STAD MECHELEN
Gemeenteraad – Uittreksel uit de notulen
Vergadering van 27 maart 2018 - Openbare zitting

Aanwezig:

Christiaan Backx, voorzitter
Bart Somers, burgemeester
Marc Hendrickx, Walter Schroons, Greet Geypen, Marina De Bie, Katleen Den Roover, Björn Siffer, Stefaan Deleus, Bart De Nijn, Koen Anciaux, schepenen
Frank Nobels, Frank Creyelman, Ali Salmi, Catherine François, Hans Keldermans, Caroline Gennez, Karel Geys, Hamid Riffi, Fabienne Blavier, Glenn Nason, Alexander Vandersmissen, Kristof Calvo, Tine Van den Brande, Tom Kestens, Melikan Kucam, Martine De Raedemaeker, Rita Van den Bossche, Johan De Vleeshouwer, Patrick Princen, Toon Diependaele, Zineb El Boussaadani, Jan Verbergt, Kerstin Hopf, Patricia Verbeeck, Freya Perdaens, Anne Delvoye, Bert Delanoeije, gemeenteraadsleden
Erik Laga, stadssecretaris

---

9. INFORMATIEVEILIGHEIDSBELEID. Goedkeuring aanpassingen aan het informatieveiligheidsbeleid stad en Sociaal Huis Mechelen in het kader van de nieuwe Europese Algemene Verordening Gegevensbescherming.

De beslissing wordt genomen met eenparigheid van stemmen.

Motivering

Voorgeschiedenis

- In 2015 werd Hilde Nys door de Stad Mechelen en het Sociaal Huis Mechelen aangesteld als informatieveiligheidsconsulente voor zowel de Stad als het Sociaal Huis.
- Op 16 maart 2016 werd het informatieveiligheidsbeleid (versie 1.0) goedgekeurd door het College Burgemeester en Schepenen.
- Op 11 april 2016 werd het informatieveiligheidsbeleid (versie 1.0) goedgekeurd door het bijzonder comité Algemeen Beleid.
- Op 18 april 2016 werd het informatieveiligheidsbeleid (versie 1.0) goedgekeurd door de Raad voor Maatschappelijk Welzijn.
- Op 26 april 2016 (punt 27) werd het informatieveiligheidsbeleid (versie 1.0) goedgekeurd door de Gemeenteraad.
- Op 27 april 2017 treedt de nieuwe Europese privacywet, de Algemene Verordening Gegevensbescherming (AVG of General Data Protection Regulation GDPR) in voege. Deze Europese wetgeving wordt van toepassing vanaf 25 mei 2018. In tussentijd dienen organisaties zich in orde te stellen aan de nieuwe wetgeving.
- Op 2 maart 2018 (punt 28) werd het informatieveiligheidsbeleid (versie 2.0) goedgekeurd door het College Burgemeester en Schepenen en doorverwezen naar de gemeenteraad.
- Op 5 maart 2018 werd het informatieveiligheidsbeleid (versie 2.0) goedgekeurd door het Vast Bureau van het sociaal huis.

Feiten en context

- Het beleid en zijn management spelen een cruciale rol om informatieveiligheid te borgen binnen de organisatie. Zij dienen te demonstreren dat zij informatieveiligheid ondersteunen en zich hierbij betrokken voelen, door het uitbrengen en handhaven van een informatieveiligheidsbeleid van en voor het hele lokale bestuur.
- Het informatieveiligheidsbeleid dient formeel goedgekeurd te worden door het College van Burgemeester en Schepenen & de Gemeenteraad langs de kant van de Stad Mechelen en door het Vast Bureau & de Raad voor Maatschappelijk Welzijn langs de kant van het Sociaal Huis. Zo wordt het normenkader, samen met de rollen & verantwoordelijkheden, vastgelegd.

- Informatieveiligheid draait rond meer dan enkel ICT, computers en automatisering. Het gaat om àlle 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 mensen en processen.
- De volledige beleidsnota wordt ter goedkeuring voorgelegd.

Juridische grond

- Wet houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid. van 15 januari 1990;
- Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Privacywet);
- Koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ter opzichte van de verwerking van persoonsgegevens;
- Vlaamse e-Government Decreet van 18 juli 2008 betreffende het elektronisch bestuurlijk gegevensverkeer;
- Archiefwet van 24 juni 1955 gewijzigd bij wet van 6 mei 2009;
- Besluit van de Vlaamse Regering van 15 mei 2009 betreffende veiligheidsconsulenten;
- Minimale normen Kruispuntbank Sociale Zekerheid van 15 juni 2012;
- Telecomwet herzien op 10 juli 2012;
- 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" versie 3 december 2015;
- 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: Algemene Verordening Gegevensbescherming.

