Hilversum Mediastad

Bescherming van persoonsgegevens

Een onderzoek van de rekenkamer Hilversum

Rekenkamer Hilversum - juni 2021

Inhoudsopgave

1. Bestuurlijk rapport

1.1 Aanleiding en context

Op 25 mei 2018 trad de Algemene Verordening Gegevensbescherming (AVG) in werking. Dit is een Europese Verordening waarin maatregelen en voorschriften zijn opgenomen die betrekking hebben op de bescherming van de persoonsgegevens van alle inwoners van Europa. De Europese verordening heeft directe werking in Nederland. Nu was de verordening zelf al in mei 2016 vastgesteld. Lidstaten hadden dus twee jaar de tijd om de inwerkingtreding voor te bereiden. Ook voor 2016 was het nodige met betrekking tot de bescherming van privacy van burgers in Nederland vastgelegd, zoals bijvoorbeeld in de Wet bescherming persoonsgegevens (Wbp). Alle overheden, waaronder dus ook Hilversum, hadden niet alleen al ervaringen met privacybeleid, zij hadden ook ruim de tijd gehad om zich voor te bereiden op de inwerkingtreding van de AVG.

Kernpunten van de AVG

De AVG bevat de belangrijkste regels voor de omgang met persoonsgegevens door overheden en bedrijven. Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met de wet en met een gerechtvaardigd doel. Bij het verwerken van persoonsgegevens moet een aantal uitgangspunten in acht worden genomen. Zo moeten overheden en bedrijven zo min mogelijk gegevens verwerken en dat binnen een passend beveiligingsregime doen. Zij zijn verwerkingsverantwoordelijk. Overheidsorganen moeten een interne toezichthouder hebben. Dit is de functionaris gegevensbescherming (FG). Ook is er een externe toezichthouder. In Nederland is dat de Autoriteit Persoonsgegevens.

De inwerkingtreding van de AVG gaf veel overheden aanleiding om hun beleid met betrekking tot de bescherming van de persoonsgegevens kritisch te beschouwen en te actualiseren. In ieder geval moeten zij ervoor zorgen dat het lokale beleid in lijn is met de eisen die in de AVG zijn gesteld, zodat burgers ervan uit kunnen gaan dat de overheid zorgvuldig met hun privacygevoelige gegevens omgaat. Als een instantie in gebreke blijft, loopt deze het risico op boetes of - als er zich met betrekking tot de privacy incidenten zouden voordoen - om schadevergoedingen te moeten betalen.

Over de verhouding tussen privacy en de bescherming van persoonsgegevens

Begrippen als privacy en gegevensbescherming worden geregeld als synoniemen gebruikt. Privacy is een mensenrecht en is als zodanig vastgelegd in verschillende mensenrechtenverdragen[1] en in de Grondwet. Het is een recht dat beschermt dat mensen onbespied mogen leven en ruimte moeten krijgen om hun eigen identiteit te vormen.

Het recht op bescherming van persoonsgegevens ziet erop toe dat op een zorgvuldige manier wordt omgegaan met (digitale) persoonsgegevens. Het is daarmee een specifiek onderdeel van het recht op privacy. Dit wordt ook wel informationele privacy genoemd. Persoonsgegevens mogen niet

[1] Art. 8 Europese Verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden (EVRM) en art. 7 en 8 van het Handvest Grondrechten van de EU

zomaar door organisaties worden verwerkt. Als organisaties persoonsgegevens mogen verwerken moeten ze dit op een zorgvuldige, correcte en transparante wijze doen.

Elke gemeente in Nederland verwerkt veel persoonsgegevens om haar taken te kunnen uitvoeren. Zowel binnen de gemeente als met derden worden persoonsgegevens uitgewisseld, een uit privacy-oogpunt altijd kwetsbaar proces. Daarmee lopen gemeenten ook de nodige risico's. Het voorkomen van aantastingen van de privacy van de inwoners is voor hen van groot belang. Overheden moeten zich tot het uiterste inspannen om de bescherming van de privacy te waarborgen.

Deze verantwoordelijkheid is voor de rekenkamer Hilversum aanleiding geweest om het initiatief te nemen voor een onderzoek dat zich richt op de bescherming van persoonsgegevens van de inwoners van Hilversum, de wijze waarop dit in beleid en maatregelen is geregeld en de wijze waarop de gemeente met persoonsgegevens omgaat. De centrale vraag van dit onderzoek is als volgt geformuleerd:

Centrale onderzoeksvraag:

In hoeverre is de bescherming van persoonsgegevens van inwoners van de gemeente Hilversum gewaarborgd, zowel in beleid als in de uitvoeringspraktijk?

Deze centrale vraag is uitgewerkt in de volgende vijf deelvragen:

Onderzoeksvragen	
1	Welk **beleid** hanteert de gemeente Hilversum rond de verwerking van persoonsgegevens, om ervoor te zorgen dat privacy van burgers optimaal en in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) worden beschermd?
2	Hoe is dit beleid uitgewerkt in **regels, procedures en werkprocessen**?
3	Worden deze regels, procedures en werkprocessen in **de dagelijkse uitvoeringspraktijk** ook daadwerkelijk gehanteerd en wordt daarmee voldaan aan **de voorwaarden en vereisten uit de AVG**?
4	Op welke manier wordt de **gemeenteraad** geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te sturen en te controleren?
5	Wat moet de gemeente doen om ervoor te zorgen dat privacy van burgers **optimaal en in overeenstemming met de AVG** wordt beschermd?

Het onderzoek is gestart in het najaar van 2020 en in het voorjaar van 2021 afgerond. In dit eerste hoofdstuk van het rapport, dat geldt als de bestuurlijke rapportage, worden eerst de belangrijkste verkregen inzichten gepresenteerd. Daaraan worden de door de rekenkamer getrokken conclusies verbonden die vervolgens leiden tot de formulering van de aanbevelingen.

1.2 Algemene bevindingen

In het onderzoek is gebleken is dat de uitgangspunten van het privacybeleid van Hilversum voldoen aan de eisen die daar op grond van wet- en regelgeving aan kunnen worden gesteld. Ook heeft de rekenkamer vastgesteld dat dit beleid op een structurele en consequente wijze wordt uitgewerkt in regels en procedures voor de organisatie.

In de dagelijkse uitvoeringspraktijk van dit beleid in Hilversum heeft de rekenkamer verschillende tekortkomingen geconstateerd. Er zijn zeker onderdelen van de organisatie waar er veel en goede aandacht is voor privacy; de medewerkers gaan hier bewust mee om. Maar er zijn redenen om aan te nemen dat dit niet voor de volledige organisatie het geval is.
In de AVG wordt voorgeschreven om beleidsprocessen regelmatig en systematisch te toetsen op een zorgvuldige omgang met de gegevens van inwoners van de gemeente. Hilversum heeft vooralsnog te weinig gevolg gegeven aan deze verplichting.

Raadsleden hebben er behoefte aan om regelmatig over de stand van zaken met betrekking tot privacy geïnformeerd te worden, en daar onderling en met het college van B&W het gesprek over te willen voeren. Het gebruikelijke jaarverslag van de Functionaris Gegevensbescherming zou daarvoor een goede aanleiding kunnen bieden. Tot op heden is de praktijk dat de raad dit verslag louter ter kennisname afdoet.

Deze algemene bevindingen worden in de volgende paragrafen verder uitgewerkt. Dit hoofdstuk wordt afgesloten met de conclusies van dit onderzoek. Vervolgens worden daar enkele aanbevelingen mee verbonden
Een uitgebreide presentatie en beschrijving van de in het kader van dit onderzoek opgedane inzichten en bevindingen zijn opgenomen in het feitelijk deel van deze rapportage. Dit feitelijk deel begint bij hoofdstuk 2.

1.3 Over het privacybeleid van de gemeente

Mede in reactie op de inwerkingtreding van de AVG heeft het college van B en W van Hilversum in maart 2020 het Privacybeleid 2020-2024[2] vastgesteld. Dit beleid vervangt eerder vastgesteld privacybeleid en het privacyreglement 2018-2022. Ten opzichte van het oude beleid is er meer aandacht voor risico-gestuurd werken, de visie van het gemeentebestuur op privacy in het digitale tijdperk en de verbinding met de planning & control-cyclus.
In aansluiting op de AVG worden de wettelijke kaders uitgelicht en wordt ingegaan op de uitgangspunten bij verwerking van persoonsgegevens. Ook worden de verantwoordelijkheden voor de uitvoering van dit beleid toegelicht en wordt beschreven hoe de ondersteuning van medewerkers in de organisatie en controle op de naleving van het beleid plaatsvindt.

Bij de gemeente Hilversum zijn er op drie niveaus rollen verdeeld. In het beleid is vastgelegd dat proceseigenaren - dit zijn vaak de lijnmanagers - binnen de gebruikelijke P&C-cyclus periodiek verslag doen over de naleving van het beleid. Dit wordt in de context van het privacybeleid wel de eerste waarborg of verdedigingslinie van dit beleid genoemd (‘first line of defence’).
De tweede ‘lijn van verdediging’ bestaat in Hilversum uit het Privacy & Informatieveiligheid Team, afgekort als PIT. Dit team ondersteunt, adviseert en coördineert alle voor het privacybeleid relevante activiteiten binnen de organisatie. Het PIT bestaat uit een zogeheten privacy officer, security officer, adviseur informatie en de Chief Information Security Officer (CISO). Door hun coördinerende functie kan dit team bewaken dat binnen de organisatie aandacht is voor privacy en bijsturen als de teamleden van mening zijn dat dit onvoldoende is.

[2] Gemeente Hilversum, Privacybeleid 2020 - 2024

Functie	Functieomschrijving
Privacy officer	De privacy officer is specialist op het gebied van de bescherming van persoonsgegevens, en ondersteunt en adviseert het lijnmanagement vanuit de tweede verdedigingslijn omtrent de bescherming van persoonsgegevens.
Security officer	De security officer is verantwoordelijk voor het vormgeven en bewaken van het informatiebeveiligingsbeleid, en ondersteunt en adviseert het lijnmanagement vanuit de tweede verdedigingslijn/ De SO richt zich op tactische uitwerking van beleid en normen uit de Baseline Informatiebeveiliging Overheid en operationele taken bijvoorbeeld rondom bewustwording binnen de gemeente.
Adviseur informatie	De adviseur Informatie is de kenner op het gebied van de gemeentelijke producten, informatiestromen, processen en informatiesystemen. Hij is de spin in het web en adviseert op vraagstukken die betrekking hebben op de bescherming van persoonsgegevens.
Chief Information Security Officer (CISO)	De CISO heeft een ondersteunende en adviserende rol op het gebied van privacy. Op het gebied van informatiebeveiliging heeft hij een controlerende en toezichthoudende rol.
Teammanager informatiemanagement	De teammanager informatiemanagement, de lijnmanager van de afdeling die zich bezighoudt met gegevensbeheer en gegevensbescherming, maakt eveneens deel uit van het PIT.

In lijn met de AVG heeft het College van B en W een onafhankelijk toezichthouder op de naleving van het privacybeleid aangewezen die op grond van een dienstverleningsovereenkomst zijn werkzaamheden verricht. Dit is de zogeheten Functionaris Gegevensbescherming (FG). In zijn rol als toezichthouder stelt hij vast in hoeverre het privacybeleid van de gemeente voldoet aan de eisen die daar door wet- en regelgeving aan worden gesteld.

Taken van de FG

De FG:

- informeert en adviseert de organisatie over de werking van de AVG, overige wetgeving en het gemeentelijk beleid;
- houdt toezicht op de nakoming van het privacy-beleid en achterliggende wettelijke verplichtingen;
- helpt privacy-klachten tot een goed einde te brengen (ombudsfunctie);
- adviseert bij privacy-incidenten over ernst en omvang;
- ziet toe op het beheer van het register van verwerkingen conform artikel 30 AVG;
- controleert de naleving van afspraken door de gemeente en ketenpartners, eventueel ook in samenwerking met auditors;
- helpt het privacy-beleid uit te dragen en bewustzijn te creëren bij interne en externe doelgroepen;
- is het contactpunt voor landelijke toezichthouders – met name de AP.

Zoals bij veel organisaties gebruikelijk is, vormt in Hilversum de FG de derde ‘verdedigingslijn’. Over zijn bevindingen brengt de FG jaarlijks een verslag uit.

Binnen de gemeente Hilversum is een zogeheten CIO-office ingericht; dit CIO office bestaat nu ongeveer 2 jaar. Een van de directieleden geeft invulling aan de functie van CIO (Chief Information Officer). Het PIT rapporteert een keer per kwartaal aan de CIO. De CIO informeert vervolgens de wethouder tijdens het PHO middels dezelfde kwartaalrapportage.

Voor 2018 was er al privacybeleid binnen de gemeente opgesteld, maar vanwege de AVG moest dit aangepast worden. Met name aan de verplichting om het beleid actief te toetsen en te evalueren, is tot 2020 weinig gevolg gegeven. Met de vaststelling van het Privacybeleid 2020-2024 voldoet de gemeente inmiddels aan de eis uit de AVG[3] dat een 'passend gegevensbeschermingsbeleid' vereist. Daarmee is er een belangrijke stap gezet in het actualiseren van het beleid.

Privacybeleid en informatiebeveiliging

Eén van de eisen uit de AVG is dat een verwerkingsverantwoordelijke, in het geval bij de gemeente gaat het dan om het College van B en W, de burgemeester of de Gemeenteraad, zelf passende technische en organisatorische maatregelen treft om persoonsgegevens te beschermen. Daarmee ontstaat een belangrijke relatie tussen informatiebeveiliging en gegevensbescherming. Door deze eis bestaat er overlap tussen het beschermen van persoonsgegevens en informatieveiligheid. Persoonsgegevens van inwoners van de gemeente Hilversum worden verwerkt met behulp van informatiesystemen die moeten voldoen aan deze 'technische en organisatorische maatregelen'. In het informatiebeveiligingsbeleid wordt aangegeven wat deze maatregelen zijn voor de omgang met informatie. Het informatiebeveiligingsbeleid ziet op de bescherming van alle informatie. Dus *ook* op het beschermen van gegevens die *geen* persoonsgegevens zijn.

Informatiebeveiliging

Voor een organisatie is de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zoals persoonsgegevens) van groot belang. Informatiebeveiliging is het proces van het nemen en beheren van passende technische en organisatorische maatregelen om dit te garanderen. Voor Nederlandse overheden is de Baseline Informatiebeveiliging Overheid (BIO) als normenkader van toepassing. In de BIO zijn (verplichte) beheersmaatregelen opgenomen. Verder gaat de BIO uit van risicomanagement op basis van een Plan-Do-Check-Act cyclus om de beveiliging continu bij te stellen en te verbeteren.

De gemeente Hilversum heeft een Strategisch Informatiebeveiligingsbeleid 2020-2024[4] geformuleerd. Het doel van het Strategisch Informatiebeveiligingsbeleid is om de gemeente een strategisch kader te geven dat gebruikt dient te worden bij de invulling van tactisch en operationeel beleid. In een jaarlijks bij te stellen Informatiebeveiligingsplan wordt het strategisch beleid uitgewerkt in concrete maatregelen.

Het Strategisch Informatiebeveiligingsbeleid beschrijft de uitgangspunten die aan het beleid ten grondslag liggen. Deze uitgangspunten zijn in lijn met de uitgangspunten van het privacybeleid. Zo is vastgelegd dat het college van Burgemeester en Wethouders eindverantwoordelijk is voor informatiebeveiliging. De uitvoering van het beleid is een verantwoordelijkheid van de eigenaren van informatiebronnen en -systemen (c.q. de lijnmanagers). Op dezelfde wijze zoals het privacybeleid dat voorschrijft doen zij periodiek verslag via de P&C-cyclus over de naleving van het beleid (eerste lijn van verdediging). Het beleid gaat verder ook in op de rol van medewerkers: zij dienen verantwoord om te gaan met persoonsgegevens en andere informatie, zij moeten getraind worden in het gebruik van beveiligingsprocedures. De organisatie dient erop toe te zien dat medewerkers kennisnemen van de regels en richtlijnen voor informatiebeveiliging.

[3] Art. 24 AVG lid 2
[4] Gemeente Hilversum, Strategisch Gemeentelijk Informatiebeveiligingsbeleid Hilversum, 2020-2024

Net zoals in het privacybeleid wordt ook ingegaan op de tweede lijn van verdediging en de functionarissen in het PIT. Het PIT heeft nu eveneens een ondersteunende, adviserende en coördinerende rol ten aanzien van informatiebeveiliging. De CISO, die ook deelnemer is aan het PIT, heeft een onafhankelijke positie en vult de derde verdedigingslijn in.[5] De CISO rapporteert aan de directie over informatiebeveiliging, in de tijd afgestemd op de P&C-cyclus.

