Privacy en informatieveiligheid in het sociaal domein

Rekenkamer Heerhugowaard

Drs. J.M.W. (Hans) Oostendorp, directeur rekenkamer
E.I.A. (Emilie) Stumphius MSc LLM, onderzoeker
G.S. (Gideon) van der Hulst MSc, onderzoeker

Rekenkamer Heerhugowaard

Mevrouw E. Witzke, MSc
Ambtelijk secretaris

T. 06-451 713 57
E. eva@necker.nl

Datum: 13 november 2018

Inhoudsopgave

Bestuurlijke nota

Onderzoeksverantwoording

Aanleiding

Gemeenten zijn verantwoordelijk voor een juiste en veilige verwerking van persoonsgegevens in het sociaal domein[1]. De aandacht voor informatieveiligheid en privacy in het sociaal domein is de afgelopen jaren enorm toegenomen. Er is namelijk veel veranderd. Door de decentralisaties in het sociaal domein in 2015 kregen gemeenten bijvoorbeeld meer taken. Daarnaast is er snel veel veranderd op het gebied van informatieveiligheid en privacy: de introductie van de meldplicht datalekken, de Algemene Verordening Gegevensbescherming (AVG) die van kracht ging in mei 2018 en de resolutie van de Vereniging van Nederlandse Gemeenten (VNG) die gemeenten oproept om adequaat beveiligingsbeleid te implementeren. In reactie hierop hebben gemeenten hun privacy- en informatiebeveiligingsbeleid herijkt.

De tweede aanleiding voor dit onderzoek is de volgende. In het sociaal domein is een bekend spanningsveld de verhouding tussen de bescherming van privacy enerzijds en het delen van gegevens om goede zorg te kunnen leveren anderzijds. Integraal werken is gebaat bij gegevensverwerking en met name gegevensdeling, terwijl in het kader van privacy en informatieveiligheid juist wordt gestreefd om zo min mogelijk gegevens op te slaan en te delen.

Ook de gemeenteraad in Heerhugowaard ziet het belang van en de spanning omtrent privacy en informatieveiligheid in het sociaal domein. In de raadsworkshop, die de rekenkamer jaarlijks met de raad houdt om te komen tot mogelijke onderzoeksonderwerpen, kwam het onderwerp ‘privacy in het sociaal domein’ als gewenst onderzoeksonderwerp naar voren. De raadsworkshop vond in 2018 plaats op 5 februari.

Om deze drie redenen heeft de rekenkamer een onderzoek uitgevoerd naar de stand van zaken van informatieveiligheid en privacy in Heerhugowaard; toegespitst op het sociaal domein.

Doelstelling en vraagstelling

Doelstelling onderzoek

De doelstelling van dit onderzoek is om de raad inzicht te bieden in de mate waarin privacy en informatieveiligheid in het sociaal domein voldoende gewaarborgd zijn en indien nodig mogelijkheden voor verbetering aandragen.

Hoofd- en deelvragen

Op basis van deze doelstelling is de volgende hoofdvraag geformuleerd:

In hoeverre is de privacy van inwoners en de beveiliging van persoonsgegevens in het sociaal domein van de gemeente Heerhugowaard gewaarborgd?

Deze hoofdvraag is door de rekenkamer vertaald in de volgende deelvragen, gerangschikt naar thema:

[1] Autoriteit persoonsgegevens: https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/gemeente/sociaal-domein

Beleid

1 Op welke wijze heeft de gemeenteraad kaders gesteld ten aanzien van informatiebeveiliging en privacybeleid in het sociaal domein; en welke rol neemt zij ten aanzien van dit onderwerp in?

Governance en werkprocessen

2 Hoe is de governance van het privacybeleid en informatieveiligheid in het sociaal domein vormgegeven?
3 Hoe functioneert de governance in de praktijk?
4 Welke werkafspraken zijn er binnen de gemeente gemaakt rondom gegevensverwerking en –beveiliging en rondom beveiligingsincidenten in het sociaal domein?
5 Hoe verloopt de omgang met persoonsgegevens in de praktijk?
6 Op welke wijze geeft het college van B&W invulling aan de actieve en passieve informatieverstrekking aan de gemeenteraad met betrekking tot informatieveiligheid en privacy in het sociaal domein?

Beheer en opslag gegevens

7 Is er zicht op:
   a. welke informatiesystemen er binnen de gemeente persoonsgegevens registreren;
   b. hoe de toegang van medewerkers tot informatiesystemen is geregeld (autorisatieregisters);
   c. hoe de verwerking van persoonsgegevens door samenwerkende partijen is geregeld (bewerkersovereenkomsten).

Bewustzijn

8 Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers in het sociaal domein op het gebied van privacy en informatieveiligheid?

Onderzoeksuitvoering

Dit onderzoek is opgenomen in het jaarplan van de rekenkamer voor het jaar 2018. Dit jaarplan is uitgebracht op 20 maart 2018. De onderzoeksopzet van dit onderzoek is op 3 mei 2018 afgerond en op 22 mei tijdens de vergadering van het presidium besproken.