Argumentatie

- Informatieveiligheid is een continu verbeterproces. Het informatieveiligheidsbeleid dient in lijn te zijn met veranderende omstandigheden op allerlei vlakken. In dit geval dient het herbekeken te worden naar aanleiding van de nieuwe Europese Algemene Verordening Gegevensbescherming (AVG of General Data Protection Regulation GDPR). Er werden een aantal specifieke zaken, die in de Europese wetgeving gedefinieerd worden, toegevoegd. Onder andere het aanstellen van een Functionaris voor Gegevensbescherming of Data Protection Officer (DPO). Zo groeien stad en Sociaal Huis steeds meer naar conformiteit met de nieuwe Europese wetgeving.
- De rol van DPO zal opgenomen worden door de huidige informatieveiligheidsconsulente (IVC). De Europese Algemene Verordening Gegevensbescherming verplicht, onder andere overheidsbedrijven, om een DPO aan te stellen.
- Volgende zaken werden gewijzigd ten opzichte van het informatieveiligheidsbeleid versie 1.0.:
  - Toevoeging versiebeheer;
  - Toevoeging specifieke definities uit de Algemene Verordening Gegevensbescherming: persoonsgegeven(s), verantwoordelijke voor de verwerking, verwerker, verantwoordingsplicht, gegevensbescherming door ontwerp en Privacy Impact Analyse (PIA);
  - Benaming "Bijzonder comité Algemeen Beleid" vervangen door "Vast Bureau";
  - Rollen en verantwoordelijkheden:
    - Toevoeging rol adjunct secretaris
    - Toevoeging rol Chief Information Security Officer (CISO)
    - Toevoeging rol Functionaris voor Gegevensbescherming of Data Protection Officer (DPO)
    - Toevoeging verantwoordelijkheid "inbouwen van gegevensbescherming bij ontwerp en uitvoeren van Privacy Impact Analyse (PIA)" voor de rollen projectmanagers, projecteigenaren, gegevenseigenaren & proceseigenaren
    - Aanstellen informatieveiligheidsconsulent (IVC) als functionaris voor gegevensbescherming (DPO).
  - Toevoeging Algemene Verordening Gegevensbescherming bij wet- en regelgeving.

Besluit:

Artikel 1
De gemeenteraad hecht goedkeuring aan de nieuwe beleidsnota met betrekking tot informatieveiligheid en gegevensbescherming en legt zo het normenkader, samen met de rollen & verantwoordelijkheden.

(bijlage)

Namens de gemeenteraad:

De stadssecretaris
(get.) Erik Laga

De voorzitter
(get.) Christiaan Backx

Voor eensluidend uittreksel:
NAMENS DE GEMEENTERAAD:

STADSBESTUUR VAN MECHELEN ★ PROV. ANTWERPEN

Bij verordening:

Erik Laga
stadssecretaris

Mechelen, 29 maart 2018

Christiaan Backx
voorzitter

Informatieveiligheidsbeleid
Stad en Sociaal Huis Mechelen

Beleidsnota

(Information Security Policy – ISP)

Gebaseerd op de Richtsnoeren Informatieveiligheid v.3

Inhoudsopgave

0. Versiebeheer

Het beheer van dit document berust bij het informatieveiligheidsteam van de Stad en het Sociaal Huis Mechelen

Versie	Status	Datum	Auteur(s)	Wijziging(en)	Goedgekeurd
1.0.0	Ontwerp versie 1.0	14/12/2015	F.Leyssens (V-ICT-OR)	Eerste ontwerp na 3-daagse doorlichting op basis van de richtsnoeren v3	n.v.t.
1.0.1	Ontwerp versie 1.0	05/02/2016	H. Nys	Aanpassingen besproken Informatieveiligheidsteam	n.v.t.
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
2.0.0	Ontwerp versie 2.0	31/10/2017	H. Nys	Aanpassingen in kader van Europese Algemene Verordening Gegevensbescherming (AVG/GDPR)	n.v.t.
2.0.1	Ontwerp versie 2.0	12/12/2017	H. Nys	Aanpassingen besproken in informatieveiligheidsteam	n.v.t.
2.0	Definitief	12/02/2018	H. Nys	Definitieve versie ter goedkeuring	n.v.t.

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 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 informatieveiligheidsbeleid 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?

Informatie is één van de belangrijkste bedrijfsmiddelen van een lokaal bestuur. Toegankelijke en betrouwbare overheidsinformatie 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 et cetera) 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 tekort schietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn bv: de internet & e-mail policy, 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).

2. Definities

2.1 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.

2.2 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 voor de verwerking van persoonsgegevens vaststelt.

2.3 Verwerker

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

2.4 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 (AVG of General Data Protection Regulation GDPR) zullen geschieden.

2.5 Gegevensbescherming door ontwerp en Privacy Impact Analyse

Door middel van gegevensbescherming door ontwerp (Privacy by Design) en gegevensbeschermingseffectbeoordelingen (Privacy Impact Assessment of Privacy Impact Analyse PIA) dient gegevensbescherming standaard ingebouwd te worden in de werking van de organisatie. Dit is een duidelijke wettelijke vereiste van de Europese Algemene Verordening Gegevensbescherming (AVG).