Het Strategisch Informatiebeveiligingsbeleid beschrijft ook het proces van controle en verantwoording. De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren aan de portefeuillehouder(s).

1.4 Over de uitwerking van het beleid

Procesbeschrijvingen en DPIA's

Verschillende aspecten van het privacybeleid van Hilversum zijn uitgewerkt in regels, procedures en werkprocessen. Een belangrijk aspect van het beleid is dat alle werkprocessen binnen de organisatie worden geïnventariseerd en aangepast op vereisten met betrekking tot privacy en informatiebeveiliging. De coördinatie van deze opdracht wordt ingevuld door het PIT. De verantwoordelijkheid voor het inventariseren van de werkprocessen en daarin aandacht besteden aan het waarborgen van de privacy ligt bij de betrokken lijnmanagers.

Vooralsnog zijn er door de FG dertien werkprocessen geïdentificeerd. De FG heeft in 2018 de organisatie geadviseerd om voor deze processen op basis van een zogeheten DPIA een procesplan op te stellen en te implementeren om zo in die werkprocessen vaste afspraken te maken voor een correcte omgang met privacygevoelige gegevens. Uit diverse jaarverslagen van de FG blijkt dat verschillende van de genoemde processen nog niet (aantoonbaar) zijn onderzocht op mogelijke privacyrisico's.[6]

Wat is een DPIA?

DPIA staat voor *Data Protection Impact Assessment*. Dit wordt ook wel een Gegevens-beschermingseffectbeoordeling of een Privacy Impact Assessment (PIA) genoemd. De AVG vereist dat er in verschillende situaties, bijvoorbeeld bij grootschalige verwerking van persoonsgegevens, vooraf aan die verwerking moet worden bepaald wat het effect van de geplande verwerkingsactiviteit is op de bescherming van de persoonsgegevens van een persoon. Met een DPIA wordt hieraan voldaan. Een DPIA geeft inzicht in de impact van de verwerking op de privacy van deze persoon. Op basis van een DPIA kunnen er maatregelen worden genomen om de impact zo nodig te verminderen. Een DPIA wordt altijd uitgevoerd op een verwerking van *persoons*gegevens.

Verwerkingsregister

In aansluiting op artikel 30 van de AVG dient de gemeente een Verwerkingsregister in te richten. In dat artikel in de AVG wordt gespecificeerd dat het gaat om een integraal overzicht van alle verwerkingen van persoonsgegevens die onder verantwoordelijkheid van de gemeente plaatsvinden.

[5] PIT kwartaalrapportage Q1 2021

[6] Uit in het kader van het onderzoek verkregen informatie blijkt dat er vanaf 2020 vier DPIA's zijn uitgevoerd, twee zich in het stadium van afronding bevinden en er twee in uitvoering zijn. In 2021 zullen er nog drie worden gestart.

In de verslagen van het PIT wordt genoemd dat momenteel (2021) wordt gewerkt aan een verbeterslag en actualisatie van het register.

Coördinatie en planning

De uitvoering van het privacybeleid wordt gemonitord door de Privacy Officer (PO). Die stelt het jaar- en meerjarenplan op. In het Jaarplan 2019-2020[7] zijn de relevante processen, aanbevelingen van de FG, maatregelen voor organisatorische inbedding, acties voor waarborging van de rechten van betrokkenen, samenwerking met derden, maatregelen t.b.v. beveiliging en op welke manier er verantwoording wordt afgelegd opgenomen.

Interne instructies

Een andere uitwerking van het beleid vindt plaats door middel van interne instructies. Interne instructies hebben betrekking op de wijze waarop medewerkers en lijnmanagers inhoudelijke ondersteuning kunnen krijgen bij vragen die leven over privacy, over het waarborgen van privacy in thuiswerksituaties en over de wijze waarop informatie veilig gedeeld kan worden.

Datalekken

Er is een procedure opgesteld die aangeeft wat er moet gebeuren als er sprake is van een zogenaamd datalek. Dit is een situatie waarbij sprake is van vrijgekomen informatie die betrekking heeft op persoonsgegevens en in handen van onbevoegden is gekomen, voor onbevoegden toegankelijk was, of verloren is gegaan.[8] Tussen 2018 en 2020 stijgt het aantal gerapporteerde datalekken van 15 naar 24. Dit wijst volgens geïnterviewden die actief zijn in het PIT niet zozeer op een toenemende onzorgvuldigheid in de omgang met privacygevoelige informatie, maar eerder op een grotere alertheid in de organisatie op mogelijke incidenten.

Uitwerking informatieveiligheidsbeleid

Het Strategisch Informatiebeveiligingsbeleid krijgt een uitwerking in een jaarlijks informatiebeveiligingsplan. In dit informatiebeveiligingsplan zijn concrete tactische en operationele activiteiten uitgewerkt.

In 2020 heeft de gemeente inzichtelijk gemaakt aan welke normen uit de Baseline Informatiebeveiliging Overheid (BIO; zie kader op pagina 4) (nog niet) wordt voldaan. Daarbij is ook in kaart gebracht welke maatregelen genomen moeten worden om wél aan de normen te voldoen.

De gemeente besteedt op verschillende manieren aandacht aan het bewustzijn van medewerkers op het gebied van informatiebeveiliging en de veilige omgang met (persoons)gegevens. In 2020 is gestart met een driejarig bewustwordingsprogramma (het iBewustzijn-traject). Naast de bewustwordingscampagne heeft de gemeente ook een e-learning module over informatiebeveiliging. Alle medewerkers dienen deze module te doorlopen en met goed gevolg af te sluiten. Vrijwel iedereen binnen de gemeente heeft deze module inmiddels afgerond. Deze module is echter nog geen vast onderdeel van het standaard inwerktraject van alle medewerkers.

---

7 Gemeente Hilversum, Jaarplan 2019-2020; in het kader van het onderzoek is ook inzage gekregen in het jaarplan 2021.

8 Gemeente Hilversum, Procedure datalekken – procedure bij melding van een inbreuk in verband met persoonsgegevens (artikel 33 en 34 AVG), 2020

Rapportage en verantwoordingsstructuur
Het PIT stelt elk kwartaal een rapportage op waarin wordt ingegaan op de voortgang in de implementatie van het privacybeleid en het informatiebeveiligingsbeleid. Deze rapportage wordt uitgebracht aan de portefeuillehouder.

In het beleid is vastgelegd dat de FG jaarlijks een verslag opstelt met betrekking tot de stand van zaken op het gebied van privacy. Dit verslag wordt uitgebracht aan het college van B en W.

Korte beschrijving van de inhoud van het (meest recente) jaarverslag van de FG

In het jaarverslag toetst de FG de naleving van de AVG op basis van tien kritieke prestatieindicatoren (KPI). Deze zijn: bestuurlijk beleid; regie & support; toezicht; werkprogramma; ketenregie; privacy by design[9]; verzoeken, klachten en incidenten; communicatie, training en opleiding; informatiebeveiliging en budget. Per KPI beoordeelt de FG de doelmatigheid en doeltreffendheid. Hierbij kijkt de FG naar de opzet (papieren beleid), het bestaan (de maatregelen worden daadwerkelijk in praktijk gebracht) en de werking (de maatregelen blijken in de praktijk voldoende). In het verslag uit 2020[10] is opgenomen hoe de gemeente op deze tien aandachtspunten scoort. Volgens dit verslag is de score op de indicatoren 'Toezicht' en 'verzoeken, klachten en incidenten' 100%[11]. Op aspecten als beleid en werkprogramma digitale duurzaamheid is de score bijna 100%. Er is nog nauwelijks enige vooruitgang geboekt op het implementeren van Privacy by design en het verbeteren van de ketenregie.

Na bespreking van het jaarverslag van de FG in het college van B en W en besluitvorming over de daarin opgenomen aanbevelingen, verstuurt het college van B en W een informatiebrief aan de raad. In de jaarrekening legt het college van B en W verantwoording af aan de gemeenteraad over de realisatie en de toepassing van het privacybeleid in relatie tot informatiebeveiligingsbeleid.

Uitgangspunten bij de communicatie met de burgers
De website van Hilversum bevat een privacyverklaring.[12] In deze verklaring stelt de gemeente inwoners op de hoogte over welke wetgeving van toepassing is en hoe gemeente deze heeft vertaald naar eigen beleid. Tevens wordt aangegeven op welke wijze de gemeente invulling geeft aan de wijze waarop de gegevens van inwoners worden gebruikt. Ook worden inwoners gewezen op de rol en de verantwoordelijkheid van de FG. Daarna legt de gemeente op hoofdlijnen uit dat zij verschillende soorten persoonsgegevens verwerkt en geeft zij een aantal voorbeelden waarom dit nodig is. Ook verschaft de website informatie over bewaartermijnen van persoonsgegevens. Eveneens wordt genoemd dat de gemeente soms persoonsgegevens deelt met andere organisaties. Daarnaast wordt het informatiebeveiligingsbeleid kort toegelicht. Er wordt aangegeven welke rechten inwoners hebben ten aanzien van hun gegevens en hoe er wordt omgegaan met datalekken. Tot slot wordt uitgelegd waar inwoners terechtkunnen met vragen of klachten.

1.5 Over de uitvoeringspraktijk

Voor een goede omgang met privacy kan niet louter worden volstaan met het vastleggen en uitwerken van beleid. In de context van verantwoord privacybeleid wordt geregeld benadrukt dat elke

9 De toelichting hierbij is als volgt in het verslag verwoord: "De AVG-verantwoordelijke draagt ervoor zorg dat aantoonbaar passende maatregelen zijn genomen voor doelmatige en doeltreffende beheersing van risico's."
10 In het kader van het onderzoek is inzage gekregen in het jaarverslag 2020 dat in de vergadering van het college van B en W van 20 april 2021 is besproken. Het collegebesluit en de daaraan gekoppelde raadsinformatiebrief worden ter informatie aan de raad verzonden. In dit verslag maakt de FG melding van positieve ontwikkelingen ten aanzien van het privacybewustzijn in de organisatie.
11 100% staat voor 'Volledig aanwezig en aantoonbaar'
12 https://www.hilversum.nl/Configuratie/Contact_metde_gemeente/Privacyverklaring_gemeente_Hilversum

medewerker zich niet alleen bewust moet zijn van het belang van privacy, maar daar ook, in elke activiteit, naar handelt.

Over de manier waarop medewerkers van de gemeente Hilversum in de dagelijkse praktijk omgaan met privacy zijn in het onderzoek verschillende inzichten verkregen. Om te beginnen is al eerder vastgesteld dat de eerste verantwoordelijkheid voor een goede naleving van het privacybeleid en de daarmee verbonden voorschriften en procedures is belegd bij de lijnmanagers. Dit geeft helderheid wie er moet toezien op de uitvoering van het beleid in de praktijk.

Als er zich vragen voordoen met betrekking tot privacy waarop niet simpel in het beleid een antwoord is te vinden, kunnen medewerkers of hun lijnmanagers een beroep doen op de medewerkers van het PIT. Deze medewerkers beschikken over een goede kennis van het privacybeleid. Wanneer, zelfs na collectieve bespreking van lastige vragen in het PIT, de kennis en ervaring tekortschieten, kan het PIT een beroep doen op juristen werkzaam bij de gemeente of op de FG. Naast zijn toezichthoudende functie heeft de FG ook een adviserende en coachende rol ten aanzien van de organisatie. Medewerkers kunnen zelfstandig contact leggen met de FG. Als eerder genoemd neemt de FG ook met enige regelmaat deel aan de overleggen van het PIT. In dit overleg worden dan de meer urgente risico's besproken.

In het onderzoek is vastgesteld dat er binnen Hilversum geen sprake is van regelmatig overleg tussen lijnmanagers en medewerkers van het PIT. Lijnmanagers worden in hun verantwoordingsprocessen niet bevraagd over hoe zij met de bescherming van persoonsgegevens omgaan of met de informatiebeveiliging. Daarmee blijven de contacten beperkt tot ad hoc vragen. Volgens diverse betrokkenen in de uitvoering zijn er niet genoeg handvatten voor alle werknemers om hun voldoende houvast te bieden hoe zij in hun dagelijks werk met persoonsgegevens moeten omgaan. Er zijn voor hen nog weinig procedures voor werkprocessen opgesteld. Wel wordt gemeld dat de medewerkers in de afgelopen jaren steeds bewuster en zorgvuldiger zijn omgegaan met de bescherming van privacygevoelige gegevens, overigens zonder dat in dit onderzoek kan worden vastgesteld of en in welke mate hiervan daadwerkelijk sprake is. In de uitvoering ervaren sommige medewerkers de AVG als belemmerend voor hun werk. Het PIT stuurt erop dat de AVG eerder als een kwaliteitsinstrument wordt gezien dan een beperkende wet. De AVG kan richtlijnen geven die het werk beter en efficiënter kunnen maken. Deze manier van kijken naar de AVG wordt nog niet door iedereen in de organisatie overgenomen.

In 2019 is vanwege onvoldoende personele capaciteit door ziekte vertraging opgelopen bij de implementatie van de AVG. In de loop van 2020 is onder meer door middel van de inzet van externe ondersteuning een begin gemaakt met het inhalen van de ontstane achterstand. Deze is nog niet ingehaald. Er is nog geen praktijk van het uitvoeren van DPIA's en de beschrijvingen van werkprocessen voor de meeste processen binnen de gemeente missen nog.

1.6 Over de betrokkenheid van de raad

De FG doet conform beleid jaarlijks verslag aan het college van B en W over de stand van zaken met betrekking tot de omgang met privacygevoelige gegevens binnen de gemeente. Het college van B en W verzendt dit verslag ter informatie aan de gemeenteraad. Via de paragraaf bedrijfsvoering in de jaarstukken legt het college van B en W verantwoording af aan de gemeenteraad over de realisatie en de toepassing van het privacybeleid in relatie tot informatiebeveiligingsbeleid.

Een deel van de raadsleden ervaart tekortkomingen in de informatievoorziening over het privacybeleid. Volgens verschillende raadsleden wordt in relevante besluiten te weinig aandacht besteed aan privacyaspecten. Ook ervaren raadsleden het als een tekortkoming dat de raad geen overzicht heeft van privacy-incidenten en datalekken die zich hebben voorgedaan binnen de gemeente. De deelnemers geven aan dat zij graag expliciet over de inrichting en uitvoering van het privacybeleid geïnformeerd willen worden. Impliciet geven zij hiermee aan dat de voor de raad beschikbare rapportages daarin naar hun mening onvoldoende voorzien. In ieder geval hebben zij genoemd dat het voor hen niet voldoende is wanneer beleidsinhoudelijke documenten louter een paragraaf over de privacy bevatten. Natuurlijk geeft dat hun wel inzicht over de wijze waarop rond dat thema aandacht wordt besteed aan privacy. Maar de raadsleden zouden ook over de verschillende thema's heen geïnformeerd willen worden. Het jaarverslag van de FG is daar geschikt voor, maar wordt door de raadsleden niet in dat opzicht herkend en gebruikt.[13]

Verder hechten raadsleden aan een duidelijke en consistente communicatie over de inrichting van het privacybeleid aan de burgers. Burgers moeten nadrukkelijk worden geïnformeerd over hun rechten en wat de gemeente doet (of juist niet doet) met hun persoonlijke gegevens.

1.7 Beantwoording onderzoeksvragen

In het onderzoek is geconstateerd dat Hilversum privacybeleid heeft vastgesteld. Dit is uitgewerkt in regels en procedures. Gebleken is dat er binnen de organisatie ook uitvoering wordt gegeven aan dit beleid, al is die uitvoering niet altijd een direct gevolg van het privacybeleid als zodanig. Het komt soms meer voort uit gewoonten en historie binnen verschillende organisatieonderdelen van de gemeente. Het is lastig een algemeen beeld te schetsen van de gemeente omdat het niveau waarin er uitvoering wordt gegeven aan het beleid sterk verschilt per afdeling en zelfs per team.

Het de gevolgen van het privacybeleid voor de zes werkprocessen binnen de gemeente is (nog) vrijwel geheel niet nader uitgewerkt.[14] Het ontbreekt in het algemeen binnen de organisatie aan relevante basiskennis over privacy. Tegelijkertijd zijn er ook onderdelen binnen de organisatie waar aantoonbaar wordt geanticipeerd op de uitdagingen die besloten liggen op een verstandige omgang met privacy.