Op 31 mei 2018 vond het startgesprek plaats. Hierbij was de Chief Information Security Officer (CISO) van de gemeente Heerhugowaard aanwezig. De onderzoekers voerden hun werkzaamheden uit in de periode juni-september 2018. De werkzaamheden bestonden uit een documentstudie, interviews en het schrijven van de rapportage. De interviews vonden op 5 en 12 juli 2018 plaats (zie bijlage 1 voor een overzicht van personen die de rekenkamer in het kader van dit onderzoek sprak). Van deze gesprekken zijn verslagen gemaakt. De verslagen zijn ter verificatie aan de respondenten voorgelegd en geaccordeerd.

Op 27 september is de Nota van bevindingen aan de organisatie aangeboden voor een toets op de feitelijke juistheid van de bevindingen in het kader van het ambtelijk wederhoor. Op **18 oktober** ontving de rekenkamer de reactie in het kader van het ambtelijk wederhoor. Op 25 oktober is het rapport verstuurd voor een bestuurlijke reactie. Het eindrapport is op 13 november verstuurd naar de griffie ten behoeve van de gemeenteraad.

Leeswijzer

Dit rapport bestaat uit twee delen: de Bestuurlijke nota en de Nota van bevindingen. De Bestuurlijke nota bevat deze onderzoeksverantwoording, die wordt gevolgd door de centrale boodschap en de reactie van het college van B&W. De Nota van bevindingen bestaat uit vier hoofdstukken. Hoofdstuk 1 gaat in op het privacy- en informatieveiligheidsbeleid van Heerhugowaard. Hoofdstuk 2 beschrijft de governance van de gemeente Heerhugowaard met betrekking tot privacy en informatieveiligheid, zowel gemeentebreed als specifiek in het sociaal domein. Daarnaast wordt de rol die de raad inneemt beschreven. Hoofdstuk 3 richt zich op de werkprocessen en de omgang met gegevens in de praktijk. In hoofdstuk 4 wordt het bewustzijn omtrent privacy en informatieveiligheid van verschillende relevante groepen besproken, zoals medewerkers van de ambtelijke organisatie, gemeenteraadsleden en inwoners van de gemeente. Tot slot heeft dit rapport twee bijlagen. De vermelding van bronnen en respondenten is opgenomen in bijlage I en een verklaringen- en begrippenlijst in bijlage II.

Centrale boodschap

Conclusie

Heerhugowaard ziet het belang van privacy en informatieveiligheid in het algemeen, én specifiek voor de afdeling sociaal domein. Er is een centrale governancestructuur voor informatieveiligheid met een kernteam dat elkaar kan vervangen, en in aanloop naar de inwerkingtreding van de AVG is extra capaciteit aangetrokken om de voorbereiding goed te laten verlopen. Verder werkt de gemeente in 2018 aan nieuw beleid en zijn er cursussen omtrent veilig digitaal werken voor medewerkers. Eenieder die de website van de gemeente Heerhugowaard bezoekt, kan daar de benodigde informatie vinden over bewaartermijnen, het delen van gegevens met derden en de specifieke verwerkingen van persoonsgegevens binnen de gemeente.

Dit onderzoek toont echter ook aan dat er nog verbetermogelijkheden zijn:

/ Het actualiseren van het informatieveiligheidsbeleid en het privacybeleid in het najaar van 2018 betekent dat er qua beleid – anders dan op het niveau van specifieke maatregelen - niet is geanticipeerd op de AVG;
/ Niet alle geïnterviewden waren op de hoogte van het feit dat er binnen het sociaal domein een privacybeheerder is;
/ Datalekken worden gemeld bij de Autoriteit Persoonsgegevens, maar de procedure die hiervoor is vastgesteld komt niet geheel overeen met de praktijk;
/ Versleuteld mailen is (nog) niet mogelijk. Bijlagen kunnen wel beveiligd verzonden worden, maar het beeld is dat nog niet alle medewerkers weten hoe dit moet;
/ Recent werd geconstateerd dat medewerkers documenten soms op hun eigen schijf opslaan;
/ Zowel het flexwerken als de inrichting van fysieke werkplekken van de medewerkers van het sociaal domein bemoeilijken het waarborgen van de veiligheid van gegevens.

Daarmee komt de rekenkamer tot het beeld dat de gemeente Heerhugowaard goede stappen heeft gezet om privacy en informatieveiligheid te waarborgen, maar dat er zeker nog een verbeterslag gemaakt kan worden. Inhoudelijk geeft de rekenkamer daarvoor de onderstaande aanbevelingen mee.

