenkader als basis: “richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens in steden en gemeenten, in instellingen die deel uitmaken van het netwerk dat beheerd wordt door de Kruispuntbank van Sociale Zekerheid en bij de integratie OCMW – Gemeente”.

Het lokaal bestuur stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het ‘pas toe of leg uit’ –principe. Overheidsorganisaties zijn verplicht om de standaarden toe te passen ('pas toe'). Is dit om zwaarwegende redenen niet (volledig) mogelijk, dan moeten zij dit op transparante wijze verantwoorden ('leg uit').

De volgende uitgangspunten zijn ontleend aan de *Norm voor Informatiebeveiliging ISO 27002:2013:*

1. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor het lokaal bestuur. De specifieke verantwoordelijkheden worden beschreven in de rollen;

2. Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatieveiligheidsbeleid vormt samen met het informatieveiligheidsplan het fundament onder een betrouwbare informatievoorziening. In het informatieveiligheidsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, nieuwe wetgeving, registraties in het incidentenregister en bestaande risicoanalyses;

3. Informatieveiligheid is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatieveiligheid;

4. De functionaris voor gegevensbescherming of DPO ondersteunt vanuit een onafhankelijke positie (niet onverenigbaar) de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover aan het dagelijks bestuur;

5. Het lokaal bestuur stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid;

6. Regels en verantwoordelijkheden voor het veiligheidsbeleid dienen te worden vastgelegd en vastgesteld;

7. Alle medewerkers van het lokaal bestuur worden bij hun indiensttreding en daarna op regelmatige basis op de hoogte gesteld van het veiligheidsbeleid d.m.v. gedragscodes, richtlijnen, procedures, opleidingen, intranet en andere gebruikelijke communicatiekanalen, … enzoverder m.b.t. informatieveiligheid & gegevensbescherming;

8. Iedere medewerker, zowel vast als tijdelijk, intern of extern is verplicht
    a. Waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht van gegevens
    b. Is verplicht melding te maken van vermeende inbreuken m.b.t. (mogelijke) ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht van gegevens of informatiesystemen.

Het Informatieveiligheidsbeleid treedt in werking na vaststelling door college van burgemeester en schepenen en vast bureau.

Aldus vastgesteld door het college van burgemeester en schepenen van de Stad Mechelen op 25/01/2021
Aldus vastgesteld door de gemeenteraad van de Stad Mechelen op 01/03/2021

Aldus vastgesteld door het vast bureau van het OCMW Mechelen op 25/01/2021
Aldus vastgesteld door de raad voor maatschappelijk welzijn van het OCMW Mechelen op 01/03/2021

Erik Laga	Alexander Vandersmissen
Algemeen directeur	Burgemeester wd Voorzitter Vast Bureau