Als gekeken wordt naar basisvereisten die voortkomen uit de AVG, dan kan worden vastgesteld dat er sprake is van een onafhankelijke FG, van een verwerkingsregister[15] en een gegevensbeschermingsbeleid. In het beleid worden de rechten van betrokkenen[16] toegelicht. Ook wordt het beleid op verschillende manieren gecommuniceerd aan inwoners.[17] De AVG stelt ook de eis dat er DPIA's worden uitgevoerd.[18] Geconstateerd is dat Hilversum achterloopt als het gaat om het (goed) in kaart hebben van de aandacht voor en bescherming van privacy in de essentiële (dertien) werkprocessen. Dit blijkt uit de jaarverslagen van de FG en het betrekkelijk geringe aantal DPIA's dat is uitgevoerd sinds de inwerkingtreding van de AVG. Tegelijkertijd is vanaf 2020 sprake van een

[13] Het jaarverslag van de FG wordt in eerste instantie aangeboden aan het College van B en W. Na bespreking van dit verslag in het college van B en W en daaraan gekoppelde besluitvorming, informeert het College van B en W de raad hierover door middel van een raadsinformatiebrief. De raadsinformatiebrief die betrekking heeft op het jaarverslag over 2019, is in 2020 ter kennisname, zonder inhoudelijke bespreking, aangenomen door de raad.

[14] Het gaat hierbij om de domeinen Cultuur en sport, Fraudeonderzoek, Gemeenteraadsprocessen, Lokale economie, Milieu en duurzaamheid en Wonen, ruimte en bereikbaarheid.

[15] Art. 30 AVG

[16] Hoofdstuk III AVG

[17] Art. 12 AVG

[18] Art. 35 AVG

inhaalslag. Zo heeft het uitvoeren van de DPIA's nu prioriteit gekregen binnen het privacy-jaarplan. In hoeverre dit daadwerkelijk leidt tot het inhalen van de achterstand op dit aspect van het beleid, kon in dit onderzoek niet worden vastgesteld.

Uit het onderzoek komt tevens naar voren dat het privacybeleid nog weinig in de organisatie is geborgd. Zo heeft niet iedereen binnen de gemeente scherp dat privacy een gedeelde verantwoordelijkheid is die het eigen werk of dat van de afdeling overstijgt.

Op basis van de gepresenteerde bevindingen kunnen de eerste vier[19] van de gestelde onderzoeksvragen nu als volgt worden beantwoord:

Beantwoording onderzoeksvragen[20]	
Vr.	*Welk **beleid** hanteert de gemeente Hilversum rond de verwerking van persoonsgegevens, om ervoor te zorgen dat privacy van burgers optimaal en in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) worden beschermd?*
Antw.	Het beleid van Hilversum met betrekking de privacybescherming van de burgers voldoet aan de (basis)eisen en voorwaarden die daaraan op basis van wet- en regelgeving kunnen worden gesteld.
Vr.	*Hoe is dit beleid uitgewerkt in **regels, procedures en werkprocessen**?*
Antw.	De uitwerking van het privacybeleid in regels, procedures en werkprocessen is planmatig en systematisch ter hand genomen, nadat aanvankelijk vanwege personele wisselingen enige vertraging was ontstaan. Deze uitwerking is nog niet voor alle werkprocessen op orde.
Vr.	*Worden deze regels, procedures en werkprocessen in de **dagelijkse uitvoeringspraktijk** ook daadwerkelijk gehanteerd en wordt daarmee **voldaan aan de voorwaarden en vereisten uit de AVG**?*
Antw.	De uitvoeringspraktijk sluit aan bij het beleid en volgt daarmee de vereisten uit de AVG. Desalniettemin wordt niet volledig voldaan aan alle voorwaarden en vereisten. Het belang van het besteden van aandacht voor de privacy van de burgers is nog niet volledig geïntegreerd in het dagelijks handelen van de medewerkers. Verder schiet de aandacht voor het verrichten van zogenaamde DPIA's tekort. Dit maakt dat de gemeente in de praktijk onvoldoende zicht heeft op de risico's ten aanzien van de bescherming van persoonsgegevens.
Vr.	*Op welke manier **wordt de gemeenteraad geïnformeerd** over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te **sturen en te controleren**?*
Antw.	De gemeenteraad wordt geïnformeerd over de uitvoering van het beleid door middel van het jaarverslag van de FG en daarnaast via de P&C-cyclus. Raadsleden zelf hebben de behoefte uitgebreider en gerichter geïnformeerd te worden, en ook meer specifieke informatie te ontvangen, zoals over privacy-incidenten, datalekken en de wijze waarop burgers worden geïnformeerd over privacy. Ook zouden ze graag zien dat bij relevante beleidsinhoudelijke thema's expliciet wordt gerapporteerd over de aandacht voor privacy.

Met gebruikmaking van de beantwoording van de deelvragen kan ook de centrale vraag worden beantwoord:

[19] Zoals ook bij aanvang is aangegeven, heeft één van de onderzoeksvragen veeleer betrekking op aanbevelingen die uit de constateringen volgen. Deze beantwoording van deze paragraaf komt daarmee in de volgende paragraaf aan de orde.
[20] Onderzoeksvraag 5 wordt in 1.7 beantwoord.

Centrale onderzoeksvraag en - antwoord

Vr.	*In hoeverre is de bescherming van persoonsgegevens van inwoners van de gemeente Hilversum gewaarborgd, zowel in beleid als in de uitvoeringspraktijk?*
Antw.	Geconstateerd is dat de bescherming van persoonsgegevens van inwoners van de gemeente Hilversum in de basis voldoende is gewaarborgd. Het beleid voldoet aan de eisen die vanuit wet- en regelgeving daaraan worden gesteld. Ook wordt het beleid gestructureerd en gecoördineerd uitgewerkt, geïmplementeerd en gemonitord in de organisatie. Wel is tussen 2018-2020 vertraging opgetreden, hetgeen er toe leidt dat er momenteel in de uitvoeringspraktijk sprake is van achterstanden en tekortkomingen.

1.8 Conclusies en aanbevelingen

- Het beleid voldoet
In het onderzoek is vastgesteld dat het privacybeleid van de gemeente Hilversum op hoofdlijnen staat. Deze algemene bevinding is ook getoetst aan het vooraf in het kader van het onderzoek door de rekenkamer opgestelde normenkader. Het overzicht daarvan is opgenomen in bijlage C. Uit deze bijlage blijkt dat Hilversum weliswaar grotendeels, maar niet volledig voldoet aan de gestelde normen.

- De focus ligt sterk op de eigen organisatie, de raad is minder in beeld
Er is geconstateerd dat momenteel de focus in de organisatie sterk is gericht op het realiseren van een aanvaardbaar niveau van gegevensbescherming in de organisatie. Het belang van het informeren en betrekken van de gemeenteraad bij het beleid is op de achtergrond geraakt.

- Er zijn risico's, maar die zijn beheersbaar
Niet alle risico's met betrekking tot de bescherming van de privacy van de inwoners van Hilversum zijn afgedekt. Dit komt onder meer naar voren uit het gegeven dat nog niet alle essentiële werkprocessen zijn getoetst op een juiste omgang met privacygevoelige aspecten. In de context van het onderzoek is gemeld dat het privacybewustzijn van medewerkers toeneemt, maar dat er toch redenen zijn om aan te nemen dat er in de volle breedte van de organisatie nog onvoldoende sprake is van een goede benadering en dagelijkse omgang met privacy. Er kan daardoor nog steeds dagelijks sprake zijn van een onzorgvuldige omgang met persoonsgegevens. Concreet zijn er de volgende risico's:

- Incidenten en gebleken tekortkomingen kunnen ten minste leiden tot negatieve beeldvorming rond het functioneren van de gemeente;
- Ingrijpende incidenten of tekortkomingen kunnen leiden tot schadeclaims van gedupeerden of boetes vanuit toezichthoudende instanties zoals de AP;
- Een onzorgvuldige omgang met informatie en het beheer daarvan kan er ook toe leiden dat er op grotere schaal sprake is van datalekken, dat de gemeente kwetsbaar wordt voor diefstal van privacygevoelige gegevens of hacks door externe - meestal kwaadwillende - organisaties.

Het noemen van deze tekortkomingen en risico's laat toch onverlet dat in het algemeen de gemeente voldoet aan de minimum vereisten van de AVG. De hierboven genoemde risico's zijn aanwezig, maar er zijn in dit onderzoek geen concrete voorbeelden gevonden van ingrijpende incidenten of een opzettelijke onzorgvuldige omgang van persoonsgegevens.

- Aanbevelingen
De geconstateerde tekortkomingen vragen om de nodige aanbevelingen vanuit de rekenkamer. De aanbevelingen vormen tevens een antwoord op deelvraag vijf: wat moet de gemeente doen om ervoor te zorgen dat privacy van burgers optimaal en in overeenstemming met de AVG wordt beschermd?

De rekenkamer doet de volgende aanbevelingen aan **het college van B en W**:

- Het is noodzakelijk om te blijven sturen op het inlopen van de eerder ontstane achterstanden. Dit is met name de uitwerking van alle relevante instructies en procedures en de geregelde uitvoering van DPIA's, en de actualisatie van het verwerkingsregister.
- Over de volle breedte van de organisatie, c.q. bij elke medewerker, dient permanent aandacht te worden besteed aan het bevorderen van het bewustzijn om in het dagelijks handelen correct en prudent om te gaan met gevoelige informatie van de inwoners.
- Benadruk in dat verband de belangrijke rol die lijnmanagers hebben in het bieden van een eerste waarborg dat dit gebeurt. Dit kan onder meer gebeuren door privacy expliciet onderdeel te maken van het inwerktraject van nieuwe medewerkers. In de periodieke beoordelingscyclus dient eveneens structureel aandacht te zijn voor de wijze waarop medewerkers blijk geven van privacybewustzijn. Dit kan bijvoorbeeld door in dit gesprek na te gaan of de medewerker (aangeboden) cursussen heeft gevolgd of in te gaan op de mate waarin de medewerker vastgestelde werkprocessen en richtlijnen volgt.
- Ga in gesprek met de raad over de gewenste inrichting van de informatievoorziening ten behoeve van de raad. Dat betreft zowel het niveau van de informatie als de frequentie waarin de raad geïnformeerd wordt.
  - Onder meer zou een jaarlijkse themapresentatie (bijvoorbeeld op de dag van de privacy) kunnen worden overwogen, waarbij de FG of de PO de raad meeneemt in werkwijzen en dilemma's rond een specifieke casus.
  - Agendeer het jaarverslag van de FG ter bespreking in de raad.
  - Besteed bij beleidsinhoudelijke onderwerpen expliciet aandacht aan de positie van privacy binnen dit onderwerp. Dat is in het bijzonder relevant bij behandeling van onderwerpen in het sociaal domein of in het kader van 'Smart City'.

Aan de gemeenteraad doet de rekenkamer de volgende aanbeveling:

- Besteed proactief aandacht aan de informatie die nu al beschikbaar is voor de raad. Agendeer en bespreek deze informatie.

2. Inrichting van het onderzoek

In de inwerkingtreding van de Algemene Verordening Gegevensbescherming in mei 2018 hebben veel overheden, het Rijk, provincies, waterschappen en gemeenten, aanleiding gezien om hun privacybeleid te actualiseren. Dit betrof ook Hilversum. Deze ontwikkeling maakt aandacht voor de actuele stand van zaken in het gemeentelijk privacybeleid een relevant thema voor een onderzoek door een (lokale) rekenkamer. Immers, wet- en regelgeving stellen de norm waaraan lokaal beleid moet voldoen. Voor elk rekenkameronderzoek is het dan relevant om daadwerkelijk te onderzoeken of dat het geval is.

De bescherming van de persoonsgegevens van inwoners is ook een onderwerp met een groot maatschappelijk belang: privacy is een grondrecht voor alle inwoners. De overheid moet zich daarom tot het uiterste inspannen om de bescherming van de privacy te waarborgen. Dit geldt ook voor gemeenten. Elke gemeente in Nederland beheert en verwerkt veel persoonsgegevens om haar taken te kunnen uitvoeren. Zowel binnen de gemeente als met derden worden persoonsgegevens van haar burgers uitgewisseld, een uit privacy-oogpunt altijd kwetsbaar proces. Daarmee lopen gemeenten ook de nodige risico's. Het voorkomen van aantastingen van de privacy van de inwoners is voor hen van groot belang.

De rekenkamer Hilversum heeft daarom een onderzoek uitgevoerd dat zich richt op de bescherming van persoonsgegevens van de inwoners van Hilversum, de wijze waarop dit in beleid en maatregelen is geregeld en de wijze waarop de uitvoering met persoonsgegevens omgaat. Het onderzoek betreft de gehele gemeente. Door middel van twee casestudies is nadere aandacht besteed aan het beleid en de uitvoering van de Participatiewet en Smart City.

De hoofdvraag van dit onderzoek is als volgt:

In hoeverre is de bescherming van persoonsgegevens van inwoners van de gemeente Hilversum gewaarborgd, zowel in beleid als in de uitvoeringspraktijk?

Deze centrale vraag is vertaald naar vijf deelvragen:

	Onderzoeksvragen
1	Welk **beleid** hanteert de gemeente Hilversum rond de verwerking van persoonsgegevens, om ervoor te zorgen dat privacy van burgers optimaal en in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) worden beschermd?
2	Hoe is dit beleid uitgewerkt in **regels, procedures en werkprocessen**?
3	Worden deze regels, procedures en werkprocessen in **de dagelijkse uitvoeringspraktijk** ook daadwerkelijk gehanteerd en wordt daarmee voldaan **aan de voorwaarden en vereisten uit de AVG**?
4	Zo nee, wat moet de gemeente doen om ervoor te zorgen dat privacy van burgers optimaal en in overeenstemming met de AVG wordt beschermd?
5	Op welke manier wordt **de gemeenteraad geïnformeerd** over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om **te sturen en te controleren**?

In onderzoeken van rekenkamers is het gebruikelijk om te werken met een normenkader. Dit biedt de mogelijkheid om de bevindingen mee te beoordelen. Zo'n normenkader wordt opgesteld aan de hand van bestaande inzichten en eerdere studies over wat verantwoord is rond dit specifieke onderwerp. Dit heeft geresulteerd in het volgende normenkader. In bijlage C wordt verslag gedaan van de toetsing van de bevindingen aan de opgestelde normen.

Normen

Gemeentelijk beleid (onderzoeksvragen 1, 2 en 3)

- Het gemeentelijk beleid voldoet tenminste aan de eisen die in wet- en regelgeving worden gesteld: generiek aan de AVG, en specifiek voor de genoemde materiewetten.
- In het gemeentelijk beleid wordt ingegaan op:
  - Juridische aspecten op basis van de AVG en de materiewetten.
  - Vertaling naar de beleidskaders privacy.
  - Organisatie, taken en verantwoordelijkheden.
  - Inrichting werkprocessen.
  - De toepassing van informatiesystemen en ICT.
  - De gegevens- en informatiestromen.
  - De positie van en communicatie met de burger.
- De gemeente hanteert landelijke standaarden, zoals de Baseline Informatiebeveiliging Overheid (BIO).
- In de procesbeschrijvingen en instructies is duidelijk welke functionaris welke gegevens in welke processtap mag verwerken, en onder welke condities dat mag.
- De gemeente heeft beleid voor incidenten waarbij sprake is van schending van de privacy van inwoners. Dit beleid voldoet aan de wettelijke vereisten.
- De gemeente verschaft aan burgers schriftelijk en mondeling begrijpelijke informatie over het gebruik van hun persoonsgegevens, zowel in algemene zin als afgestemd op de verschillende fasen in het dienstverleningsproces. Daarbij wordt aangegeven met welk doel dit gebeurt, wie inzage heeft en wat er vervolgens met de gegevens gebeurt.
- De gemeente informeert de burger op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling.

Leren en verbeteren (onderzoeksvraag 4)

- De gemeente heeft vastgelegd hoe en wanneer medewerkers worden getraind in/ er aandacht besteed wordt aan het onderwerp privacy.
- Het toezicht op gebruik van persoonsgegevens is vastgelegd in een controleplan, waarin onder meer staat: hoe dit proces verloopt, de periodiciteit van de controles, wie daarbij betrokken zijn (functienamen en persoonsnamen), wie controles uitvoert, aan wie wordt gerapporteerd, hoe de resultaten worden vastgelegd, wat de criteria zijn voor vervolgstappen, welke de vervolgstappen kunnen zijn en wie die neemt.
- Het controleplan sluit aan op het gemeentelijk beveiligingsplan en op het Integriteitsbeleid.
- De medewerkers zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens.
- In de praktijk wordt gehandeld conform de wijze waarop de bescherming van de persoonsgegevens is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming.
- De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt.
- De gemeente heeft een routine voor het meten en verbeteren van de bescherming van persoonsgegevens en legt vast wat de bevindingen en maatregelen zijn. Deze routine is al tenminste één keer uitgevoerd.