Aanbevelingen

1. Besteed aandacht aan het privacyproof maken van de fysieke werkomgeving van medewerkers uit het sociaal domein.

Er zijn verschillende verbetermogelijkheden voor de werkplekken van medewerkers in het sociaal domein. Afsluitbare kasten zorgen er bijvoorbeeld voor dat een offline dossier niet voor iedereen toegankelijk is. Sommige gemeenten waar medewerkers van verschillende afdelingen door elkaar zitten, gebruiken privacyfilters voor het beeldscherm, om te zorgen dat alleen de gebruiker van de computer kan lezen wat er op het scherm staat. Bij de verbouwing van het gemeentehuis kan worden nagedacht over het inrichten van aparte werkruimtes voor medewerkers binnen het sociaal domein, zodat zij – bijvoorbeeld tijdens overleg – geen rekening hoeven te houden met de aanwezigheid van collega's van andere afdelingen die kunnen horen wat er over individuele inwoners wordt besproken.

2. Werk gestructureerd aan het privacybewustzijn in de organisatie.

In het huidige beleid wordt gesproken over 'onder de aandacht brengen bij medewerkers' en 'medewerkers waar nodig trainen'. Hier kunnen ook concrete acties benoemd worden. De handelswijzen van medewerkers zijn namelijk sterk bepalend voor de bescherming van privacy en informatieveiligheid in een gemeente: in 2016 had 60% van de datalekken in Heerhugowaard een menselijke oorzaak, in 2017 50% van de datalekken. Dat geeft aan dat het belangrijk is om constant aan het bewustzijn van medewerkers te werken. Daar zijn verschillende mogelijkheden voor. In plaats van het laten ondertekenen van een verklaring kan de organisatie nieuwe medewerkers praktijkdilemma's voorleggen; dat beklijft over het algemeen beter dan een verwijzing naar het beleid. Verder verspreidt de gemeente 'iBewust'-nieuwsberichten onder de medewerkers. Momenteel is niet bekend wat het effect hiervan is. Een overweging is om te monitoren hoe vaak deze nieuwsberichten worden gelezen, en om uit te zoeken of het tijdstip van verzending daar effect op heeft. Daaruit kan de gemeente afleiden welke thema's als minder interessant worden bevonden en mogelijk minder bekend zijn, en op welke momenten het nieuwsbericht het grootste bereik heeft. Daar kan dan op een andere manier informatie over worden verstrekt, bijvoorbeeld in teamoverleggen.

3. Zorg dat beleid en procedures op korte termijn geactualiseerd worden.

Actuele documenten kunnen als kapstok gebruikt worden voor de overige benodigde verbeterpunten. Bij het opstellen van beleidsstukken kan het raadzaam zijn om uitvoerend medewerkers te betrekken. Zij weten welke dilemma's er in de praktijk spelen en kunnen aangeven waar zij qua beleidsvoering behoefte aan hebben.

Reactie college van B&W

Heerhugowaard
Stad van kansen

Necker van Naem
T.a.v. mevr. E. Stumphius
Woudenbergseweg 50
3953 MH MAARSBERGEN

Contactpersoon:	dhr. T Quist	Ons kenmerk:	E201841011
Telefoon:	14 072	Relatiekenmerk:	
E-mail:	post@heerhugowaard.nl		
Onderwerp:	Bestuurlijke reactie rekenkameronderzoek sociaal domein		

Heerhugowaard, 9 november 2018

Geachte mevrouw Stumphius,

De rekenkamer heeft een onderzoek uitgevoerd naar privacy en informatieveiligheid in het sociaal domein en de resultaten opgenomen in een concept-rapportage. Zoals door u verzocht sturen wij u hierbij onze bestuurlijke reactie op deze rapportage.

Bestuurlijke reactie
Het college van de gemeente Heerhugowaard heeft kennis genomen van de resultaten van uw onderzoek naar privacy en informatieveiligheid in het Sociaal Domein. Zoals u terecht stelt zijn we, als gemeente, verantwoordelijk voor een juiste en veilige verwerking van persoonsgegevens. De Algemene Verordening Gegevensbescherming (AVG) heeft ertoe geleidt dat onze verantwoordelijkheid en de bijbehorende inspanning meer aandacht heeft gekregen. Deze verantwoordelijkheid hebben we niet alleen in het Sociaal Domein, maar in alle domeinen binnen onze organisatie. Het Sociaal Domein heeft daarbij onze verhoogde aandacht aangezien hierin zeer gevoelige gegevens van burgers in een afhankelijke positie ten opzichte van de gemeente worden verwerkt. Tegelijkertijd bemerken we bij ons streven naar een TOP-dienstverlening dat gegevensdeling soms gewenst is maar door de wetgeving wordt bemoeilijkt. Dit zorgt voor lastige bestuurlijke keuzes.

Onze organisatie heeft goede stappen gezet richting compliancy. Hierbij is prioriteit gegeven aan het inrichten van de governance, bewustwording creëren in de organisatie en het wegnemen van de grootste risicofactoren door technische danwel organisatorische maatregelen. We zien daardoor het bewustzijn toenemen binnen onze organisatie. Wel is hier nog borging van de gewenste houding en het gewenste gedrag noodzakelijk. De prioriteitstelling heeft ertoe geleid dat bijvoorbeeld het opstellen van privacybeleid een lagere prioriteit heeft gekregen. Om volledig compliant te worden met de AVG en privacy en informatieveiligheid in onze organisatie te borgen pakken we de beleidsvorming, samen met andere nog uit te voeren maatregelen, planmatig op. Deze gefaseerde aanpak doet ook recht aan de complexiteit en dagelijkse praktijk ten aanzien van informatieveiligheid en privacy in de uitvoering van het Sociaal Domein. De in uw aanbevelingen genoemde maatregelen worden nadrukkelijk in die gefaseerde aanpak opgepakt.

