## Opschrift

**Vergadering van** 12 april 2021

**Nummer:** 2021_MV_00211

**Onderwerp:**
**Mondelinge vraag van raadslid Christophe Peeters: Data gebruiken en beschermen**

**Raadslid(-leden):**
Christophe Peeters -

**Bevoegd:** Sofie Bracke

## Omschrijving van de vraag

**Toelichting:**
Onze samenleving werkt steeds meer datagestuurd, ook ons stadsbeleid kan niet achterblijven. We kunnen door beschikbare data verstandig te gebruiken onze dienstverlening naar de burger namelijk een stuk klantvriendelijker maken. Het zou voor de burger alleszins een meerwaarde zijn als alle mogelijke attesten (burgerlijke stand, omgevingsvergunning,…) op een centrale plaats te vinden zijn.

In uw beleidsnota las ik dat u sterk wil inzetten op die klantvriendelijkheid, o.a. door het 'only once'-principe te hanteren: een burger moet zijn of haar gegevens dan maar één maal overmaken aan de stad, ze worden bij een volgende toepassing of aanvraag automatisch overgenomen. Hetzelfde principe werkt ook over verschillende overheden of partners heen, de stad werkt op dat vlak dan ook samen met het Vlaamse en federale niveau.

Het is ook de ambitie om de burger op die manier te laten weten op welke subsidies of ondersteuning hij of zij mogelijk recht heeft. Door die automatische rechtentoekenning zorgen we er maximaal voor dat ondersteuning ook effectief terechtkomt bij wie er aanspraak op kan maken.

Het is evident dat we met al deze data van burgers en andere klanten ook verstandig moeten omspringen. En ze maximaal moeten beschermen. Kijk maar naar het recente Facebook-lek waarbij de gegevens van 533 miljoen gebruikers, waaronder 3 miljoen Belgen, buitgemaakt werden. Er zijn online nu eenmaal malafide figuren en organisaties die deze data maar al te graag gebruiken om mensen te misleiden, we beschermen onze gegevens dus maar beter zelf.

In uw beleidsnota besteedt u de nodige aandacht aan gegevensbescherming, en uiteraard handelen we als stad bij het verzamelen en de verwerking van persoonsgegevens ook steeds conform de Europese wetgeving ter zake, GDPR.

**Vraag:**
Ziet u nog mogelijke toepassingen om met de data waarover de stad beschikt de dienstverlening nog te verbeteren?

Welke initiatieven werden er al genomen om de beschikbare data maximaal te beschermen? Welke stappen kunnen er nog gezet worden?

Hoe verloopt de samenwerking met de Vlaamse en federale overheid, zowel qua data-uitwisseling i.f.v. proactieve dienstverlening als qua gegevensbescherming?

## Antwoord

- Ziet u nog mogelijke toepassingen om met de data waarover de stad beschikt de dienstverlening nog te verbeteren?

Om de dienstverlening nog te verbeteren door middel van gebruik van data lopen er verschillende initiatieven. Ik som enkele op:

- 'PROBE': door de data die in de College en GR-besluiten zit computer-leesbaar te maken, wordt ze ook toegankelijker voor burgers. Het wordt eenvoudiger om de besluiten te doorzoeken en te achterhalen wat voor hen specifiek van belang is. Dit verbetert zowel de toegankelijkheid van het bestuur, als de transparantie. Omdat dit gaat over data die publiek beschikbaar (moeten) zijn, is hier geen probleem voor GDPR en privacy voorzien.
- Project 'Innovatieve dienstverlening': via dit project wil de Stad Gent inzetten op gepersonaliseerde en proactieve dienstverlening. Een actie trouwens die ook in mijn beleidsnota Publiekszaken vermeld stond. Er wordt gestart met een onderzoekstraject waarbij nagegaan wordt welke databanken er gebruikt kunnen worden, hoe de gegevens extra beschermd kunnen worden, en hoe een burger kan aangeven van welke data de toepassing gebruik mag maken (de toepassing kan je bijvoorbeeld aanraden om een subsidie aan te vragen voor het isoleren van je spouwmuren als die mag weten dat je een aanvraag tot verbouwing ingediend hebt). Maar de burger blijft controle houden, en kan zelf aangeven wat er gebruikt mag worden en wat niet via een persoonlijk profiel. De voornaamste win is dat burgers op deze manier meer gepersonaliseerde dienstverlening krijgen, en weten voor welke subsidies ze in aanmerking komen of welke andere diensten nuttig zouden kunnen zijn voor hun.
- Hierop volgt **het chatbot project**. Deze bouwt voort op het project 'innovatieve dienstverlening'. Naast het eenvoudig kunnen opvragen van informatie, kan de