Kaderstellende en controlerende rol van de raad (onderzoeksvraag 5)

- In de bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop een correcte omgang met persoonsgegevens is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles.
- Bij de ontwikkeling van beleid heeft aandacht voor het waarborgen van privacy op de agenda van de raad gestaan.

Het onderzoek is begonnen met een startbijeenkomst met de direct betrokken ambtenaren. In deze bijeenkomst is ingegaan op de inrichting van het onderzoek en zijn afspraken gemaakt over het verkrijgen van de relevante documenten en het interviewen van de relevante functionarissen.

Om inzicht te krijgen in het beleid is kennisgenomen van de relevante beleidsdocumenten van de gemeente. Deze documentenanalyse is aangevuld met een aantal gesprekken met functionarissen binnen de gemeente die betrokken zijn bij het opstellen van de relevante beleidsdocumenten en het doorvoeren van de aanpassingen. Een overzicht van de geïnterviewde personen is opgenomen in Bijlage A.

Om meer inzicht te krijgen in zowel de heersende organisatiecultuur met betrekking tot privacy als in de dagelijkse uitvoeringspraktijk zijn twee korte casestudies uitgevoerd. Eén over Hilversum als ‘Smart City’ en één over de rol van privacy bij de Participatiewet. In deze casussen is de omgang met vertrouwelijke gegevens binnen een proces of werkgebied (met de betrokken functionarissen) geïnventariseerd en beoordeeld. In deze twee casestudies is nader onderzocht hoe privacy geborgd wordt, zowel binnen de eigen organisatie als in de relatie met de inwoners.

De navolgende feitelijke hoofdstukken 3, 4, 5 en 6 sluiten steeds aan bij de verschillende relevante onderzoeksvragen. Aan onderzoeksvraag 4 is geen feitenhoofdstuk verbonden, omdat deze vraag betrekking heeft op de aanbevelingen die uit het onderzoek volgen.

3. Het gemeentelijk beleid

Mede in reactie op de inwerkingtreding van de AVG heeft de gemeente Hilversum in maart 2020 het Privacybeleid 2020-2024[21] vastgesteld. Dit beleid vervangt het eerdere privacybeleid en reglement 2018-2022. Ten opzichte van het oude beleid is er meer aandacht voor risico-gestuurd werken, de visie van het gemeentebestuur in het digitale tijdperk en de verbinding met de planning & control-cyclus. Het privacybeleid is opgesteld door het college van Burgemeester en Wethouders. In het Privacybeleid wordt expliciet gesteld dat de verantwoordelijkheid om de uitvoering van het beleid te controleren berust bij de gemeenteraad.

In aansluiting op de AVG worden de wettelijke kaders uitgelicht en wordt ingegaan op de uitgangspunten bij verwerking van persoonsgegevens. Ook worden de verantwoordelijkheden voor de uitvoering van dit beleid toegelicht en wordt beschreven hoe de ondersteuning van medewerkers in de organisatie en controle op de naleving van het beleid plaatsvindt.
Gesteld wordt dat het college van B en W integraal verantwoordelijk is voor de zorgvuldigheid van verwerking van persoonsgegevens. De uitvoeringsverantwoordelijkheid voor gegevensbescherming ligt bij de gemeentesecretaris. De algemeen directeur is samen met de directie verantwoordelijk voor de uitvoering van het aan het privacybeleid verbonden meerjarenplan. Kernpunten in het privacybeleid zijn een juiste uitvoering van privacybeleid en het sturen op risico's. De zorgvuldige omgang van verwerkingen, oftewel hoe persoonsgegevens worden opgeslagen, uitgewisseld en verwijderd, vallen onder de lijnmanagers (proceseigenaar) binnen de verschillende vakafdelingen. Medewerkers zijn er elk voor verantwoordelijk dat zorgvuldig wordt omgegaan met persoonsgegevens.

In het beleid is eveneens vastgelegd dat proceseigenaren - dit zijn vaak de lijnmanagers - binnen de gemeentelijke vastgestelde P&C-cyclus periodiek verslag doen over de naleving van het beleid. Dit wordt in de context van het privacy-beleid wel de eerste waarborg of verdedigingslinie van dit beleid genoemd ('first line of defence'). Op deze wijze wordt de gemeenteraad geïnformeerd en kan zo nodig ook invulling geven aan de controlerende verantwoordelijkheid van de gemeenteraad.

De tweede 'lijn van verdediging' bestaat in Hilversum uit het zogeheten Privacy & Informatieveiligheid Team, afgekort als PIT. Dit team ondersteunt, adviseert en coördineert alle voor het privacybeleid relevante activiteiten binnen de organisatie. Het PIT bestaat een zogeheten Privacy Officer, Security Officer, Adviseur Informatie en de Chief Information Security Officer (CISO). Door hun coördinerende functie kan dit team bewaken dat binnen de organisatie aandacht is voor privacy en bijsturen als de teamleden van mening zijn dat dit onvoldoende is.

[21] Gemeente Hilversum, Privacybeleid 2020 - 2024

Functies binnen het Privacy en Informatieveiligheid Team

Functie	Functieomschrijving
Privacy Officer	De Privacy Officer is specialist op het gebied van de bescherming van persoonsgegevens, en ondersteunt en adviseert het lijnmanagement vanuit de tweede verdedigingslijn omtrent de bescherming van persoonsgegevens. De privacy Officer adviseert de organisatie bij vragen op het gebied van bescherming van persoonsgegevens.
Security Officer	De Security Officer is verantwoordelijk voor het vormgeven en bewaken van het informatiebeveiligingsbeleid, en ondersteunt en adviseert het lijnmanagement vanuit de tweede verdedigingslijn. De Security Officer richt zich op de tactische uitwerking van beleid en normen uit de Baseline Informatiebeveiliging Overheid en operationele taken bijvoorbeeld rondom bewustwording binnen de gemeente.
Adviseur Informatie	De Adviseur Informatie is de kenner op het gebied van de gemeentelijke producten, informatiestromen, processen en informatiesystemen. Hij is de spin in het web en adviseert op vraagstukken die betrekking hebben op de bescherming van persoonsgegevens.
Chief Information Security Officer (CISO)	De CISO heeft een ondersteunende en adviserende rol op het gebied van privacy. Op het gebied van informatiebeveiliging heeft hij een controlerende en toezichthoudende rol.
Teammanager Informatiemanagement	De Teammanager Informatiemanagement, de lijnmanager van het team dat zich bezighoudt met gegevensbeheer en gegevensbescherming, maakt eveneens deel uit van het PIT.

Binnen de gemeente is sinds twee jaar een zogeheten CIO-office ingericht. CIO is de afkorting voor Chief Information Officer. Hiermee wordt een functionaris bedoeld die op directieniveau verantwoordelijk is voor het informatiebeleid. Hiertoe behoren zowel het privacybeleid als het informatiebeveiligingsbeleid. Het PIT rapporteert een keer per kwartaal aan de CIO.

In lijn met de AVG heeft het college van B en W een onafhankelijk toezichthouder op de naleving van het privacybeleid aangewezen, die op grond van een dienstverleningsovereenkomst zijn werkzaamheden verricht. Dit is de zogeheten Functionaris Gegevensbescherming (FG). In zijn rol als toezichthouder stelt hij vast in hoeverre het privacybeleid van de gemeente voldoet aan de eisen die daar door wet- en regelgeving aan worden gesteld.

Taken van de FG

De FG:

- informeert en adviseert de organisatie over de werking van de AVG, overige wetgeving en het gemeentelijk beleid;
- houdt toezicht op de nakoming van het privacy beleid en achterliggende wettelijke verplichtingen;
- helpt privacy-klachten tot een goed einde te brengen (ombudsfunctie);
- adviseert bij privacy-incidenten over ernst en omvang;
- ziet toe op het beheer van het register van verwerkingen conform artikel 30 AVG;
- controleert de naleving van afspraken door de gemeente en ketenpartners, eventueel ook in samenwerking met auditors;
- helpt het privacy beleid uit te dragen en bewustzijn te creëren bij interne en externe doelgroepen;
- is het contactpunt voor landelijke toezichthouders – met name de AP.

De FG vormt in Hilversum de derde ‘verdedigingslijn’. Over zijn bevindingen brengt de FG jaarlijks een verslag uit.

De totstandkoming van het privacybeleid is, in overleg met de betrokken portefeuillehouders, voorbereid door een ambtelijke werkgroep. Het functioneren van deze werkgroep is kort na aanvang beperkt door de uitval van de privacy officer. Eerst is afgewacht op welke termijn deze functionaris mogelijk weer actief zou worden. Al met al hebben de voorbereidingen op de actualisatie van het gemeentelijk privacybeleid daarmee langere tijd in beslag genomen dan oorspronkelijk voorzien. Voor 2018 was er al privacybeleid binnen de gemeente opgesteld, maar in het jaarverslag over 2018 heeft de FG aangedrongen op actualisering van dit beleid. Dit heeft tot 2020 vertraging opgelopen door de personele uitval, met name daar waar het gaat om de verplichting vanuit de AVG om het beleid actief te toetsen en te evalueren. Met de vaststelling van het Privacybeleid 2020-2024 voldoet de gemeente aan de eis uit de AVG[22] dat een ‘passend gegevensbeschermingsbeleid’ vereist en is er een belangrijke stap gezet in het actualiseren van het beleid. Dit nieuwe beleid wordt actief gemonitord door het PIT dat waar nodig extra maatregelen neemt t.a.v. privacy en informatiebeveiliging.

Privacybeleid en informatiebeveiliging

Eén van de eisen uit de AVG is dat het verwerkingsverantwoordelijke bestuursorgaan (in het geval van de gemeente kan dat het College van B&W zijn of de gemeenteraad) passende technische en organisatorische maatregelen treft om persoonsgegevens te beschermen. Daarmee ontstaat een belangrijke relatie tussen informatiebeveiliging en gegevensbescherming. Door deze eis bestaat er overlap tussen het beschermen van persoonsgegevens en informatieveiligheid. Persoonsgegevens van inwoners van de gemeente Hilversum worden verwerkt met behulp van informatiesystemen die moeten voldoen aan deze ‘technische en organisatorische maatregelen’. In het informatiebeveiligingsbeleid wordt aangegeven wat deze maatregelen zijn voor de omgang met informatie. Het informatiebeveiligingsbeleid ziet op de bescherming van alle informatie. Dus *ook* op het beschermen van gegevens die *geen* persoonsgegevens zijn.

Informatiebeveiliging

Voor een organisatie is de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zoals persoonsgegevens) van groot belang. Informatiebeveiliging is het proces van het nemen en beheren van passende technische en organisatorische maatregelen om dit te garanderen. Voor Nederlandse overheden is de Baseline Informatiebeveiliging Overheid (BIO) als normenkader van toepassing. In de BIO zijn (verplichte) beheersmaatregelen opgenomen. Verder gaat de BIO uit van risicomanagement op basis van een Plan-Do-Check-Act cyclus om de beveiliging continu bij te stellen en te verbeteren.

De gemeente Hilversum heeft een Strategisch Informatiebeveiligingsbeleid 2020-2024[23] geformuleerd. Dit beleidsdocument vervangt het Informatiebeveiligingsbeleid 2015-2018. Het doel van het Strategisch Informatiebeveiligingsbeleid is om de gemeente een strategisch kader te geven dat gebruikt dient te worden bij de invulling van tactisch en operationeel beleid. In een jaarlijks bij te stellen Informatiebeveiligingsplan wordt het strategisch beleid uitgewerkt in concrete maatregelen.

[22] Art. 24 AVG lid 2

[23] Gemeente Hilversum, Strategisch Gemeentelijk Informatiebeveiligingsbeleid Hilversum, 2020-2024. Vastgesteld door het College van Burgermeester en Wethouders op 17 maart 2020.

Het Strategisch Informatiebeveiligingsbeleid beschrijft de uitgangspunten die aan het beleid ten grondslag liggen. Deze uitgangspunten zijn in lijn met de uitgangspunten van het privacybeleid. Zo is vastgelegd dat het college van Burgemeester en Wethouders eindverantwoordelijk is voor informatiebeveiliging. De uitvoering van het beleid is een verantwoordelijkheid van de eigenaren van informatiebronnen en -systemen (een lijnmanager). Op dezelfde wijze zoals het privacybeleid dat voorschrijft doen zij periodiek verslag via de P&C-cyclus over de naleving van het beleid (eerste lijn van verdediging). Het beleid gaat verder ook in op de rol van medewerkers: zij moeten verantwoord om te gaan met persoonsgegevens en andere informatie, zij moeten getraind worden in het gebruik van beveiligingsprocedures en de organisatie ziet er op toe dat medewerkers kennisnemen van de regels en richtlijnen voor informatiebeveiliging. Het beleid is verder in lijn met de AVG.

Net zoals in het privacybeleid wordt ook ingegaan op de tweede lijn van verdediging en de functionarissen in het PIT. Het PIT heeft nu eveneens een ondersteunende, adviserende en coördinerende rol ten aanzien van informatiebeveiliging. De CISO, ook onderdeel van het PIT, heeft een onafhankelijke positie en vult de derde verdedigingslijn in.[24] De CISO rapporteert aan de directie over informatiebeveiliging, in de tijd afgestemd op de P&C-cyclus.

Het Strategisch Informatiebeveiligingsbeleid beschrijft ook het proces van controle en verantwoording. De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren aan de portefeuillehouder(s). Voor de verantwoording over informatiebeveiliging gebruikt de gemeente de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). Via deze systematiek legt de gemeente verantwoording af over de informatieveiligheid van een aantal basisregistraties en informatiestelsels (waaronder de Basisregistratie Personen, DigiD en Suwinet). Dit gebeurt via een zelfevaluatie door de gemeente (waarbij lijnmanagers informatie aanleveren) en een audit door een externe (IT-)auditor. Het college van Burgemeester en Wethouders geeft jaarlijks een verklaring af in hoeverre de gemeente voldoet aan de normen die aan de beveiliging van DigiD en Suwinet gesteld worden. Over 2019 stelt de collegeverklaring dat aan alle normen ten aanzien van de DigiD-aansluitingen van de gemeente en Suwinet wordt voldaan.

De relatie tussen informatiebeveiliging en de bescherming van persoonsgegevens wordt in het Strategisch informatiebeveiligingsbeleid op verschillende punten expliciet gemaakt. Het Strategisch informatiebeveiligingsbeleid is in lijn met het privacybeleid. Dit komt bijvoorbeeld naar voren in de taken en verantwoordelijkheden van verschillende functionarissen, de aansluiting op de P&C cyclus en de rapportage van de FG als onderdeel van de verantwoording.

[24] PIT kwartaalrapportage Q1 2021

4. Uitwerking van het beleid

Procesbeschrijvingen en DPIA's

Verschillende aspecten van het privacybeleid van Hilversum zijn uitgewerkt in regels, procedures en werkprocessen. Een belangrijk aspect van het beleid is dat alle werkprocessen binnen de organisatie worden geïnventariseerd en aangepast op vereisten met betrekking tot privacy en informatiebeveiliging. De verantwoordelijkheid voor het waarborgen van de privacy in de verschillende werkprocessen berust bij de betrokken lijnmanagers. Dit is in aansluiting met het uitgangspunt dat de lijnmanagers verantwoordelijk zijn voor de correcte naleving van het privacybeleid in de tot hun verantwoordelijkheid berustende processen.
Voor de hele gemeente zijn er door de FG dertien werkprocessen geïdentificeerd waar de aandacht voor privacy hoge prioriteit heeft. Het gaat om de werkprocessen op de volgende terreinen:

Dertien belangrijke werkprocessen m.b.t. privacy binnen Hilversum

1. Belastingheffing	6. Jeugd en onderwijs	11. Ruimte en bereikbaarheid
2. Burgerzaken	7. Lokale economie	12. Veiligheid en openbare orde
3. Cultuur en sport	8. Welzijn en zorg	13. Werk en inkomen
4. Fraudeonderzoek	9. Bescherming en opvang	
5. Interne organisatie	10. Milieu en duurzaamheid	

De FG heeft in 2018 de organisatie geadviseerd om voor deze processen op basis van een zogeheten DPIA een procesplan op te stellen en te implementeren om zo in die werkprocessen vaste afspraken te maken voor een correcte omgang met privacygevoelige gegevens.