Mocht u naar aanleiding van onze reactie nog vragen hebben kunt u contact opnemen met de heer Quist.

Hoogachtend,
Burgemeester en wethouders van Heerhugowaard,
namens hen,

M.A.C. Quist,
CISO/PO

Parelhof 1 | Postbus 390 | 1700 AJ Heerhugowaard
Telefoon: 14 072 | Fax: (072) 575 55 56 | E-mail: post@heerhugowaard.nl | Internet: www.heerhugowaard.nl
IBAN: NL94 BNGH 0285 0035 77

Nota van bevindingen

1 Beleid

In dit hoofdstuk wordt eerst een algemene beschouwing gegeven op de aard van informatiebeveiligings- en privacybeleid in Heerhugowaard. Vervolgens wordt voor zowel informatiebeveiliging als privacy uiteengezet welke beleidsstukken gelden, wat de inhoud van deze stukken is en waar er nog ontwikkelpunten zitten. Ten slotte gaat dit hoofdstuk in op de rol van de gemeenteraad.

De volgende deelvraag staat centraal in dit hoofdstuk:

Beleid

/ *Op welke wijze heeft de gemeenteraad kaders gesteld ten aanzien van informatiebeveiliging en privacybeleid in het sociaal domein; en welke rol neemt hij ten aanzien van dit onderwerp in?*

1.1 / Algemene observaties privacy- en informatieveiligheidsbeleid

Beleid geeft vooral hoofdlijnen of uitgangspunten weer

Heerhugowaard kent een gemeentebreed informatieveiligheidsbeleid, opgesteld in 2015. Er is geen algemeen privacybeleid, maar voor het sociaal domein is wel een afdelingsspecifiek privacybeleid opgesteld, ook in 2015.[2] Beide documenten zijn beter te typeren als een verzameling van brede uitgangspunten dan als uitgebreide handleiding met voorschriften voor specifieke handelingen. In het Privacybeleid Sociaal Domein beschrijft het college waarom de gemeente kiest voor deze algemene uitgangspunten: door het opstellen van uitgangspunten verwacht de gemeente dat medewerkers zowel aan de specifieke als algemene eisen kunnen voldoen.[3] In de interviews bleek dat hier een visie aan ten grondslag ligt. De gemeente Heerhugowaard ziet zichzelf als een professionele organisatie waarin waarde wordt gehecht aan de eigen verantwoordelijkheid van medewerkers. Met de vastgestelde uitgangspunten in het achterhoofd kunnen de medewerkers zelf op professionele wijze hun afwegingen maken.

Om de uitgangspunten van het informatieveiligheidsbeleid ook in een praktijkomgeving te laten leven, is het beleid in werkoverleggen aan medewerkers gepresenteerd met concrete voorbeelden die aansluiten bij hun werkzaamheden. Dit draagt volgens geïnterviewden bij aan het bewustzijn van de medewerkers op het gebied van privacy en informatieveiligheid.

In paragrafen *1.2 privacybeleid* en *1.3 informatieveiligheidsbeleid* gaan we verder in op de inhoud van de beleidsstukken.

---

[2] Privacybeleid Sociaal Domein Heerhugowaard.

[3] Privacybeleid Sociaal Domein Heerhugowaard.

Baseline Informatievoorziening Gemeenten is de norm

In zowel het gemeentebrede informatieveiligheidsbeleid en het privacybeleid voor de afdeling Sociaal Domein van de gemeente Heerhugowaard komt naar voren dat de Baseline Informatiebeveiliging Gemeenten (BIG), zoals opgesteld door de Vereniging van Nederlandse Gemeenten (VNG), de norm is voor informatiebeveiliging.[4,5] Gemeentebreed moet dit zorgen voor een goede, zorgvuldige en veilige gegevensuitwisseling en procesuitvoering.

De BIG is een set normen en maatregelen voor een basis beveiligingsniveau op drie niveaus: strategisch, tactisch en operationeel.

Figuur 1 Overzicht Baseline Informatiebeveiliging Gemeenten[6]

Nieuw beleid is in de maak

In de interviews werd toegelicht dat de gemeente Heerhugowaard werkt aan zowel een privacybeleid als een nieuw informatieveiligheidsbeleid. De bedoeling is dat de twee beleidsstukken nog in 2018 worden vastgesteld.