chatbot met jou ook de stappen doorlopen die ik net benoemde in het project innovatieve dienstverlening. Ook dit project zal bijna aan de onderzoeksfase beginnen.

- Welke initiatieven werden er al genomen om de beschikbare data maximaal te beschermen? Welke stappen kunnen er nog gezet worden?

**Security & systeembeveiliging**

Data beschermen wordt toegepast in verschillende lagen en systemen binnen onze infrastructuur. Om een beter zicht te krijgen op hoe we onze data beschermen is het ook nuttig om te weten tegen welk type bedreigingen we onze data beschermen.

In de maand maart 2021 werden bijvoorbeeld 124 security incidenten gemeld aan de servicedesk door de Groep Gent medewerkers. 94 daarvan werden gecategoriseerd onder 'phishing'. Bij verdere analyse bleek maar liefst 1498 medewerkers een phishing e-mail te hebben ontvangen. Een hacker kan met behulp van dergelijke phishing e-mails toegang krijgen tot de account van een medewerker en op die manier data stelen waar deze medewerker toegang tot heeft. Daarnaast werden ook 8 hoge risico aanmeldingen gedetecteerd door Microsoft op onze O365-omgeving. Microsoft kan, met behulp van Artificiële Intelligentie, detecteren wanneer een aanmelding op een O365-account niet legitiem is door middel van de plaats van het aanmelden (bijvoorbeeld Verenigde Staten of China) en/of het tijdstip (bijvoorbeeld 's nachts in het weekend). Van deze 8 hoge risico aanmeldingen bleken er 6 positieve hacking pogingen tussen te zitten. De overige 19 incidenten hadden te maken met verschillende zaken zoals onbeschikbaarheden, potentiële hacking en gestolen toestellen. Zoals steeds nemen we security incidenten ernstig en pakken we deze met hoge prioriteit op.

Dit met betrekking tot de gemelde security incidenten door medewerkers van Groep Gent en collega's bij District09. Maar onze security infrastructuur houdt hierbij al zeer veel zaken tegen alvorens het terecht komt bij onze medewerkers. Dagelijks worden er gemiddeld 40 000 spam of phishing e-mails onderschept, 1 000 websites geblokkeerd die malware verspreiden en 5 malware geblokkeerd op de pc's van medewerkers. Malware is trouwens elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Om deze bedreigingen te beperken hebben we al verschillende acties en initiatieven ondernomen. We zijn onder andere een phishing campagne gestart in oktober 2020 voor alle medewerkers. Hierbij hebben we specifiek gerichte phishing e-mails gestuurd naar de medewerkers. Na de test hebben we ook informatie gegeven over hoe een phishing e-mail kan gedetecteerd worden en wat de medewerker moet doen in het geval de medewerker een phishing e-mail ontvangt. Daarnaast hebben we in het recente verleden twee security projecten opgestart omtrent GDPR en veilige softwareontwikkeling. Het team Security binnen de dienst IT-Coördinatie van District09 werkt, samen met collega's van de dienst IT services, permanent aan een veilige en betrouwbare IT omgeving. Al blijft security een opdracht voor alle gebruikers.