Wat is een DPIA?

DPIA staat voor *Data Protection Impact Assessment*. Dit wordt ook wel een Gegevens-beschermingseffectbeoordeling of een Privacy Impact Assessment (PIA) genoemd. De AVG vereist dat er in verschillende situaties, bijvoorbeeld bij grootschalige verwerking van persoonsgegevens, vooraf aan die verwerking moet worden bepaald wat het effect van de geplande verwerkingsactiviteit is op de bescherming van de persoonsgegevens van een persoon. Met een DPIA wordt hieraan voldaan. Een DPIA geeft inzicht in de impact van de verwerking op de privacy van deze persoon. Op basis van een DPIA kunnen er maatregelen worden genomen om de impact zo nodig te verminderen. Een DPIA wordt altijd uitgevoerd op een verwerking van *persoons*gegevens.

In het jaarverslag van de FG van 2019 geeft hij het advies om zogenaamde DPIA's uit te voeren bij verwerkingen van persoonsgegevens met een hoog risicoprofiel, zoals bij een verwerking van bijzondere persoonsgegevens. Uit datzelfde verslag blijkt tevens dat op dat moment de meeste processen nog niet (aantoonbaar) waren onderzocht.[25]

[25] Uit in het kader van het onderzoek verkregen informatie blijkt dat er vanaf 2020 vier DPIA's zijn uitgevoerd, twee zich in het stadium van afronding bevinden en er twee in uitvoering zijn. Er zijn DPIA's uitgevoerd op twee processen bij het Sociaal Plein. In 2021 zullen er nog drie worden gestart.

De uitvoering van de DPIA's is de verantwoordelijkheid van de verschillende afdelingen waarbinnen de verwerkingen plaatsvinden. Deze uitvoering draagt bij aan de bescherming van burgers, omdat het een organisatie in een vroegtijdig stadium inzicht geeft in de risico's en dus een organisatie in staat stelt deze te mitigeren. Hierdoor kunnen incidenten en datalekken worden voorkomen.

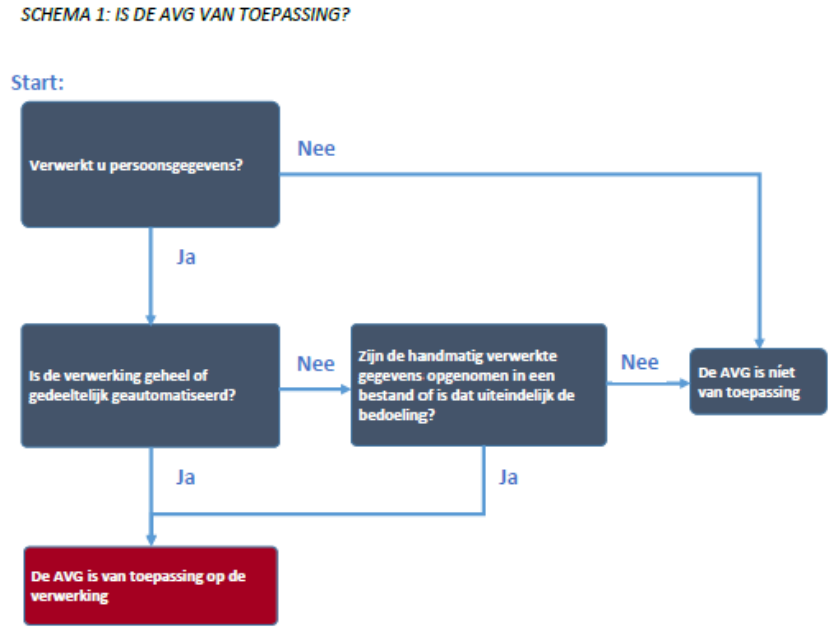
Verwerkingsregister
In aansluiting op artikel 30 van de AVG dient de gemeente een Verwerkingsregister in te richten. Dit register is een integraal overzicht van alle verwerkingsactiviteiten van persoonsgegevens die onder verantwoordelijkheid van de gemeente plaatsvinden. In de verslagen van het PIT wordt genoemd dat momenteel (2021) wordt gewerkt aan een verbeterslag en actualisatie van het register. Onder meer moet in het register melding worden gemaakt van categorieën van betrokkenen. In de oorspronkelijke versie waren dat meer dan tachtig categorieën. Dit wordt teruggebracht tot een overzichtelijker en beter werkbaar aantal van zestien categorieën. Ook de categorisering van persoonsgegevens wordt aangepast.

Coördinatie en planning
De uitvoering van het privacybeleid wordt gemonitord door de Privacy Officer (PO). Die stelt het jaar- en meerjarenplan op. De jaarplannen bevatten een opsomming van de concrete activiteiten die in het kader van het privacybeleid in dat jaar worden ondernomen. Het team PIT rapporteert per kwartaal aan de directie. De directie informeert vervolgens de portefeuillehouder.
Daarnaast coördineert de PO de uitvoering van de meerjarenplanning in samenwerking met de Functionaris Gegevensbescherming (FG). In het Jaarplan 2019-2020[26] zijn de relevante processen, aanbevelingen van de FG, maatregelen voor organisatorische inbedding, acties voor waarborging van de rechten van betrokkenen, samenwerking met derden, maatregelen t.b.v. beveiliging en op welke manier er verantwoording wordt afgelegd opgenomen. Ook worden in dit document de eerdere ontwikkelingen gemonitord: de voortgang van de DPIA's, de datalekken en de vragen die over beveiliging, wettelijke grondslagen, communicatie naar de burger, de voortgang en actualiteit van het verwerkingsregister en over de rechten van betrokkenen worden gesteld aan de PO.

Interne instructies
Een andere uitwerking van het beleid vindt plaats door middel van interne instructies. Interne instructies hebben betrekking op de wijze waarop medewerkers en lijnmanagers inhoudelijke ondersteuning kunnen krijgen bij vragen die leven over privacy, over het waarborgen van privacy in thuiswerksituaties en over de wijze waarop informatie veilig gedeeld kan worden. In deze laatste instructie wordt aan de medewerkers toegelicht welke platforms de medewerkers kunnen gebruiken voor informatiedeling, hoe bestanden kunnen worden uitgewisseld via de mail en hoe papieren informatie kan worden beveiligd en uiteindelijk, als deze niet meer bewaard hoeft te worden, vernietigd. Er zijn ook instructies 'Gouden Regels' opgesteld voor de omgang met digitale informatie.
Voor het thuiswerken is er een interne instructie opgesteld[27] waarin wordt uitgelegd hoe werknemers ervoor kunnen zorgen dat zij ook thuis privacyproof aan de slag kunnen. Er is ook een interne instructie over veilig informatie delen[28]. In deze instructie wordt er uitgelegd wat voor platforms door werknemers kunnen worden gebruikt voor informatiedeling en hoe bestanden kunnen worden uitgewisseld via de mail en via een link. Ook staat er hoe je papieren kan vernietigen.

[26] Gemeente Hilversum, Jaarplan 2019-2020; in het kader van het onderzoek is ook inzage gekregen in het jaarplan 2021.
[27] Gemeente Hilversum, interne instructie – Gouden Regels Veilig thuiswerken
[28] Gemeente Hilversum, interne instructie – Veilig informatie delen met anderen

Binnen een onderdeel van gemeente waar veel (privacygevoelige) gegevens worden uitgewisseld is voor de medewerkers een speciale, zogenaamde toolbox ontwikkeld, die tips, achtergrondinformatie en een toegankelijke beschrijving van de relevante regels bevat. Zie Figuur 1 voor een voorbeeld uit deze toolbox.



Figuur 1 Een voorbeeld van een 'tool' uit de Toolbox Uitwisselen Gegevens

Wanneer de gemeente als verwerkingsverantwoordelijke een andere partij opdracht geeft om persoonsgegevens te verwerken, moet er met die partij een verwerkingsovereenkomst worden gesloten. Daarvoor gebruikt de gemeente een Handreiking[29] die werknemers ondersteunt bij het begrijpen wanneer zo'n overeenkomst moet worden opgesteld en templates geeft voor verwerkersovereenkomsten die werknemers verder kunnen invullen. Hiervoor wordt de standaard verwerkersovereenkomst van de VNG gebruikt.
Ook voor andere specifieke situaties, zoals de samenwerking met derden of het cameratoezicht rond het gemeentehuis, heeft de gemeente aanvullende documentatie opgesteld om de privacy te waarborgen.

Datalekken

Er is een procedure opgesteld die aangeeft wat er moet gebeuren als er sprake is van een zogenaamd datalek; dit betreft een situatie waarbij sprake is van vrijgekomen informatie die betrekking heeft op persoonsgegevens en in handen van onbevoegden is gekomen, voor onbevoegden toegankelijk was, of zijn verloren is gegaan.[30] In het document wordt het wettelijk kader geschetst en aangegeven hoe mensen met verschillende rollen behoren te acteren. Er is een stappenplan dat beschrijft wat iemand moet doen als hij/zij denkt dat er een beveiligingsincident is. Ook staat daar kort wat voor soort zaken moeten worden gemeld. Hier worden zaken genoemd als 'een document onbeheerd bij de printer of op bureaus laten slingeren' en 'het verstrekken van informatie naar onjuiste

[29] Gemeente Hilversum, Handreiking VNG verwerkersovereenkomst 2.0, 2020
[30] Gemeente Hilversum, Procedure datalekken – procedure bij melding van een inbreuk in verband met persoonsgegevens (artikel 33 en 34 AVG), 2020

perso(o)n(en)'. Vanuit de instructie wordt de lezer doorverwezen naar het Meldingsformulier dat bij een incident kan worden ingevuld om melding te doen.

In het beleid wordt gesteld dat als er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene, dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, een geconstateerd datalek binnen 72 uur gemeld moet worden bij de Autoriteit Persoonsgegevens (AP). Tevens wordt genoemd dat een datalek altijd aan betrokken personen wordt gemeld wanneer er sprake is van een hoog risico voor de rechten en vrijheden van de betrokken personen. Ernstige gevolgen zijn bijvoorbeeld identiteitsfraude. Veelal voert het PIT, indien nodig in overleg met de FG, de afhandeling van de datalekken uit. Alle meldingen, en wijze van afhandeling, worden in een register bijgehouden.

In het kader van het onderzoek is de volgende informatie over datalekken verkregen:

Gerapporteerde datalekken bij de gemeente Hilversum

Jaar	Totaal aantal datalekken	Gemeld bij de AP	Gemeld aan betrokkene(n)
2018	15	2	6
2019	16	5	4
2020	24	11	9

Uit de tabel blijkt dat een melding aan de AP niet automatisch leidt tot een melding aan de betrokkene (of andersom). Bij elke melding wordt de afweging gemaakt of melden aan de betrokkene nodig is.

Een melding bij de AP wordt gedaan als het gaat om persoonsgegevens van gevoelige aard, of als er om andere reden sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens. Een melding aan de betrokkene wordt gedaan als de gegevens niet goed beschermd waren of als er andere redenen zijn die ongunstige gevolgen hebben voor de betrokkene.

Over het algemeen wordt in het geval van een melding aan de AP ook de betrokkene geïnformeerd. Hierbij wordt ook rekening gehouden met de impact van de melding aan de betrokkene in relatie tot de ernst van de gelekte gegevens.[31]

Het melden van datalekken aan de AP beperkt zich niet tot het invulling aan de wettelijke verplichting daartoe. De melding geeft ook aanleiding om lering te trekken uit het geconstateerde lek, en om vervolgens verbetermaatregelen te treffen.

Uitwerking informatieveiligheidsbeleid

Het Strategisch Informatiebeveiligingsbeleid krijgt een uitwerking in een jaarlijks informatiebeveiligingsplan. In dit informatiebeveiligingsplan zijn concrete tactische en operationele activiteiten uitgewerkt, onder andere gebaseerd op de inbreng van lijnmanagers, het advies van de CISO, eventuele incidenten die hebben plaatsgevonden en de uitkomsten van de ENSIA-audit. De Security Officer is verantwoordelijk voor het vormgeven en bewaken van het

[31] Ter illustratie: Het verschil tussen de meldingen AP en aan betrokkene in 2018 komt o.a. door een aantal interne datalekmeldingen. Bij het scannen van ingekomen post, zijn per abuis documenten doorgezet naar de afdeling Sociaal Plein die bedoeld waren voor de gemeentelijke personeelsadministratie. Het ging hierbij dus om persoonsgegevens van een medewerker van de gemeente. Er was geen aanleiding deze incidenten te melden bij de AP, maar het was wel noodzakelijk om de medewerker hiervan in kennis te stellen.

informatiebeveiligingsplan en adviseert en ondersteunt het lijnmanagement bij de uitvoering van de activiteiten.

In 2020 heeft de gemeente een zogenaamde GAP-analyse uitgevoerd om vast te stellen in hoeverre de gemeente voldoet aan de normen uit de Baseline Informatiebeveiliging Overheid (BIO). Deze GAP-analyse is een belangrijk instrument om inzicht te krijgen in de het niveau van beveiliging binnen de gemeente en de (nog) te nemen maatregelen. Over deze analyse is gerapporteerd aan lijnmanagers en de Chief Information Officer (CIO). Daarbij zijn ook adviezen gegeven over de te nemen maatregelen om aan alle normen te voldoen.
De beheersing van informatiebeveiliging en het bewaken van de invulling van de normen uit de BIO wordt ondersteund door informatievoorziening. In 2020 is de gemeente gestart met het inrichten van tooling om dit proces beter te ondersteunen. Met behulp van deze tooling kan de bewaking van de normen uit de BIO efficiënter en effectiever worden uitgevoerd.
Het is de ambitie van de gemeente om eind 2021 ‘in control’ te zijn. Daarmee wordt bedoeld dat volledig inzichtelijk is bij welke normen acties noodzakelijk zijn. In de praktijk is er daarmee sprake van een proces van continue verbetering. Vanuit de tweede verdedigingslijn wordt de voortgang op de invulling van de normen uit de BIO bewaakt.

Binnen de gemeente ontbreekt het nog aan een risicoanalyse op de belangrijkste processen en informatiesystemen van de gemeente. De gemeente is bezig dit uit te voeren, maar de uitvoering gaat trager dan voorzien.[32]

De gemeente is in 2020 gestart met een driejarig bewustwordingsprogramma voor medewerkers, het iBewustzijn-traject. In het eerste jaar (2020-2021) ligt de nadruk van dit programma op informatiebeveiliging, in het tweede jaar (2021-2022) op privacy en in het derde jaar (2022-2023) op integriteit. Dit programma start met een nulmeting om inzicht te hebben in de startsituatie. Bij de daaropvolgende metingen kunnen nu de verbeteringen - na maatregelen die zijn genomen om het bewustzijn van medewerkers te versterken - inzichtelijk worden gemaakt. Naast dit programma worden er nog meer activiteiten uitgevoerd om het bewustzijn van medewerkers op het vlak van informatiebeveiliging te vergroten. Zo krijgen alle medewerkers de 'Gouden regels Informatiebeveiliging en Privacy' uitgereikt (bij het begin van dit traject en wanneer ze nieuw in dienst komen). Daarmee wordt duidelijk welke eisen we aan de medewerkers stellen.
Aan het begin van de pandemie zijn de ‘Gouden Regels voor veilig thuiswerken’ bij alle medewerkers onder de aandacht gebracht. Daarnaast dienen alle medewerkers een e-learning module omtrent informatiebeveiliging te doorlopen en met goed gevolg af te ronden. Hier wordt op toegezien door leidinggevenden.

Rapportage en verantwoordingsstructuur
Het PIT stelt elk kwartaal een rapportage op waarin wordt ingegaan op de voortgang in de implementatie van het privacybeleid en het informatiebeveiligingsbeleid. Deze rapportage wordt uitgebracht aan het CIO-office. Zoals eerder vermeld geeft een lid van de directie invulling aan de rol van CIO. De directie informeert de portefeuillehouder.

In het beleid is vastgelegd dat de FG jaarlijks een verslag opstelt met betrekking tot de stand van zaken op het gebied van privacy binnen de gemeente. Dit verslag is gericht aan het college van B en W.