Het nieuwe informatieveiligheidsbeleid en privacybeleid zullen volgens geïnterviewden de kapstok voor de protocollen en werkprocessen voor de afdelingen vormen. Tevens dienen beide beleidstukken volgens geïnterviewden als kapstok voor de bijbehorende actieplannen. De Functionaris Gegevensbescherming (FG) en de Chief Information Security Officer (CISO) kunnen de medewerkers hierbij ondersteunen en adviseren. De geïnterviewden gaven aan dat er ook in de opzet van het nieuwe beleid wordt vertrouwd op de professionaliteit van medewerkers. De FG en CISO zouden echter graag zien dat er meer toezicht komt op de uitvoering van het beleid. Dit is in overeenstemming met de AVG: overeenkomstig artikel 39 van de AVG is het de taak van de FG om toe te zien op de naleving.

Ook beleidsontwikkelingen op specifieke punten

Uit de interviews bleek dat voor sommige zaken nog geen richtlijn of beleid is ontwikkeld. De gemeente Heerhugowaard heeft bijvoorbeeld geen beleid opgesteld wat bepaalt of medewerkers gegevens op hun eigen devices mogen opslaan en bewaren. Recentelijk werd vastgesteld dat medewerkers nog veel informatie, veelal uit het verleden, in de vorm van bestanden bewaren op de netwerkschijven. Veel van deze bestanden bleken (bijzondere) persoonsgegevens te bevatten. Op basis van deze constatering is een ad hoc “schoonmaakactie” gehouden waarbij de betreffende medewerkers deze bestanden verwijderden dan wel in een map opsloegen die alleen voor geautoriseerde medewerkers toegankelijk is.

Onder het mom van ‘liever voorkomen dan genezen’ zouden de geïnterviewden graag zien dat er beleid op dit punt vastgesteld wordt, dat dit wordt uitgedragen en dat op de naleving wordt toegezien.

Uitvoerend medewerkers minder betrokken bij totstandkoming beleid privacy en informatieveiligheid

Volgens de geïnterviewden worden uitvoerend medewerkers over het algemeen vanaf het begin betrokken bij het vormgeven van beleid in de gemeente Heerhugowaard. Dit wordt door zowel uitvoerend medewerkers als

[4] Privacybeleid Sociaal Domein Heerhugowaard.

[5] Informatieveiligheidsbeleid Heerhugowaard.

[6] www.informatiebeveiliging-gemeenten.nl

beleidsbepalers gewaardeerd. Bij het opstellen van beleid specifiek op het gebied van informatieveiligheid en privacy ervaren medewerkers op de afdeling Sociaal Domein dat zij minder vaak worden gevraagd om input. Hierbij is het overigens wel relevant om op te merken dat de laatste keer dat beleidsstukken ten aanzien van privacy werden vastgesteld, in 2015 was.

1.2 / Privacybeleid

Zes uitgangspunten in het Privacybeleid Sociaal Domein

Ten tijde van de decentralisaties in het sociaal domein (2015) is het privacybeleid voor het sociaal domein vastgesteld.[7] Zes uitgangspunten vormen de basis van het privacybeleid van de gemeente Heerhugowaard. Deze zijn hieronder in tabel 1 weergegeven.

Tabel 1 Uitgangspunten Privacybeleid Sociaal Domein[8]

Uitgangspunten Privacybeleid Sociaal Domein (2015) inclusief korte toelichting
1. Wet bescherming persoonsgegevens (Wbp) is leidend
○ Vanuit de Wbp wil de gemeente zorgvuldige afwegingen te maken m.b.t. noodzaak, subsidiariteit en proportionaliteit en doelmatigheid van de gegevensverwerking. Verder wil de gemeente dat persoonsgegevens op een behoorlijke en zorgvuldige manier verwerkt worden en alleen voor duidelijk omschreven doelen worden gebruikt.
2. De hulpvraag van een burger is het vertrekpunt en burger wordt geïnformeerd
○ De hulpvraag (gevraagde voorzieningen, ondersteuning, uitkering) staat altijd centraal en het doel van gegevensverwerking staat hier altijd mee in verband. Inwoners worden daarbij geïnformeerd over wat er met de gegevens gebeurt en waarom.
3. Versterking positie van de burger
○ Het is van belang dat inwoners invloed en controle hebben over wat de gemeente met de gegevens van de inwoners doet. De drempel hiertoe dient laag te zijn.
4. Onderscheid tussen statusinformatie en inhoudelijke dossiers
○ Alleen regie- en statusinformatie kan gedeeld worden met als doel dubbel werk te voorkomen. Andere gegevens zijn alleen toegankelijk voor de desbetreffende afdeling.
5. Gegevensverwerking is ingebed in werkproces met duidelijk afwegingsmomenten
○ Door in het werkproces expliciet momenten voor gegevensverwerking op te nemen, blijft de organisatie gedwongen telkens keuzes te maken en daarin de aspecten integraal werken en privacy mee te nemen.
6. Ruimte om te leren
○ Aangezien de praktijk verandert, is het niet wenselijk om alles vooraf dicht te timmeren met regels. Hierdoor blijven er altijd keuzes. Het is belangrijk om medewerkers bewust te maken van de keuzes die ze hebben en hen bewust keuzes te laten maken. Dit biedt ook ruimte om te leren.