Om security en privacy correct en proportioneel toe te passen binnen de organisatie is correct beheer en beleid nodig. Om een antwoord te bieden op onze hedendaagse bedreigingen staan er nog een aantal initiatieven op de plank. Concreet hebben we onderzocht hoe we ons netwerk veiliger kunnen maken met behulp van 'Network Access Control' (Dit is een benadering van computerbeveiliging die probeert de technologie voor eindpuntbeveiliging, gebruikers- of systeemverificatie en handhaving van netwerkbeveiliging te verenigen). Daarnaast werd ook een 'e-mail security' initiatief ingediend om de hedendaagse voelbare bedreigingen omtrent e-mail (zoals phishing) te verminderen. Beide zaken staan moeten binnenkort verdere uitvoering kennen (na goedkeuring van de digitaliseringscommissie).

De ambities omtrent security die beschreven staan in mijn beleidsnota 'Meer dan een slimme stad – Data, innovatie en digitalisering' willen we dan ook verder realiseren. We onderzoeken momenteel hoe een Security Operations Center er zou kunnen uitzien in District09. Het spreekt voor zich dat, met behulp van een Security Operations Center, we een beter en completer zicht krijgen op de hedendaagse bedreigingen op de vertrouwelijkheid, integriteit en beschikbaarheid van data en hier ook adequaat naar kunnen handelen. Daarnaast willen we inzetten op ethisch hacken met behulp van betrouwbare en beheersbare ethisch hackerplatformen. Om een veiliger netwerk na te streven wordt gewerkt naar een zerotrust-netwerk. (Met het 'Network Access Control' zetten we hierbij alvast een eerste stap naar een zero-trust netwerk).

**Organisatie en data**

Naast security en systeembeveiliging sluit de organisatie ook mee aan op het 'Burgerprofiel' dat ontwikkeld is door de Vlaamse overheid, en dat open staat voor lokale besturen. In het voorjaar 2021 publiceren we de eerste statussen van Gentse producten binnen dit Burgerprofiel. Het burgerprofiel is enkel te openen met een digitale sleutel (= sterke authenticatie via bvb eID of itsme). Het is een bewuste keuze om statussen van uw dossiers als burger niet in Mijn Gent op te nemen (dat beveiligd is met gebruikersnaam en wachtwoord) en hiervoor dus wel aan te sluiten op het Burgerprofiel omwille van de hogere beveiligingsgraad. Eind 2021 publiceren we de eerste statussen voor producten voor ondernemers in het e-loket voor ondernemers. In het Vlaamse Burgerprofiel kan de burger zelf zijn attesten uit het rijksregister opvragen. Hij kan dit ook via stad.gent, eveneens na sterke authenticatie. Er zullen geleidelijk aan meer en meer producten uit onze dienstverlening gekoppeld worden aan het Burgerprofiel. Op die manier kan de Gentse burger zijn interacties met de Vlaamse/federale en lokale overheid op 1 plek digitaal opvolgen.

Omdat digitaliseringsprojecten te maken kunnen krijgen met het verwerken van persoonsgegevens, geeft onze DPO feedback hierop in de voorbereidende organen. Deze betrokkenheid van de DPO zorgt ervoor dat we preventief te werk kunnen gaan. Dit past volledig binnen het GDPR-principe van 'privacy by design'.

Hoe verloopt de samenwerking met de Vlaamse en federale overheid, zowel qua data-uitwisseling i.f.v. proactieve dienstverlening als qua gegevensbescherming?

Ons Gents project ‘proactieve dienstverlening’ werkt  een oplossing uit om op basis van beschikbare gegevens bij authentieke bronnen, maar ook bij eigen OCMW- en stadsbronnen, onze dienstverlening proactief aan rechthebbenden toe te kennen. Doelstelling is enerzijds om de non-take up van bepaalde rechten tegen te gaan en anderzijds om de administratieve lasten te verminderen en het only-once principe (=1 keer je gegevens geven) te realiseren op een GDPR-conforme werkwijze.