Een Privacy Impact Analyse (PIA) moet uitgevoerd worden voor verwerkingen met een waarschijnlijk hoog risico voor de betrokkenen (onder andere: mogelijke discriminatie, mogelijke identiteitsdiefstal, mogelijkheid dat betrokkenen hun rechten & vrijheden niet kunnen uitoefenen, als het gaat om gevoelige persoonsgegevens, evalueren van persoonlijke aspecten, enzoverder). Het houdt in dat risicosituaties op voorhand ingeschat worden, 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:

Doelgroep	**Relevantie voor Informatieveiligheid**
Vast Bureau (VB)/College van Burgemeester en Schepenen (CBS)	Integrale verantwoordelijkheid, goedkeuring informatieveiligheidsbeleid en -plan
Raad voor Maatschappelijk Welzijn (RMW) /Gemeenteraad (GR)	Goedkeuring informatieveiligheidsbeleid
Secretaris & adjunct secretaris	Kaderstelling en implementatie
Proceseigenaar (bv. diensthoofden)	Sturing op informatieveiligheid en controle op naleving. Beoordelen van de risico's en toekennen van de toegangsrechten.
Gegevenseigenaar (dienst die de gegevens voor de eerste keer binnen de organisatie brengt)	Bepaling van beschermingseisen van informatie aan de hand van dataclassificatie

Informatieveiligheidsconsulent (IVC)	Dagelijkse coördinatie (adviseren, stimuleren, documenteren en controleren) van het informatieveiligheidsbeleid en uitwerken plan
Chief Information Security Officer (CISO)	Informatieveiligheidsconsulent wordt bij Kruispuntbank Sociale Zekerheid (KSZ) ook CISO genoemd
Functionaris voor Gegevensbescherming of Data Protection Officer (DPO)	Toezien op de gegevensverwerkingen binnen de organisatie. Controleren van de naleving van de Europese Algemene Verordening Gegevensbescherming (AVG) en de interne regels. Bijstand verlenen bij de uitvoering van Privacy Impact Analyses (PIA), moet op z'n minst het resultaat ervan zien. Bijstand verlenen bij het opmaken van het register van de verwerkingsactiviteiten. Samenwerken met de toezichthoudende autoriteit. Fungeren als contactpersoon, zowel voor interne medewerkers, als externe betrokkenen.
Informatieveiligheidsteam (IVT)	Bijstaan informatieveiligheidsconsulent en/of DPO bij de uitvoering van zijn taken, onder andere opmaak en uitvoering informatieveiligheidsplan
Personeelszaken	Arbeidsvoorwaardelijke aspecten
Facilitair beheer	Fysieke toegangsbeveiliging
ICT-diensten (en -ontwikkelaars)	Technische beveiliging
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

De rol van functionaris voor de gegevensbescherming (DPO) zal voor Stad en Sociaal Huis Mechelen opgenomen worden door de informatieveiligheidsconsulent (IVC).

4. Beleidsverklaring Stad en Sociaal Huis Mechelen

Het beleid en zijn 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 secretaris, samen met zijn management team, geeft een duidelijke richting aan informatieveiligheid en demonstreert dat zij informatieveiligheid ondersteunen en zich hierbij betrokken voelen, door het uitbrengen en handhaven van een informatieveiligheidsbeleid van en voor het hele lokale bestuur. Dit beleid 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 Federale, Regionale en Europese wet- en regelgeving. Het lokale bestuur is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid.

Er is wet- en regelgeving zoals:

- Op Federaal vlak, *de Kruispuntbankwet* van 15/01/1990,
- de *Privacy wet* 8/12/1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens,
- de *minimale wet KSZ* van 15/06/2012
- *Telecomwet* herzien op 10/07/2012.
- Op Europees vlak: 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: *Algemene Verordening Gegevensbescherming*

Aanvullend is er het:

- *Vlaamse e-Government Decreet* van 18/07/2008 betreffende het elektronisch bestuurlijk gegevensverkeer
- *Besluit van de Vlaamse Regering van 15/05/2009 betreffende veiligheidsconsulenten.*

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 management systeem van informatieveiligheid;

4. De informatieveiligheidsconsulent 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. Alle medewerkers van het lokaal bestuur worden getraind in het gebruik van informatieveiligheidsprocedures;

7. Iedere medewerker, zowel vast als tijdelijk, intern of extern is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Het Informatieveiligheidsbeleid treedt in werking na vaststelling door college van Burgemeester en Schepenen en Vast Bureau

Aldus vastgesteld door burgemeester en schepenen van de Stad Mechelen op xx/xx/2018
Aldus vastgesteld door Vast Bureau van het OCMW/Sociaal Huis Mechelen op xx/xx/2018

Erik Laga
Secretaris Stad Mechelen

Bart Somers
Burgemeester Stad Mechelen

Jan Bal
Secretaris Sociaal Huis

Koen Anciaux
Voorzitter Sociaal Huis