Naast de uitgangspunten bevat het privacybeleid informatie over hoe er om dient te worden gegaan met dossiers, autorisaties en bewaartermijnen. In het privacybeleid wordt ook verwezen naar de geheimhoudingsplicht die alle ambtenaren hebben, als onderdeel van de eed die zij afleggen bij indiensttreding.[9]

[7] Privacybeleid Sociaal Domein Heerhugowaard.

[8] Privacybeleid Sociaal Domein Heerhugowaard.

[9] Privacybeleid Sociaal Domein Heerhugowaard.

Privacybeleid Sociaal Domein benoemt verschillende acties

In het privacybeleid zijn verschillende acties opgenomen.[10] Het opstellen van het beleid was daarmee niet het slotstuk van een proces, maar één van de stappen in de doorlopende aandacht voor het thema privacy. Wat betreft het uitgangspunt "ruimte om te leren" wil de gemeente bijvoorbeeld in de praktijk ervaring opdoen en op basis hiervan mogelijk bijsturen.[11]

Concreet worden in het Privacybeleid Sociaal Domein de volgende acties benoemd:[12]

- Het beleid onder de aandacht brengen bij de medewerkers en waar nodig trainen.
- Het beleid onder de aandacht brengen bij alle inwoners en (keten)partners.
- Het beleid uitwerken en vastleggen in de werkprocessen (incl. autorisaties in systemen en archivering en vernietiging van gegevens en rollen en verantwoordelijkheden).
- Een convenant opstellen met de partners in de toegang.
- Opzetten van een lerende organisatie onder leiding van de Functionaris Privacybeleid, inclusief evaluatiecriteria, continue monitoren en jaarlijks een evaluatie/audit van het privacybeleid.

In 2018 wordt een nieuw privacybeleid opgesteld

Om te voldoen aan de verplichtingen uit de AVG wordt in 2018 een privacybeleid opgesteld. Een uitgangspunt in het huidige beleid is bijvoorbeeld dat de Wet bescherming persoonsgegevens (Wbp) leidend is. De Wbp is echter sinds 25 mei 2018 vervangen door de AVG. Het nieuwe privacybeleid krijgt een gemeentebreed karakter en vervangt daarmee het huidige beleid van het sociaal domein.

In de interviews werd aangegeven dat het nieuwe beleid ook antwoorden moet geven op dilemma's uit de praktijk. Sinds de decentralisaties wordt er meer integraal en klantgericht gewerkt binnen het sociaal domein. Dit staat soms op gespannen voet met de wijze waarop de privacy van inwoners beschermd moet worden. Denk hierbij bijvoorbeeld aan de situatie dat inwoners meermaals hun verhaal moeten doen bij verschillende medewerkers, omdat medewerkers de gegevens over de inwoner niet zomaar mogen delen. De geïnterviewden geven aan dat het goed is om in het nieuwe beleid te kijken naar dit spanningsveld, zowel om de medewerkers te faciliteren in hun werk als om te waarborgen dat inwoners de best mogelijke ondersteuning krijgen.

1.3 / Informatieveiligheidsbeleid

Informatieveiligheid is meer dan alleen ICT

Het huidige informatieveiligheidsbeleid van de gemeente Heerhugowaard dateert van 19 januari 2015. In het beleid geeft de gemeente duidelijk aan dat informatiebeveiliging méér is dan alleen ICT.[13] De gemeente beschrijft informatiebeveiliging als de beveiliging van alle uitingsvormen van informatie, alle mogelijke informatiedragers en alle informatie verwerkende systemen. Hieronder vallen ook, vooral, mensen en hun houdingen en gedragingen.[14] In het beleid zijn daarom ook ten aanzien van verantwoordelijkheden, werkprocessen, risico's en toegangsbeveiliging bepalingen vastgelegd.

Tien beleidsuitgangspunten als basis informatiebeveiligingsbeleid

Het college van B&W van de gemeente Heerhugowaard heeft in het informatiebeveiligingsbeleid tien uitgangspunten vastgesteld. De uitgangspunten hebben betrekking op de grondslagen van het beleid en op wie verantwoordelijkheid dragen voor het beleid. De uitgangspunten zijn als volgt:[15]

---

[10] Privacybeleid Sociaal Domein Heerhugowaard.

[11] Privacybeleid Sociaal Domein Heerhugowaard.

[12] Privacybeleid Sociaal Domein Heerhugowaard.

[13] Informatieveiligheidsbeleid Heerhugowaard .

[14] Informatieveiligheidsbeleid Heerhugowaard.

[15] Informatieveiligheidsbeleid Heerhugowaard.

