MECHELEN

GEMEENTERAAD **STAD MECHELEN**

SCHRIFTELIJK ANTWOORD OP SCHRIFTELIJKE VRAAG BUITEN DE GEMEENTERAADSZITTING

2017/032

Indiener: Rita Van den Bossche

Datum indiening: 27 oktober 2017

Vraag: Implementatie GDPR in de stad Mechelen
Coördinator: Informatieveiligheidsconsulente

Andere bevoegde ambtenaren (diensten): ICT, Beleids- en managementinformatie manager

Antwoord college

Het beleid en management spelen een cruciale rol om informatieveiligheid en gegevensbescherming te borgen binnen de organisatie. Het is zeer belangrijk dat zij informatieveiligheid ondersteunen en zich hierbij betrokken voelen, door het uitbrengen en handhaven van een informatieveiligheidsbeleid van en voor het hele lokale bestuur.

Sinds 2015 hebben we er voor gekozen om een informatieveiligheidsbeleid gezamenlijk uit te werken voor Stad én Sociaal Huis. Een eerste stap in dit proces was het aanstellen in 2015 van Hilde Nys als informatieveiligheidsconsulent (IVC) voor zowel Stad als Sociaal Huis Mechelen. De consulent heeft een adviserende, documenterende, sensibiliserende en intern auditerende taak betreffende informatieveiligheid.

Een volgende stap was het oprichten van een gemeenschappelijk Informatieveiligheidsteam (IVT) voor Stad en Sociaal Huis Mechelen. Daarna werd een informatieveiligheidsbeleid uitgewerkt dat voor Stad en Sociaal Huis Mechelen werd goedgekeurd door het College Burgemeester & Schepenen, het bijzonder comité Algemeen Beleid, de Raad voor Maatschappelijk Welzijn en de Gemeenteraad in april 2016.

In uitvoering van dit informatieveiligheidsbeleid werd een meerjarenplanning informatieveiligheid opgesteld. Dit informatieveiligheidsplan werd goedgekeurd door het College Burgemeester & Schepenen en het bijzonder comité Algemeen Beleid in juli 2016. In het informatieveiligheidsplan wordt de Europese Algemene Verordening Gegevensbescherming (AVG of GDPR

General Data Protection Regulation) mee opgenomen. Dit aan de hand van de het 13 stappen plan dat opgesteld werd door de Privacycommissie.

De Privacycommissie deed op 24 mei 2017 een aanbeveling rond de rol van de DPO (Data Protection Officer) of Functionaris voor de Gegevensbescherming. Hierin stelde ze dat de rol van functionaris opgenomen kan worden door de informatieveiligheidsconsulent. De groep Mechelen is van plan te kiezen voor dit scenario waarbij de rol van functionaris voor gegevensbescherming wordt opgenomen door de informatieveiligheidsconsulent.

Om een goed zicht te krijgen over waar in de organisatie gewerkt wordt met persoonsgegevens en de bijzondere categorie van zeer vertrouwelijke persoonsgegevens is er geopteerd om prioriteit te geven aan het maken van het register van de verwerkingsactiviteiten. Dit register is verplicht onder de nieuwe Europese verordening. Het register zal nuttig zijn om te voldoen aan verschillende verplichtingen (verantwoordingsplicht, documenteren, uitvoeren rechten van de betrokkenen o.a. inzage, enzoverder) van de verordening. Op 14 juni 2017 heeft de Privacycommissie een aanbeveling gedaan over hoe dit register dient opgevat te worden en welke elementen er verplicht in aanwezig moeten zijn.

Momenteel zijn we hiermee aan de slag om een register op te maken voor de groep Mechelen. Gezien de grootte van de groep Mechelen en de verschillende diensten, waarbij er persoonsgegevens verwerkt worden, is dit een grote uitdaging. Het informatieveiligheidsteam zal daarom zich in eerste instantie focussen op de verwerkingsactiviteiten waarbij er grote hoeveelheden persoonsgegevens en/of zeer vertrouwelijke persoonsgegevens verwerkt worden (bijvoorbeeld rijksregister, sociale zekerheid, minderjarigen jonger dan 16 jaar).

In dit kader is dataclassificatie van groot belang. Dataclassificatie is nodig om te bepalen welke informatie binnen welke categorie van gegevens valt. Afhankelijk van de categorie is er meer of minder bescherming nodig van de informatie. Er zijn 4 beschermingsniveaus voorzien:

- Publiek (Openbaar)
- Intern
- Vertrouwelijk (Persoonlijk)
- Zeer vertrouwelijk (Privacygevoelig)

Ondertussen is de Privacycommissie bezig zichzelf te hervormen naar de Belgische Gegevensbeschermingsautoriteit (GBA). Privacycommissie zal nieuwe bevoegdheden krijgen onder de Europese verordening. Vandaar dat zij hun werking aan het herzien en herorganiseren zijn. Tegelijkertijd brengen ze adviezen uit om een aantal zaken binnen de AVG te verduidelijken, zoals bijvoorbeeld de reeds aangehaalde aanbeveling rond het register van de verwerkingsactiviteiten. Ook de zogenoemde "werkgroep 29" is op Europees vlak bezig met het uitbrengen van richtlijnen om de verplichtingen binnen de Europese Verordening te verduidelijken.