[32] PIT kwartaalrapportage Q1 2021

Korte beschrijving van de inhoud van het jaarverslag van de FG

In het Jaarverslag toetst de FG de naleving van de AVG op basis van tien kritieke prestatieindicatoren (KPI). Deze zijn: bestuurlijk beleid; regie & support; toezicht; werkprogramma; ketenregie; privacy by design[33]; verzoeken, klachten en incidenten; communicatie, training en opleiding; informatiebeveiliging en budget.
Per KPI beoordeelt de FG de doelmatigheid en doeltreffendheid. Hierbij kijkt de FG naar de opzet (papieren beleid), het bestaan (de maatregelen worden daadwerkelijk in praktijk gebracht) en de werking (de maatregelen blijken in de praktijk voldoende). In het verslag uit 2020[34] is opgenomen hoe de gemeente op deze tien aandachtspunten scoort. Volgens dit verslag is de score op de indicatoren 'Toezicht' en 'verzoeken, klachten en incidenten' 100%[35]. Op aspecten als beleid en werkprogramma digitale duurzaamheid is de score bijna 100%. Er is nog nauwelijks enige vooruitgang geboekt op het implementeren van Privacy by design en het verbeteren van de ketenregie.

Per KPI beoordeelt de FG de doelmatigheid en doeltreffendheid. Hierbij kijkt de FG naar de opzet (papieren beleid), het bestaan (de maatregelen worden daadwerkelijk in praktijk gebracht) en de werking (de maatregelen blijken in de praktijk voldoende). In het verslag uit 2019 is opgenomen hoe de gemeente op deze tien aandachtspunten scoort. Volgens dit verslag is de score op de indicatoren 'budget' en 'verzoeken, klachten en incidenten' 100%. Op aspecten als 'beleid' en 'toezicht' is de score bijna 100%. De prestaties op de KPI's 'privacy by design' en 'ketenregie' bevinden zich in de achterhoede.
Tijdens de uitvoering van dit rekenkameronderzoek kwam ook het jaarverslag van de FG over 2020 beschikbaar.[36] Op de KPI 'toezicht' is de score gestegen naar 100%. Bij 'budget' is de score iets afgenomen. Zowel de KPI 'beleid' als 'regie en support', 'werkprogramma' als 'informatiebeveiliging' zijn ruim voldoende. Een en ander kan worden geïnterpreteerd als een bevestiging dat het beleid organisatorisch op orde is. In de uitvoering zijn er zeker nog uitdagingen, zoals wederom blijkt uit relatief slechte scores op de KPI's 'privacy by design', 'ketenregie' en 'communicatie en training en opleiding'.
In het verslag over 2020 maakt de FG verder melding van positieve ontwikkelingen ten aanzien van het privacybewustzijn in de organisatie.

Vervolgens legt het college van B en W verantwoording af aan de gemeenteraad over de realisatie en de toepassing van het privacybeleid in relatie tot informatiebeveiligingsbeleid. Zo wordt naar aanleiding van de behandeling van het jaarverslag van FG een raadsinformatiebrief verzonden aan de gemeenteraad. Het jaarverslag van de FG over 2019 is door middel van raadsinformatiebrief 2020-28 gedeeld met de raad. Deze raadsinformatiebrief is opgenomen in de lijst van binnengekomen stukken van de gemeenteraadsvergadering van 10 juni 2020. Blijkens het verslag van deze vergadering is er niet over gesproken.

In de jaarstukken[37] wordt ingegaan op 'Informatie & automatisering' in brede zin waar onder andere de vorderingen op het gebied van informatieveiligheid en privacy worden benoemd. Dit wordt in algemene termen beschreven. Zo staat er in de jaarstukken van 2019 dat 'de ingezette koers uit 2018

[33] De toelichting hierbij is als volgt in het verslag verwoord: "De AVG-verantwoordelijke draagt ervoor zorg dat aantoonbaar passende maatregelen zijn genomen voor doelmatige en doeltreffende beheersing van risico's."
[34] In het kader van het onderzoek is inzage gekregen in het jaarverslag 2020 dat in de vergadering van het college van B en W van 20 april 2021 is besproken. Het collegebesluit en de daaraan gekoppelde raadsinformatiebrief worden ter informatie aan de raad verzonden. In dit verslag maakt de FG melding van positieve ontwikkelingen ten aanzien van het privacybewustzijn in de organisatie.
[35] 100% staat voor 'Volledig aanwezig en aantoonbaar'
[36] Dit verslag is besproken in de vergadering van het college van B en W van 20 april 2021.
[37] Gemeente Hilversum, Jaarstukken 2019, paragraaf 3.5.3 Informatie & Huishouding

[is] voortgezet', dat het privacybeleid is herschreven en dat de capaciteit binnen het privacy-team is uitgebreid.

Uitgangspunten bij de communicatie met de burgers

De gemeente communiceert op verschillende manieren aan inwoners hoe zij omgaat met hun persoonsgegevens. Om te beginnen bevat de website van de gemeente een privacyverklaring.[38] In deze verklaring stelt de gemeente inwoners op de hoogte over welke wetgeving van toepassing is en hoe gemeente deze heeft vertaald naar eigen beleid. Tevens wordt aangegeven op welke wijze de gemeente invulling geeft aan de wijze waarop de gegevens van de inwoners worden gebruikt (dit betreft de zogeheten verwerkingsverantwoordelijkheid). Ook worden inwoners gewezen op de rol en de verantwoordelijkheid van de FG. Daarna legt de gemeente op hoofdlijnen uit dat zij verschillende soorten persoonsgegevens verwerkt en geeft zij een aantal voorbeelden waarom dit nodig is. Ook verschaft de website informatie over bewaartermijnen van gegevens. Eveneens wordt genoemd dat de gemeente soms gegevens deelt met andere organisaties. Daarnaast wordt het informatiebeveiligingsbeleid kort toegelicht. Er wordt aangegeven welke rechten inwoners hebben ten aanzien van hun gegevens en hoe er wordt omgegaan met datalekken. Tot slot wordt uitgelegd waar inwoners terecht kunnen met vragen of klachten.

In het sociaal domein komt het vaak voor dat van inwoners wordt gevraagd om relatief veel en soms ook zeer privacygevoelige gegevens met de gemeente te delen. Op het 'Sociaal Plein', de plek waar inwoners een aanvraag kunnen doen, wordt onder meer door middel van een video toegelicht hoe de gemeente omgaat met de privacy.[39] In deze video wordt uitgelegd dat de gemeente alleen gegevens opvraagt die nodig zijn om inwoners te kunnen helpen. Ook wordt benoemd dat er altijd met een inwoner wordt overlegd voordat gegevens worden uitgewisseld. In de video en bij de toelichting op de website[40] wordt genoemd dat er altijd toestemming wordt gevraagd om gegevens van inwoners met een andere organisatie te delen. Voor een aantal uitwisselingen met organisaties waaronder de Belastingdienst is die toestemming echter niet noodzakelijk.[41] Uitleg over dat dit zo is en waarom ontbreekt op de website.

Overig

De gemeente heeft voor specifieke domeinen of projecten aanvullende documentatie opgesteld om de privacy te waarborgen. Zo is er in het kader van een pilot 'Vroeg Eropaf' een convenant opgesteld met samenwerkingspartners dat weer wordt ondersteund door een protocol waarin de werkwijze van partijen is vastgelegd op het gebied van privacy. Een ander voorbeeld waaruit blijkt dat er aanvullende documentatie wordt opgesteld is het Reglement cameratoezicht[42] dat betrekking heeft op het cameratoezicht in en rondom de panden van de gemeente.

---

38 https://www.hilversum.nl/Configuratie/Contact_metde_gemeente/Privacyverklaring_gemeente_Hilversum

39 https://www.youtube.com/watch?v=FU9QsRAqH0w&ab_channel=HilversumMediastad

40 Uw privacy bij het Sociaal Plein - Gemeente Hilversum

41 Voorbeelden van uitwisselingen van gegevens waar geen toestemming voor nodig is zijn:
- Uitwisseling met Belastingdienst als het gaat om uitkeringen
- Uitwisseling met CBS voor statistieken
- Uitwisseling via Suwinet: andere gemeenten kunnen een uitkeringsverhouding in Hilversum opzoeken. Die gemeente moet daar dan wel een grondslag en doelbinding voor hebben.

42 Gemeente Hilversum, Reglement Cameratoezicht beveiliging gemeentelijke gebouwen 2018.

5. De praktijk van het beleid

5.1 De algemene praktijk

Voor een goede omgang met privacy kan niet louter worden volstaan met het vastleggen en uitwerken van beleid. In de context van verantwoord privacybeleid wordt geregeld benadrukt dat elke medewerker zich niet alleen bewust moet zijn van het belang van privacy, maar daar ook, in elke activiteit, naar handelt. Gedacht kan worden aan zaken als het vergrendelen van schermen als de gebruiker niet achter de computer zit, het niet onbeheerd laten liggen van papieren die privacygevoelige gegevens bevatten of het tijdens telefoongesprekken bespreken van de persoonlijke situatie van cliënten van de gemeente, terwijl anderen kunnen meeluisteren met het gesprek.
Aandacht voor privacy is ook relevant als een medewerker toegang wil krijgen tot privacygevoelige gegevens, of als die voor een mogelijk betere uitvoering van het beleid gegevens gaat delen met andere organisaties.

Over de wijze waarop medewerkers van de gemeente Hilversum in de dagelijkse praktijk omgaan met privacy zijn in het onderzoek verschillende inzichten opgedaan.
Om te beginnen is al eerder vastgesteld dat de eerste verantwoordelijkheid voor een goede naleving van het privacybeleid en de daarmee verbonden voorschriften en procedures is belegd bij de lijnmanagers. Dat biedt enige garantie dat in het dagelijks functioneren van de verschillende gemeentelijke afdelingen aandacht wordt besteed aan privacy.

Als er zich vragen voordoen met betrekking tot privacy waarop niet simpel in het beleid een antwoord is te vinden, kunnen medewerkers of hun lijnmanagers een beroep doen op de medewerkers van het PIT. Deze medewerkers beschikken over een goede kennis van het privacybeleid. Wanneer er, zelfs na collectieve bespreking van lastige vragen in het PIT, de kennis en ervaring tekortschieten, kan het PIT een beroep doen op juristen werkzaam bij de gemeente en/of de FG. Naast zijn toezichthoudende functie heeft de FG ook een adviserende en coachende rol ten aanzien van de organisatie.
Medewerkers kunnen zelfstandig contact leggen met de FG. Als eerder genoemd neemt de FG ook met enige regelmaat deel aan de overleggen van het PIT. In dit overleg worden de meer urgente risico's besproken.

Het kan zijn dat er zich soms trends voordoen in de gestelde vragen, of dat naar aanleiding van gewijzigd of nieuw beleid veel vergelijkbare vragen aan de orde zijn. Dit wordt dan gesignaleerd binnen het PIT, waarna vanuit het PIT proactief informatie kan worden verspreid, bijvoorbeeld via het gemeentelijke intranet.
In het onderzoek is vastgesteld dat er binnen Hilversum geen sprake is van regelmatig overleg tussen lijnmanagers en medewerkers van het PIT. Lijnmanagers worden in hun verantwoordingsprocessen niet bevraagd over hoe zij met de bescherming van persoonsgegevens omgaan of met de informatiebeveiliging. Daarmee blijven de contacten beperkt tot incidentele vragen.
Een aanleiding voor dergelijk overleg is als er binnen een afdeling sprake is geweest van een datalek. Zodra het PIT melding van een datalek ontvangt, wordt contact opgenomen met de melder en de teammanager om een intake te doen en te registreren. Het PIT rapporteert over deze meldingen in de kwartaalrapportages aan de directie en portefeuillehouder. Nadat een incident is afgehandeld wordt er echter, zo is geconstateerd, niet altijd terugkoppeling gegeven aan de werkvloer.
Lijnmanagers worden in hun verantwoordingsprocessen niet bevraagd over hoe zij met de bescherming van persoonsgegevens omgaan of met de informatiebeveiliging.

Lijnmanagers en werknemers hebben een verschillende, gevarieerde betrokkenheid bij het onderwerp privacy. Sommige zijn door de aard van hun werk en hun persoonlijke affiniteit met het onderwerp goed bekend met hoe er met persoonsgegevens moet worden omgegaan. Het komt dan ook zeker voor dat medewerkers conform het privacybeleid met persoonsgegevens omgaan. Naar mening van diverse geïnterviewden komt dergelijk gedrag niet direct voort uit het beleid zelf, maar omdat er in sommige afdelingen van oudsher gewoontes en kennis zijn ontstaan rondom de bescherming van persoonsgegevens. Dat maakt het niet vanzelfsprekend dat hiervan organisatiebreed sprake is. Naar mening van diverse betrokkenen in de uitvoering zijn er nog niet genoeg handvatten voor alle werknemers om hun voldoende houvast te bieden hoe zij in hun dagelijks werk met persoonsgegevens moeten omgaan. Er zijn voor hen nog weinig procedures voor werkprocessen opgesteld. Wel wordt gemeld dat het privacybewustzijn over de afgelopen jaren is toegenomen, overigens zonder dat in dit onderzoek kan worden vastgesteld of en in welke mate dat is gebeurd.
In de uitvoering ervaren sommige medewerkers de AVG als belemmerend voor hun werk. Het PIT stuurt erop dat de AVG eerder als een kwaliteitsinstrument wordt gezien dan een beperkende wet. De AVG kan richtlijnen geven die het werk beter en efficiënter kunnen maken. Deze manier van kijken naar de AVG wordt nog niet door iedereen in de organisatie overgenomen.

In 2020 heeft elke werknemer een cursus moeten doen in het kader van het programma om iBewustzijn te bevorderen. Naar mening van het PIT heeft dit een positieve uitwerking gehad. Het voornemen bestaat om in 2021 eenzelfde cursus beschikbaar te maken over privacy. Dit moet samengaan met een bewustwordingscampagne.

In 2019 is vanwege personele uitval vertraging opgelopen bij de implementatie van de AVG. Deze achterstanden zijn in 2020 niet volledig ingelopen.

5.2 Smart City binnen Hilversum

Inzicht en ambities
Ten behoeve van een verdieping van de inzichten in het privacybeleid binnen Hilversum is nader aandacht besteed aan Smart City initiatieven binnen de gemeente Hilversum. In het ‘Programma Smart City’ formuleert de gemeente de missie omtrent Smart City als volgt: *“Smart City Hilversum is de ontwikkeling waarmee wij als gemeente samen met onze partners en gebruikers van de stad, (nieuwe) technologie en data inzetten om het leven van de bewoners van Hilversum prettiger te maken.”*[43] De initiatiefnemers zijn zich ervan bewust dat het actief gebruikmaken van data risico’s met zich meebrengt voor de privacy van inwoners. Om hierop te anticiperen is er specifiek voor Smart City privacybeleid ontwikkeld.

Onder de vlag van Smart City is er een aantal projecten in uitvoering. Dit is het meten van verkeersdrukte in de stad, het meten van de luchtkwaliteit, het doen van metingen die betrekking hebben op de veiligheid in een gebied en het ontwikkelen van een App die aan inwoners informatie verschaft over de aanwezigheid van beschermde bomen in de stad. De gemeente vindt het van belang om de inwoners te bevragen over de initiatieven. Hiervoor is in het kader van het Burgerpanel van de gemeente een vragenlijst verspreid. In de vragenlijst is geïnformeerd naar de bekendheid van het onderwerp Smart City, en is nader ingegaan op het draagvlak voor enkele van de Smart City initiatieven. Uit de enquête blijkt dat inwoners dataveiligheid en een goede omgang met privacy

[43] Programma Smart City – Doelen- en inspanningenmatrix, 2021

belangrijk vinden.[44] In de Raadsinformatiebrief 2019-69[45] staat dat de input van inwoners belangrijk blijft. Om hier mede invulling aan te geven, is ingezet op de ontwikkeling van een zogeheten 'Hilversum City Lab'. Dit lab dient de centrale plek te vormen waar vragen en suggesties vanuit de stad kunnen landen. Concreet is dit een laagdrempelige fysieke locatie waar bewoners kunnen ervaren wat de toegevoegde waarde van nieuwe technologische oplossingen is in het dagelijks leven. Daarnaast is er voor burgers hier de mogelijkheid om vragen te stellen en suggesties te doen.

Privacybeleid
Om de geformuleerde missie te bewerkstelligen heeft de gemeente een aantal basisbeginselen of programmapijlers geformuleerd.[46] Deze beginselen vormen een uitwerking van de 'Declaration of Cities Coalition for Digital Rights'.[47] Deze 'coalitie' verwijst naar een mondiaal samenwerkingsverband van steden die staan voor de lokale en globale bescherming en handhaving van mensenrechten op het internet. De door deze coalitie geformuleerde beginselen hebben betrekking op zowel privacy als informatiebeveiliging.