Tabel 2 Uitgangspunten informatieveiligheidsbeleid gemeente Heerhugowaard

Uitgangspunten Informatieveiligheidsbeleid (2015)
1. Het college is binnen de gemeente verantwoordelijk voor het (laten) opstellen, uitvoeren en handhaven van een normenkader rondom informatiebeveiliging volgens het principe van verplichtende zelfregulering (pas toe of leg uit).
2. De BIG vormt de basis voor het Heerhugowaardse informatiebeveiligingsbeleid.
3. Ambitieniveau is het voldoen aan de minimumvereisten van landelijke en Europese wet- en regelgeving.
4. Belangrijkste grondslag voor de aanpak is een risico-afweging: risico = kans x impact.
5. De informatiebeveiligingsmaatregelen zijn afgestemd op de risico's en wettelijke vereisten.
6. Het management stelt de nodige mensen en middelen beschikbaar om aan de in dit beleid gestelde normen te kunnen voorzien.
7. Informatiebeveiliging is een integraal onderdeel van de bedrijfsvoering.
8. Toegang tot het gemeentelijke netwerk afschermen op het hoogste niveau, daarbinnen is de informatie voor alle medewerkers maximaal toegankelijk.
9. De informatieveiligheid staat of valt met medewerkers die zich hiervan bewust zijn en hier taakvolwassen mee omgaan.
10. Het informatiebeveiligingsbeleid wordt minimaal één keer per twee jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.

Informatieveiligheidsniveaus ingedeeld in classificatiemodel op basis van drie kernelementen

De gemeente Heerhugowaard herkent drie kernelementen in het kader van informatiebeveiliging. Deze kernelementen zijn ontleend aan de BIG:[16]

- vertrouwelijkheid: beschermen van informatie tegen onbevoegde kennisname en verandering;
- integriteit: waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- beschikbaarheid: beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.

De gemeente hanteert een classificatiemodel op basis waarvan de wijze van beveiliging van informatie wordt bepaald. De drie hierboven genoemde kernelementen geven daar een structuur voor.[17] In tabel 3 zijn deze classificatieniveaus weergegeven.

Tabel 3 Classificatieniveaus en hun kenmerken[18]

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** Alle informatie die algemeen toegankelijk is voor eenieder. Er is geen schending van deze classificatie mogelijk. *(bv: algemene informatie op de externe website van de gemeente)*	**Beschermd** Het bedrijfsproces dat gebruikmaakt van deze informatie staat enkele (integriteits-)fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van deze classificatie kan enige (in-)directe schade toebrengen *(bv: rapportages)*	**Noodzakelijk** Er worden in de gemeente Heerhugowaard alleen gegevens verzameld en/of vastgelegd die verbonden zijn met onze bedrijfsvoering. Alle informatie en alle applicaties worden daarom beschouwd als noodzakelijk beschikbaar voor het functioneren van de Gemeente Heerhugowaard. Daarom hanteren we voor alle applicaties en gegevens een
Laag	**Bedrijfsvertrouwelijk** Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van deze		

[16] Informatieveiligheidsbeleid Heerhugowaard.

[17] Zoals vastgesteld in het informatieveiligheidsbeleid Heerhugowaard.

[18] Integraal overgenomen uit het informatieveiligheidsbeleid van de gemeente Heerhugowaard.

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
	classificatie kan enige (in)directe schade toebrengen. *(bv: informatie op het intranet)*		zelfde niveau van beschikbaarheid. (Toelichting: 80% van de programmatuur is noodzakelijk voor het dagelijks functioneren van de organisatie. Het is complexer en kostbaarder om voor het enkele programma dat geen hoge beschikbaarheid nodig heeft aparte maatregelen te treffen voor lagere beschikbaarheid.)
Midden	**Vertrouwelijk** Informatie die alleen toegankelijk mag zijn voor een beperkte groep medewerkers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen. *(bv: persoonsgegevens, financiële gegevens*	**Hoog** Het bedrijfsproces dat gebruik-maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van deze classificatie kan serieuze (in)directe schade toebrengen. *(bv: bedrijfsvoeringsinformatie en primaire procesinformatie zoals vergunningen)*	
Hoog	**Geheim** Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote schade toebrengen. *(bv: zorggegevens en strafrechtelijke informatie, Bibob)*	**Absoluut** Het bedrijfsproces dat gebruikmaakt van deze informatie staat geen (integriteits-)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen. *(bv: financiële administratie, uitekeringenadministratie, gezinsplannen in het kader van de 3 Decentralisaties)*	

In het informatieveiligheidsbeleid is daarnaast per kernelement (vertrouwelijkheid, integriteit, beschikbaarheid) een tabel opgenomen die de specifieke beveiligingseisen per classificatieniveau op dat kernelement beschrijft.[19] In deze specifieke tabellen zijn per niveau en kernelement de authenticatie, autorisatie, monitoring en beveiliging opgenomen. Voor deze tabellen verwijzen wij u graag naar het informatieveiligheidsbeleid van de gemeente Heerhugowaard.