Voor een aantal zaken is het nog onduidelijk hoe deze in de praktijk zullen verlopen. Onder andere voor het melden van de datalekken. Wat het informatieveiligheidsteam niet tegenhoudt om alvast zaken voor te bereiden en aan te pakken. Er zullen effectief procedures opgesteld moeten worden onder andere rond de rechten van de betrokkenen (inzage, verbetering, vergetelheid, bezwaar tegen direct marketing en geautomatiseerde besluitvorming & profilering, dataportabiliteit) en het melden van datalekken.

Het melden van incidenten (o.a. datalekken) of mogelijke risico's rond informatieveiligheid is sowieso een belangrijk aandachtspunt. Dit is momenteel reeds in voege binnen de organisatie. Iedereen binnen de organisatie kan meldingen doen, deze worden bijgehouden en opgevolgd in Topdesk door de informatieveiligheidsconsulent. Reeds sinds de aanstelling van de informatieveiligheidsconsulent en de oprichting van het informatieveiligheidsteam worden de belangrijkste incidenten en risico's besproken binnen het informatieveiligheidsteam.

Het bijhouden van het incidentenregiser en de opvolging ervan zal de basis vormen tot het melden van datalekken aan de Privacycommissie. Enkel datalekken, die een inbreuk inhouden voor de rechten en vrijheden van natuurlijke personen, zullen moeten gemeld worden. En dit zonder onredelijke vertraging, uiterlijk binnen 72 uur, nadat er kennis van genomen is.

In bepaalde gevallen zullen ook de betrokkenen zelf ingelicht moeten worden. Dit is het geval wanneer de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De Privacycommissie zal hiervoor, naar alle waarschijnlijkheid, nog verdere richtlijnen (wat wel, wat niet) geven. De wetgeving spreekt van inbreuken op de rechten en vrijheden van natuurlijke personen. Er is (nog) niet gespecifieerd wat deze inhouden en hoe dit geïnterpreteerd dient te worden.

Een tweede belangrijk hulpmiddel in het vermijden en analyseren van eventuele datalekken is het "Gegevensbescherming door Ontwerp"-principe (Privacy By Design) van de Europese verordening en de daarmee samenhangende "Gegevensbeschermingseffectbeoordeling" (Privacy Impact Assessment). Dit houdt in dat er bij nieuwe projecten of wijzigingen helemaal van bij de start privacybescherming dient ingebouwd te worden. Dit is onder de Europese verordening een duidelijke wettelijke vereiste (vroeger aanbeveling). Risicosituaties moeten op voorhand ingeschat worden voor verwerkingen waar persoonsgegevens aan te pas komen en die een waarschijnlijk hoog risico qua gegevensbescherming inhouden. Zo worden gegevensbescherming en maatregelen om risico's (o.a. op datalekken) te verminderen, meegenomen van in het begin.

Er werd de voorbije jaren (en wordt nog steeds) ook werk gemaakt van sensibilisering van de medewerkers en diensten binnen de organisatie. De

informatieveiligheidsconsulent informeert, onder andere via de team- en dienstvergaderingen, de medewerkers over wat informatieveiligheid (inclusief de Europese Verordening) inhoudt. Informatieveiligheid is niet enkel een ICT verhaal, het is een verhaal van en voor iedereen op elk niveau en binnen elke dienst. Sensibilisering, bewustmaking en communicatie op regelmatige basis speelt een grote rol binnen dit verhaal.

Samengevat wil dit zeggen:
- Heeft de stad een databeschermingsbeleid uitgewerkt?
Het informatieveiligheidsbeleid werd goedgekeurd door het College Burgemeester & Schepenen, het bijzonder comité Algemeen Beleid, de Raad voor Maatschappelijk Welzijn en de Gemeenteraad in april 2016. Deze wordt concreter gemaakt naar AVG richtlijnen en zal daarna terug ter goedkeuring voorgelegd worden, ook aan de Gemeenteraad.

- Is er een DPO (Data Protection Officer) aangesteld?
Hilde Nys werd als informatieveiligheidsconsulent aangesteld voor Stad en Sociaal Huis Mechelen. De rol van DPO zal opgenomen worden door de informatieveiligheidsconsulent.

- Op welke manier kunnen inwoners vragen naar de informatie die over henzelf in de stedelijke databanken is opgeslagen?
De procedure zal verder uitgewerkt worden door het informatieveiligheidsteam, deadline is mei 2018.

- Hoe zal de stad verzekeren dat, bij een eventueel lek van persoonlijke gegevens, de betrokkenen hiervan binnen de 72 uur op de hoogte worden gesteld?
De procedure zal verder uitgewerkt worden door het informatieveiligheidsteam, deadline is mei 2018.

Het voldoen aan de AVG is een groeipad dat een aantal jaren in beslag zal nemen. Vorig jaar heeft het informatieveiligheidsteam de eerste stappen gezet. Ook in 2018 zal hier continu aan gewerkt worden. Veel zaken in de wetgeving dienen nog vertaald te worden naar de praktijk. De nieuwe Privacycommissie zal (naast zichzelf reorganiseren naar de Belgische Gegevensbeschermingsautoriteit) een aantal richtlijnen naar interpretatie en werkwijzen opmaken. Hoe de AVG door rechters geïnterpreteerd zal worden, zal pas duidelijk zijn als er ook effectief rechtsspraak volgt. Dat kan pas na mei 2018.

Mechelen,7 november 2017

Erik Laga
stadssecretaris

Opdracht burgemeester
van 29.12.2015, bij toepassing
van artikel 183 gemeentedecreet

Stefaan Deleus
schepen