Om burgers blijvend te betrekken bij 'hun' Smart City[48] is er een Stadspanel Data ingericht. Dit orgaan, bestaande uit tien Hilversummers, heeft een onafhankelijke adviesrol bij het ontwikkelen van toepassingen, op de thema's privacy, dataveiligheid en inclusiviteit. Voor een rol in dit stadspanel konden geïnteresseerde inwoners van Hilversum reageren op een oproep van de gemeente. Het spreekt voor zich dat dit vooral inwoners betreft die een bovengemiddelde belangstelling en kennis hebben voor het thema 'Smart City'. Daarnaast wordt er gesteld dat de Raadscommissie Economie en Bestuur betrokken zal worden bij privacyvraagstukken. Waar sprake is van privacygevoelige informatie of verdenking van privacy-impact wordt een pentest (penetratietest, oftewel "binnendringtest") en PIA (Privacy Impact Assessment) georganiseerd door de Privacy Officer en zo nodig afgestemd met de onafhankelijke functionaris gegevensbescherming. Hierin wordt verzameling data, doelbinding, en wijze van anonimiseren/ pseudonimiseren/ aggregeren getoetst aan wetgeving. Dilemma's worden voorgelegd aan het stadspanel (zie hieronder) en ontwikkelingen die persoonsgebonden data omvatten worden aan de commissie ter advies neergelegd. Deze adviesaanvraag wordt uitgevoerd door het programma Smart City. De PO heeft hierin een adviserende rol aan het programma.

De Privacy Officer bereidt beleidsnotities en werkinstructies voor in het kader van de Smart City initiatieven en laat deze vaststellen door directie en/of wethouder Privacy. Gevraagd en ongevraagd adviseert de Privacy Officer over activiteiten ter bescherming van persoonsgegevens. De functionaris gegevensbescherming (FG) controleert de naleving van afspraken van de gemeente met ketenpartners. Daarnaast maakt de CISO ook deel uit van het programmateam Smart City.

Informatiebeveiliging
De data die wordt gebruikt voor de Smart City initiatieven moeten goed worden beveiligd. Het niveau van informatiebeveiliging wordt vastgesteld op basis van een risico-assessment, waarbij de aard van de data mede in de afweging wordt betrokken. Zo kennen metingen van luchtkwaliteit weinig privacygevoelige aspecten. Dit ligt anders voor verkeersbewegingen.

---

[44] Gemeente Hilversum, Burgerpanel Hilversum: Smart City, juli 2019
[45] Gemeente Hilversum, Raadsinformatiebrief 2019-69, zaak nr 578074, Samenwerkingsovereenkomst Smart City Hilversum
[46] Gemeente Hilversum, Bijlage 3 – SCH-AGH Dataprincipes, informatiebeveiliging en AVG
[47] https://citiesfordigitalrights.org/#:~:text=Declaration%20of%20Cities%20Coalition%20for,inseparable%20from-20our%20daily%20lives
[48] Gemeente Hilversum, Raadsinformatiebrief 2019-69, zaak nr 578074, Samenwerkingsovereenkomst Smart City Hilversum

Bij het Smart City-project is één met de gemeente samenwerkende partners het softwarebedrijf Atos. Dit bedrijf is, in zijn rol als samenwerkingspartner, verantwoordelijk voor de beveiliging van de data die worden verzameld en geanalyseerd. Voor de inrichting van de informatiebeveiliging van het platform worden veel voorkomende informatiebeveiligingsstandaarden[49] gebruikt.
Het is tevens in eerste instantie aan de leverancier van de software (Atos) om te laten zien welke informatiebeveiligingsmaatregelen zij neemt. Dit gebeurt door het opleveren van maandelijkse informatiebeveiligingsrapportages. Jaarlijks wordt er informatie verstrekt over de opzet, bestaan en werking van de relevante beveiligingsmaatregelen.

Dagelijkse praktijk
Ten tijde van het onderzoek liepen er verschillende initiatieven op het gebied van Smart City. Zo worden er metingen gedaan van de drukte in specifieke gebieden. Daarnaast is er gestart met een bomen-app die meer inzicht moet geven in de situatie rond beschermde bomen. De FG heeft een positief privacy-advies gegeven over de druktemeter.[50] Bij de bomenapp worden er geen persoonsgegevens gebruikt en was het daarom niet nodig advies te vragen aan de FG. Een derde initiatief dat ten tijde van het onderzoek in ontwikkeling was heette 'Snelliuslaan'. Door de inzet van sensoren wordt er gekeken hoe de verkeersveiligheid op de Snelliuslaan kan worden verbeterd.

Recente ontwikkelingen
Op 29 april 2021 werd bekend dat de Autoriteit Persoonsgegevens (AP) een bestuurlijke boete heeft opgelegd aan de gemeente Enschede. Aanleiding was een systeem waarmee het centrumbezoek in kaart werd gebracht. Dit systeem werkte via het opvangen van WPS-signalen door sensoren. Deze signalen worden uitgezonden door tablets en mobiele telefoons wanneer ze verbinding zoeken met een WIFI-netwerk. Volgens de Autoriteit Persoonsgegevens kan door de manier waarop dit in Enschede is toegepast herleidbaarheid naar personen ontstaan. In Hilversum is sinds 7 oktober 2020 een druktemeter operationeel. Ook dit systeem werkt met het opvangen van WPS-signalen, met dat verschil dat het systeem in Hilversum slechts telt en het onmogelijk is om personen en apparaten te identificeren of te volgen. Daarnaast dient dit systeem een ander doel, namelijk het inzichtelijk maken van de mate waarop in het centrum gezonde afstand kan worden gehouden in verband met corona (het systeem in Enschede had tot doel het in kaart brengen van passantenstromen). Direct nadat de boete bekend werd is de externe Functionaris Gegevensbescherming gevraagd de relevante verschillen en overeenkomsten te onderzoeken tussen de druktemeter in Hilversum en het systeem in Enschede. Hieruit bleek dat de Hilversumse druktemeter wezenlijk anders functioneert dan het systeem in Enschede, en blijft aansluiten bij de AVG. De gemeenteraad van Hilversum is hierover geïnformeerd per collegebrief van 4 mei 2021.

Tussenbalans naar aanleiding van het Smart City beleid
Er is veel aandacht voor privacy en de bescherming van persoonsgegevens bij de initiatieven die vallen onder Smart City. De gemeenteraad heeft meerdere malen aangegeven dit ook belangrijk te vinden. Gezien de focus op nieuwe technologie en het gebruik van data bij Smart City initiatieven is de aandacht voor privacy ook noodzakelijk. Bij alle initiatieven is er gekeken hoe er met geen of zo min mogelijk persoonsgegevens kan worden gewerkt. Als er persoonsgegevens worden uitgewisseld met anderen worden met hen verwerkingsovereenkomsten afgesloten. Wanneer er persoonsgegevens worden verwerkt wordt er een DPIA uitgevoerd op het proces en waar nodig advies gevraagd aan de FG. In 2020 is een relatief groot aandeel van alle DPIA's die in de gemeente hebben plaatsgevonden

[49] Zoals de Baseline Informatiebeveiliging Overheid, zowel op basisbeveiligingsniveau 1 (BBN1) voor publieke of laag-risico informatie, als basisbeveiligingsniveau 2 BBN2) voor de gevoeligere informatie.
[50] Gemeente Hilversum, FG-advies, de druktemeter, 17 september 2020

verricht door medewerkers die betrokken zijn bij Smart City-projecten. Uit het voor Smart City geformuleerde beleid, de consequente aandacht voor privacy binnen dit project en het uitvoeren van DPIA's komt naar voren dat wat privacy betreft dit project voorloopt op andere onderdelen van de gemeente.

5.3 Participatiewet

Een tweede nader onderzochte casus is de (uitvoering van de) Participatiewet. Het is de wettelijke taak van de gemeente om de Participatiewet uit te voeren. Het gaat daarbij om het bieden van hulp en ondersteuning aan burgers bij het verkrijgen van werk en het verstrekken van uitkeringen (zowel algemene bijstand als bijzondere bijstand) aan uitkeringsgerechtigden. Bij de uitvoering van de Participatiewet verwerkt de gemeente een groot aantal – gevoelige – persoonsgegevens over bijvoorbeeld de persoonlijke situatie van een burger, inkomen, arbeidsverleden, eventuele arbeidsongeschiktheid, opleidingen en vermogen. Het gaat daarbij ook nog eens om burgers die in een kwetsbare positie verkeren en afhankelijk zijn van de gemeente voor hun inkomenszekerheid. De Participatiewet (inclusief de bijbehorende verwerkingen van persoonsgegevens) is een breed onderwerp voor een casusstudie. Daarom is ten behoeve van dit onderzoek gekozen om de aandacht te concentreren op de inzet van Suwinet. Suwinet is een landelijk informatiesysteem dat door gemeenten en andere overheidsorganisaties gebruikt wordt om persoonsgegevens over burgers uit te wisselen bij het uitvoeren van hun wettelijke taken. Zo kan de gemeente (persoons)gegevens over bijvoorbeeld inkomen, arbeidsverleden en opleiding raadplegen.

Bescherming van persoonsgegevens en de Participatiewet
De Participatiewet wordt uitgevoerd door het Sociaal Plein van de gemeente. De uitvoering is belegd bij verschillende afdelingen, waarbij onderscheid wordt gemaakt tussen inkomen (verstrekken van uitkeringen) en participatie (begeleiden naar werk). De lijnmanagers van deze afdelingen zijn volgens het Privacybeleid verantwoordelijk voor de zorgvuldige omgang met persoonsgegevens en de naleving van het Privacybeleid binnen hun eigen organisatieonderdeel.

Hier wordt onder andere invulling aan gegeven door middel van werkinstructies waarin is vastgelegd op welke wijze de bescherming van persoonsgegevens (met betrekking tot de Participatiewet) geborgd is. In deze werkinstructies staat onder andere uitgewerkt welke persoonsgegevens mogen worden opgevraagd bij burgers of andere overheden. Ook worden er afspraken gemaakt over het delen van persoonsgegevens met derden, bijvoorbeeld in het kader van re-integratietrajecten. De verantwoordelijke lijnmanagers zien in de praktijk toe op het volgen van het beleid en het nakomen van de afspraken. Dit wordt bijvoorbeeld ingevuld via kwaliteitsmedewerkers die de verschillende dossiers onder ogen krijgen voor controle en advies. Daarnaast wordt via de informatiesystemen (bijvoorbeeld ten aanzien van de mogelijke invoer van gegevens) en formulieren (ten aanzien van welke gegevens worden uitgevraagd) van de gemeente afgedwongen welke persoonsgegevens verwerkt worden.

Hoewel de omgang met persoonsgegevens binnen het Sociaal Plein is vastgelegd in de werkinstructies, zijn de genomen maatregelen niet onderbouwd met behulp van een DPIA. Volgens het Privacybeleid van de gemeenten worden de lijnmanagers geadviseerd en ondersteund door het PIT. Er wordt in de praktijk enige afstand ervaren tussen het PIT en de afdelingen die verantwoordelijk zijn voor de uitvoering van de Participatiewet. Binnen afdelingen wordt ervaren dat er vanuit het PIT voornamelijk aandacht is voor de afdelingen als er sprake is van (een vermoeden van)

een datalek. Het PIT is echter ook beschikbaar voor vragen over gegevensbescherming die niet door de kwaliteitsmedewerkers van de afdelingen zelf kunnen worden afgedaan.

Vanuit het Sociaal Plein wordt ook met inwoners gecommuniceerd over hun privacy. Zo heeft het Sociaal Plein een aparte pagina met een informatieve video over privacy, gericht aan burgers die te maken krijgen met het Sociaal Plein.

Bewustzijn medewerkers
Uit de casusstudie blijkt dat privacy een belangrijk onderwerp is voor de betrokken medewerkers. Medewerkers hebben dagelijks te maken met privacy en persoonsgegevens en zijn zich bewust van de risico's die gepaard gaan met de verwerking van persoonsgegevens. Er is sprake van een 'actieve cultuur' als het gaat om de privacy van burgers: medewerkers hebben aandacht voor het onderwerp in hun werk, spreken er regelmatig met elkaar over, spreken elkaar aan, coachen elkaar en stellen ook vragen. Daarnaast zijn er binnen de afdelingen ook informele afspraken en werkwijzen met betrekking tot persoonsgegevens. Kortom, hieruit blijkt een sterke cultuur rondom een zorgvuldige omgang met persoonsgegevens. In de casusstudie zijn diverse voorbeelden naar voren gekomen die weliswaar anekdotisch van aard zijn, maar wel de cultuur kenschetsen:

- Het is gebruikelijk om niet de (volledige) namen van cliënten tijdens werkoverleg te delen.
- Als er meer dan de noodzakelijke informatie bij burgers wordt opgevraagd door een medewerker, dan wordt dit gesignaleerd (bijvoorbeeld door een kwaliteitsmedewerker).
- Men is alert op welke informatie gedeeld wordt als er een (medisch) adviesrapport wordt aangevraagd door de gemeente.
- In een specifiek geval heeft een medewerker, na een verandering van functie, uit eigen beweging zijn/haar toegang tot Suwinet laten verlopen.

De medewerkers met wie in het kader van de casusstudie is gesproken, hebben allen ook de e-learning module over veilige omgang met informatie gevolgd. Vanuit het lijnmanagement wordt er gestuurd op deelname aan deze module.
De betrokkenen geven aan dat de informatieverstrekking over privacy aan nieuwe medewerkers nog verbeterd kan worden zodat zij eerder bekend raken met de juiste werkwijze. Doordat een groot deel van de medewerkers in het afgelopen jaar thuis hebben gewerkt is het moeilijker geworden om de 'actieve cultuur' te behouden. Medewerkers treffen elkaar minder makkelijk en spreken elkaar minder vaak. Daarnaast gebeurt een deel van het werk meer uit het zicht van elkaar.

Gebruik van Suwinet
Suwinet is een belangrijk systeem voor de gemeente, omdat er veel informatie te vinden is die relevant is voor de uitvoering van de taken die voortvloeien uit de Participatiewet. Het gaat daarbij om gevoelige persoonsgegevens van veel personen. Daar horen ook specifieke beveiligingseisen bij. Aan een deel van deze eisen wordt invulling gegeven met het strategisch informatiebeveiligingsbeleid van de gemeente.

De gemeente legt via de ENSIA-systematiek verantwoording af over het gebruik en de beveiliging van Suwinet, waaronder de vertrouwelijkheid van de persoonsgegevens uit Suwinet.[51] Voor het uitvoeren van deze audit zijn er per organisatieonderdeel van de gemeente functionarissen aangewezen. Voor het Sociaal Plein is een functionaris aangewezen die de controles op Suwinet gaat uitvoeren, namelijk de desbetreffende teammanager.[52] Deze functionaris is recent aangewezen.

[51] Deze systematiek van verantwoording is nader toegelicht en besproken op pagina **p** van dit rapport.
[52] PIT kwartaalrapportage Q1 2021

De gemeente heeft een protocol voor de toegang tot Suwinet. De toegang wordt verschaft tot een deel van de informatie op Suwinet. Zo heeft een klantmanager participatie, meestal geen toegang nodig tot informatie over het inkomen van een burger en worden de rechten hier ook op aangepast. Daarnaast wordt, op basis van logbestanden, gecontroleerd welke informatie medewerkers raadplegen. Teammanagers krijgen regelmatig bericht over wanneer een medewerker voor het laatst in het systeem heeft ingelogd. De logbestanden wordt daarnaast gecontroleerd op ten onrechte geraadpleegde informatie (informatie die niet op grond van de uit te voeren taken geraadpleegd zou moeten zijn). Als dit het geval is dan worden medewerkers hierop aangesproken.

Balans van de opbrengsten in deze casus
In deze korte casestudie is wederom bevestigd dat het beleid van de gemeente Hilversum voldoet, en ook is uitgewerkt in instructies. Het merendeel van de bij dit beleid betrokken medewerkers hebben aantoonbaar gemaakt dat zij in hun dagelijks handelen actief anticiperen op een zorgvuldige omgang met privacygevoelige gegevens. Op onderdelen zijn er enkele kwetsbaarheden en achterstanden geconstateerd. Zo is er melding gemaakt van ‘afstand’ tussen de direct bij dit beleid betrokken medewerkers en de leden van het PIT. Blijkens het verslag van de FG heeft er (nog) geen DPIA plaatsgevonden voor de relevante werkprocessen.[53] De bijzondere omstandigheden vanwege corona zetten een goede naleving van de gewenste organisatiecultuur met betrekking tot privacy onder druk.