In september vorig jaar kende Stad Gent voor een eerste keer proactief de korting op kinderopvang en kosten in stedelijke scholen automatisch toe aan ouders die een leefloon ontvangen. In april kent  Stad Gent op basis van een bevraging van de Kruispuntbank Sociale Zekerheid (KSZ) aan Gentse burgers met een sociaal statuut gratis huisvuilzakken toe. Bovendien zal voor beide dienstverleningen per kwartaal een nieuwe bevraging van de KSZ gebeuren zodat ook nieuwe rechthebbenden in de toekomst sneller hun rechten krijgen. Hiertoe werd eind maart een nieuwe samenwerkingsovereenkomst met de KSZ ondertekend.

Verder ligt nog een project op de plank *(voetnoot: na goedkeuring op digitaliseringscommissie)* om een fundament uit te bouwen waarbij persoonsgegevens in authentieke bronnen én in eigen Gentse bronnen (bvb OCMW-gegevens over mensen in schuldbemiddeling) op het moment van een aanvraag in realtime afgetoetst worden aan de geldende criteria. Dit zal in het najaar voor UITPAS opgeleverd worden. Zo kunnen we bij aankoop van een UITPAS in realtime controleren of iemand recht heeft op het kansentarief of niet. Een medewerker zal in de uitgewerkte oplossing enkel het advies op basis van de verwerkte data te zien krijgen in plaats van de volledige gegevensset. Eens opgeleverd voor UITPAS zal deze oplossing voor vele andere dienstverleningen snel, en goedkoop opgezet kunnen worden.

De oplossing maakt gebruik van het MAGDA-platform op Vlaams niveau. Uiteraard is de DPO in dit verhaal en in dit project nauw betrokken.

We werken het only-once principe op een GDPR-conforme wijze uit. Daarbij is het weliswaar belangrijk op te merken dat elk concreet initiatief de GDPR-toets doorloopt. Volgens de GDPR mogen persoonsgegevens namelijk enkel verzameld en gebruikt worden voor welbepaalde, uitdrukkelijk omschreven doeleinden; moet elk doeleinde rechtmatig zijn door onder andere een wettelijke grond of de toestemming van de betrokkene; en mogen slechts de gegevens gebruikt worden die strikt noodzakelijk zijn voor het concrete doeleinde. Indien we persoonsgegevens van andere overheden wensen te gebruiken voor een concreet initiatief, dan dient er ook telkens per doeleinde een protocol gesloten te worden die de doorgifte toetst aan alle basisbeginselen van de GDPR.

Tot slot is op vraag van stad Gent en in samenwerking met VVSG, een wetswijziging op federaal niveau goedgekeurd waardoor nu *(voetnoot: we wachten nog op goedkeuring parlement)* ook steden en gemeenten de toegang kunnen krijgen tot fiscale inkomensgegevens van hun burgers.

Via het fundament dat in ons project nu voor UITPAS wordt uitgewerkt zullen we in de toekomst dus ook die fiscale gegevens kunnen bevragen om proactief ook andere rechten aan burgers met een laag inkomen toe te kennen. De samenwerking met andere overheden en de VVSG loopt tot nu toe meestal vlot. We vinden bereidwillige collega's op andere niveaus om samen de nodige protocollen, ter begeleiding van de uitwisseling van persoonsgegevens, op te stellen alsook om de nodige technische en organisatorische maatregelen te nemen ter beveiliging van de persoonsgegevens.

Je ziet, we hebben hier als Stad Gent reeds mooie stappen gezet, mede te danken aan een goede samenwerking tussen collega's van District 09, Data en Informatie en Organisatieontwikkeling en de dichte samenwerking met oa de Vlaamse Overheid.