[53] Bij meer specifieke werkprocessen, zoals risicovolle verwerkingen in processen op het Sociaal Plein, zijn wel DPIA’s uitgevoerd.

6. De rol van de gemeenteraad

De rol van de gemeenteraad is in het Privacybeleid 2020-2024 als volgt beschreven:

De gemeenteraad ziet er op toe dat het college overkoepelend beleid ten aanzien van bescherming van persoonsgegevens voor de organisatie vaststelt. Door de gemeenteraad worden voor de uitvoering hiervan de benodigde middelen beschikbaar gesteld. Voorts controleert zij het college bij de uitvoering van deze kaders. Zij wordt hiertoe in staat gesteld door de verantwoordingsinformatie. Dit is onder meer het jaarlijkse verslag van de Functionaris Gegevensbescherming (FG), die het college verschaft.[54]

De FG doet conform beleid jaarlijks verslag van de stand van zaken op privacygebied binnen de gemeente. Het college verschaft deze informatie aan de gemeenteraad. Zoals eerder in deze rapportage al genoemd wordt deze informatie ter kennisname geagendeerd. Het jaarverslag over 2019 is niet besproken door de raad.
Jaarlijks legt het college verantwoording af aan de gemeenteraad over de realisatie en de toepassing van het privacybeleid in relatie tot informatiebeveiligingsbeleid, via de paragraaf bedrijfsvoering in de jaarstukken. Met enige regelmaat is er sprake van beeldvormende sessies over privacy, informatiebeveiliging, Smart City, of combinaties daarvan.

Voor dit onderzoek hebben de onderzoekers gesproken met enkele raads- en commissieleden[55]. In een discussiebijeenkomst zijn aan de deelnemende raads- en commissieleden enkele stellingen op het gebied van privacy voorgelegd. Uit deze raadsessie is gebleken dat de deelnemers tekortkomingen ervaren in de informatievoorziening over het privacybeleid. Naar mening van de deelnemers wordt in relevante besluiten te weinig aandacht besteed aan privacyaspecten. Ook ervaren de deelnemers het als een tekortkoming dat de raad geen overzicht heeft van privacy-incidenten en datalekken, die zich hebben voorgedaan binnen de gemeente.[56] De deelnemers geven aan dat zij graag expliciet over de inrichting en uitvoering van het privacybeleid geïnformeerd willen worden. Zij stellen in dit verband dat het voor hen niet voldoende is wanneer beleidsinhoudelijke documenten louter een paragraaf over de privacy bevatten. Zij hebben tevens behoefte aan een algemene bespreking van het thema privacy als zodanig. Impliciet geven zij hiermee aan dat de voor de raad beschikbare rapportages daarin naar hun mening onvoldoende voorzien. Het is opmerkelijk dat het jaarverslag van de FG niet herkend wordt als een document dat een geschikte aanleiding zou kunnen verschaffen voor een bespreking en beschouwing vanuit de raad over de stand van zaken met betrekking tot het privacybeleid van de gemeente. De raadsinformatiebrief vanuit het college van B en W naar aanleiding van het jaarverslag van de FG passeert de raad zonder bespreking, als één van de documenten op de lijst van ter informatie ontvangen stukken.

Verder gaven de deelnemers aan de raadssessie aan te hechten aan een duidelijke en consistente communicatie over de inrichting van het privacybeleid aan de burgers. Burgers moeten nadrukkelijk worden geïnformeerd over hun rechten en wat de gemeente doet (of juist niet doet) met hun

---

54 Hilversum, Privacybeleid 2020-2024, p. 5
55 Zie bijlage A voor een overzicht van de raadsleden die aan de bijeenkomst hebben deelgenomen.
56 Het jaarverslag van de FG, dat ter kennisname wordt aangeboden aan de raad, bevat overigens wel een overzicht van datalekken.

persoonlijke gegevens. Van een duidelijke en consistente communicatie kan alleen sprake zijn als het beleid op orde is.
Onder de deelnemers aan de raadsbijeenkomst was sprake van verschillende opvattingen over de wenselijkheid van het verzamelen en gebruiken van grote databestanden, zoals bijvoorbeeld kan plaatsvinden in de context van Smart City initiatieven, ter ondersteuning van het gemeentelijk beleid. Sommigen benadrukten de voordelen, anderen de risico's. De deelnemers waren het erover eens dat alleen gebruik kan worden gemaakt van grootschalige databestanden, als er voldoende waarborgen zijn dat daarmee geen privacygevoelige gegevens zonder toestemming van de betrokken burgers worden benut. Dat betekent ook dat er de nodige duidelijkheid en transparantie moet zijn over de inrichting en het gebruik van dergelijke databestanden.

Bijlage A Geïnterviewde personen

Algemene interviews

Naam	Functie
Sergej Katus	Functionaris Gegevensbescherming
Marinda Gaillard	Projectleider Smart City
Jaap Huib van der Knaap	Chief Information Security Officer
Harriët Arnolds	Security Officer
Marco de Bruijn	Informatiemanager
Janneke van Straalen	Privacy Officer
Will Stoof	Teammanager Participatiewet
Karin Walters	Wethouder
Erik Pepping	Teammanager Informatiemanagement

Deelnemers verdiepende casus 'Smart City'

Naam	Functie
Lily Meulbok	Trainee
Vybeke Pieters	Informatieadviseur Smart City

Deelnemers verdiepende casus Participatiewet

Naam	Functie
Hans Piersma	Handhaver Werk & Inkomen
Gerda Bedet	Klantmanager Re-integratie
Rob Hopmans	Kwaliteitsmedewerker Participatie

Deelnemers Convergentiesessie

Naam	Functie
Theo Buijtenweg	Adviseur informatie
Rob Hopmans	Kwaliteitsmedewerker Participatie
Jaap Huib van der Knaap	Chief Information Security Officer
Erik Pepping	Teamleider Informatiebeleid
Vybeke Pieters	Informatieadviseur Smart City
Sergej Katus	Functionaris Gegevensbescherming
Will Stoof	Teammanager Participatiewet

Deelnemers raadsdiscussie 18 maart 2021

Naam	Partij
E. Göbbels	Democraten Hilversum
A. Vreugdenhil	ChristenUnie
H. Bijl	Hilversums Belang
J. Deen	D66
B. Verweij	SP
G. Dunker	SP
H. Fennema	VVD
R. Lancé	Hart voor Hilversum
P. Veenendaal	GroenLinks
F. van Drooge	PvdA

Bijlage B Bestudeerde documentatie

#	Documentnaam	Datum
1	Deelnameverklaring Hilversum convenant radicalisering en extremisme	13 november 2018
2	Convenant: Persoonsgerichte aanpak voorkoming radicalisering en extremisme	2018
3	Privacy Protocol 'Vroeg Eropaf Hilversum'	Februari 2019
4	FG-verslag 2018	13 maart 2019
5	Privacy beleid 2020-2024	25 maart 2020
6	FG-verslag 2019-2020	3 april 2020
7	Raadsinformatiebrief inzake druktemeter	29 juni 2020
8	Wethoudersbrief Enquête Smart City Hilversum	8 juli 2019
9	Raadsvoorstel Uitgangspunten Smart City samenwerking	10 juli 2019
10	Concept Raadsbesluit Gemeenteraad Uitgangspunten Smart City	10 juli 2019
11	Motie: Beleidsplan voor Smart City	10 juli 2019
12	Persbericht Smart City Hilversum	22 juli 2019
13	Strategisch Informatiebeveiligingsbeleid 2020-2024	17 maart 2020
14	Advies Stadspanel data inzake Hilversumse druktemeter	27 juli 2020
15	Register sensoren, applicaties en datasets	11 september 2020
16	Zienswijze druktemeter Functionaris Gegevensbescherming	17 september 2020
17	Collegebrief Beantwoording vragen over het meten van bezoekersstromen	29 september 2020
18	SCH-AGH Roadmap Smart City Hilversum	4 oktober 2019
19	Essaybundel: Behoorlijk datagebruik in de openbare ruimte	Oktober 2019
20	Dataprincipes, informatiebeveiliging en AVG	5 november 2019
21	DPIA: Bodycam's voor BOA's	12 november 2020
22	Raadsinformatiebrief inzake samenwerkingsovereenkomst Smart City	13 november 2019
23	Privacyreglement: Lokale Persoonsgerichte aanpak	December 2019
24	Future City: Een slimme stad, zo doe je dat	2019
25	FG-verslag 2019-2020	3 april 2020
26	Raadsinformatiebrief inzake Jaarverslag FG	25 april 2019
27	Procedure datalekken	April 2020
28	Raadsinformatiebrief inzake Jaarverslag FG	28 mei 2020
29	Privacy impact beoordeling druktemeter	15 juli 2020
30	DPIA verslag Snelliuslaan	10 augustus 2020
31	Proclaimer Gemeente Hilversum	18 november 2020
32	Datalek of informatiebeveiligingsincident melden	18 november 2020
33	Meer weten over informatiebeveiliging	18 november 2020
34	Meer weten over privacy	18 november 2020
35	Veilig informatie delen met anderen	18 november 2020
36	Handleiding VNG verwerkersovereenkomst 2.0	19 november 2020
37	Checklist onderzoek datalek	19 november 2020
38	Privacy verklaring gemeente Hilversum	November 2020
39	Rapportage PIT Q1 2020	2020

40	Rapportage PIT Q2 2020	2020
41	Rapportage PIT Q3 2020	2020
42	Rapportage PIT Q4 2020	2021
43	FG Jaarverslag 2020	2021
44	Collegebrief Druktemeter Hilversum en bestuurlijke boete Enschede	4 mei 2021
45	Memo Beoordeling druktemeter gemeente Hilversum op AP-besluit gemeente Enschede	2021
44	Gouden regels Privacy en Informatiebeveiliging	
45	Jaarplan 2021 AVG	
46		

Bijlage C Toetsing van de normen

Bij aanvang van het onderzoek zijn verschillende normen opgesteld waar de bevindingen aan zijn getoetst. Een overzicht hiervan is in deze bijlage opgenomen.
Waar de vastgestelde praktijk in lijn is met de geformuleerde norm, is in het kader het oordeel ‘positief’ vermeld. Indien de praktijk duidelijk achterblijft bij de vooraf opgestelde normen, zou dit leiden tot het oordeel ‘negatief’ in het normenkader. In de praktijk van Hilversum is er echter geen aanleiding tot een dergelijk oordeel. In sommige situaties is er in de praktijk sprake van in de context van de geformuleerde norm zowel positieve als minder positieve bevindingen. Dit leidt dan tot het oordeel ‘neutraal’.

Normen	Beoordeling
Gemeentelijk beleid (onderzoeksvragen 1, 2 en 3)	
• Het gemeentelijk beleid voldoet tenminste aan de eisen die in wet- en regelgeving worden gesteld: generiek aan de AVG, en specifiek voor de genoemde materiewetten.	Positief
• In het gemeentelijk beleid wordt ingegaan op: – Juridische aspecten op basis van de AVG en de materiewetten. – Vertaling naar de beleidskaders privacy. – Organisatie, taken en verantwoordelijkheden. – Inrichting werkprocessen. – De toepassing van informatiesystemen en ICT. – De gegevens- en informatiestromen. – De positie van en communicatie met de burger.	Positief
• De gemeente hanteert landelijke standaarden, zoals de Baseline Informatiebeveiliging Overheid (BIO).	Positief
• In de procesbeschrijvingen en instructies is duidelijk welke functionaris welke gegevens in welke processtap mag verwerken, en onder welke condities dat mag.	Positief
• De gemeente heeft beleid voor incidenten waarbij sprake is van schending van de privacy van inwoners. Dit beleid voldoet aan de wettelijke vereisten.	Positief
• De gemeente verschaft aan burgers schriftelijk en mondeling begrijpelijke informatie over het gebruik van hun persoonsgegevens, zowel in algemene zin als afgestemd op de verschillende fasen in het dienstverleningsproces. Daarbij wordt aangegeven met welk doel dit gebeurt, wie inzage heeft en wat er vervolgens met de gegevens gebeurt.	Positief
• De gemeente informeert de burger op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling.	Positief

Het gegeven dat op alle rond het gemeentelijk beleid geformuleerde normen het oordeel positief is, is in lijn met de eerdere constateringen dat dit beleid op papier volledig is. In het onderzoek is vastgesteld dat er ook informatie voor burgers beschikbaar is. Er is echter niet onderzocht of die informatie voor burgers (voldoende) begrijpelijk is.

Normen	Beoordeling
Leren en verbeteren (onderzoeksvraag 4)	
• De gemeente heeft vastgelegd hoe en wanneer medewerkers worden getraind in / er aandacht besteed wordt aan het onderwerp privacy.	Positief
• Het toezicht op gebruik van persoonsgegevens is vastgelegd in een controleplan, waarin onder meer staat: hoe dit proces verloopt, de periodiciteit van de controles, wie daarbij betrokken zijn (functienamen en persoonsnamen), wie controles uitvoert, aan wie wordt gerapporteerd, hoe de resultaten worden vastgelegd, wat de criteria zijn voor vervolgstappen, welke de vervolgstappen kunnen zijn en wie die neemt.	Positief
• Het controleplan sluit aan op het gemeentelijk beveiligingsplan en op het Integriteitsbeleid.	Positief
• De medewerkers zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens.	Neutraal
• In de praktijk wordt gehandeld conform de wijze waarop de bescherming van de persoonsgegevens is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming.	Neutraal
• De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt.	Neutraal
• De gemeente heeft een routine voor het meten en verbeteren van de bescherming van persoonsgegevens en legt vast wat de bevindingen en maatregelen zijn. Deze routine is al tenminste één keer uitgevoerd.	Positief

Ook als het gaat om ‘leren en verbeteren’ zijn de oordelen overwegend positief, maar hier is wel sprake van meer nuances. Geconstateerd is dat er geregeld trainingen en bewustwordingscampagnes zijn. Het jaarplan van het PIT doet ook dienst als controleplan. Of het controleplan aansluit op het integriteitsbeleid is niet onderzocht.
Het oordeel ‘neutraal’ bij de norm of de medewerkers bekend zijn met het gemeentelijk beleid, alsmede of in de praktijk ook zo gehandeld wordt, wordt ingegeven door de bevinding dat er signalen zijn verkregen dat hier niet over de volle breedte van de organisatie sprake van is. Er is niet geconstateerd dat er sprake is van een expliciete leer- en verbetercyclus. Wel is het zo dat door de werkwijze van het PIT in dat gezelschap ervaringen worden geïnventariseerd en systematisch worden besproken, hetgeen leidt tot aanpassingen in activiteiten of nieuwe activiteiten. Ook de stelselmatige uitvoering van DPIA’s kan gelden als een instrument om van te leren en te verbeteren. Zoals genoemd is er wat de uitvoering van DPIA’s betreft sprake van achterstanden. Echter, de formulering van de laatste norm in dit blok, namelijk dat de routine al tenminste ‘één keer’ is uitgevoerd, leidt uiteindelijk op deze norm tot een positief oordeel.

Normen	Beoordeling
Kaderstellende en controlerende rol van de raad (onderzoeksvraag 5)	
• In de bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop een correcte omgang met persoonsgegevens is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles.	Neutraal
• Bij de ontwikkeling van beleid heeft aandacht voor het waarborgen van privacy op de agenda van de raad gestaan.	Neutraal

Geconstateerd is dat de raad structureel wordt geïnformeerd, zowel via de P&C-cyclus als door middel van het jaarverslag van de FG. Deze wijze van informeren leidt zelden tot bespreking en het formuleren van conclusies en aanbevelingen. Weliswaar is de raad ook geïnformeerd over de uitgangspunten van het beleid en vervult hierin een actieve controlerende rol. Naar mening van raadsleden zijn zij te weinig in de positie om daar goede invulling aan te geven.

Bijlage D Gebruikte afkortingen

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
AI	Adviseur Informatie
BIO	Baseline Informatiebeveiliging Overheid
BIO-BBN1	Basis Informatiebeveiliging Overheidsdiensten - Basis Beveiligingsniveau 1
BIO-BBN2	Basis Informatiebeveiliging Overheidsdiensten - Basis Beveiligingsniveau 2
CISO	Chief Informatie Security Officer
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
ISMS	Information Security Management System
PDCA	Plan-Do-Check-Act
PIT	Privacy en Informatiebeveiliging Team
PO	Privacy Officer
SO	Security Officer