1.4 / Rol van de gemeenteraad

Gemeenteraad behoort niet tot de doelgroepen van het informatiebeveiligingsbeleid

In het informatiebeveiligingsbeleid uit 2015 is een lijst opgenomen met doelgroepen voor het informatiebeveiligingsbeleid.[20] Zo is bijvoorbeeld opgenomen dat het college van B&W integraal verantwoordelijk is, het management zorgt voor de kaderstelling en medewerkers van de ambtelijke organisatie relevant zijn voor het informatiebeveiligingsbeleid vanwege hun gedrag en de naleving van het beleid. De gemeenteraad wordt hierin niet als één van de doelgroepen genoemd.

Beperkte aandacht voor de gebruikersrol van de raad

In Heerhugowaard is er (nog) geen aandacht voor de gebruikersrol van de raad op het gebied van informatieveiligheid en privacy. Naast informatieverwerker is de raad, ook verwerkingsverantwoordelijke in de zin van de AVG. De CISO en de griffie hebben contact gehad over een presentatie bij de raad op het gebied van informatieveiligheid en privacy, waar ook deze rollen behandeld kunnen worden. De griffier stond hier positief tegenover.

[19] Zoals vastgesteld in het informatieveiligheidsbeleid Heerhugowaard.

[20] Informatieveiligheidsbeleid Heerhugowaard.

2 Governance

In dit hoofdstuk wordt ingegaan op hoe de governance van de gemeente Heerhugowaard is ingericht op het gebied van privacy en informatieveiligheid in het algemeen, hoe de afdeling Sociaal Domein personeel is vormgegeven en welke medewerkers werken aan privacy en informatieveiligheid binnen de afdeling Sociaal Domein. Er is daarbij zowel aandacht voor de governance op papier als in de praktijk. Het hoofdstuk gaat ook in op hoe het college van B&W invulling geeft aan informatieverstrekking aan de raad met betrekking tot informatieveiligheid en privacy in het sociaal domein.

De volgende deelvragen staan centraal in dit hoofdstuk:

Governance en werkprocessen

- *Hoe is de governance van het privacybeleid en de informatieveiligheid in het sociaal domein vormgegeven?*
- *Hoe functioneert de governance in de praktijk?*
- *Op welke wijze geeft het college van B&W invulling aan de actieve en passieve informatieverstrekking aan de gemeenteraad met betrekking tot informatieveiligheid en privacy in het sociaal domein?*

2.1 / Verantwoordelijke functionarissen informatieveiligheid en privacy

Governance in theorie: taakverdeling opgenomen in informatiebeveiligingsbeleid

In het informatieveiligheidsbeleid is een overzicht van de rollen, taken en verantwoordelijkheden rond informatiebeveiliging opgenomen. Hieronder zijn de belangrijkste functies en verantwoordelijkheden weergegeven zoals ze in het beleid voorkomen.[21] Voor de volledige lijst verwijzen wij u graag naar het informatieveiligheidsbeleid van de gemeente Heerhugowaard.

- **Het college van Burgemeester en Wethouders** is integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente (beslissende rol).
- Het **Managementteam** is verantwoordelijk voor realisatie en sturing (sturende rol).
- De **Informatie Beveiligingsfunctionaris** (IBF)[22] coördineert, bevordert en adviseert gevraagd en ongevraagd over IB en rapporteert eens per half jaar concernbreed over de stand van zaken (coördinerende rol).
- De **proceseigenaar/applicatie-eigenaar/gegevenseigenaar** stelt voor eigen proces/applicatie/gegevens onder andere beveiligingseisen en rapportages vast (vragende rol).
- De **ondersteunende organisatieonderdelen** zoals ICT, HR en facilitair zijn verantwoordelijk voor doorvertaling en implementatie (uitvoerende rol).

[21] Informatieveiligheidsbeleid Heerhugowaard.

[22] De term IBF wordt niet meer gebruikt. Deze taken worden uitgevoerd door de CISO.

Governance in de praktijk: team voor privacy en informatieveiligheid ingevuld met bijna drie fte

De rollen die hierboven zijn beschreven, bestaan ook in de praktijk. De gehele governance rondom informatiebeveiliging en privacy is echter uitgebreider dan in het beleid beschreven is. De belangrijkste functies voor privacy en informatieveiligheid maken deel uit van het team privacy en informatieveiligheid. Dit team bestaat uit bijna drie fte. Binnen dit team zijn de volgende functies actief:

- Een CISO[23]/ Privacy Officer (dubbelfunctie)
- Een coördinator informatieveiligheid/Privacy Officer (dubbelfunctie)
- Twee FG's (waarvan één ad interim tot 1 oktober 2018)

Ten aanzien van de privacy officers geldt dat zij ieder een andere focus hebben. De CISO opereert op strategisch niveau, de coördinator informatieveiligheid op tactisch/operationeel niveau.

De FG's en CISO zijn er voor alle onderdelen van de gemeente (ambtelijke organisatie, college, burgemeester en de raad) en voor de inwoners van de gemeente. De CISO en FG's zijn werkzaam bij zowel de gemeente Heerhugowaard als bij de gemeente Langedijk.

De functionarissen in het team voor privacy en informatieveiligheid gaven aan elkaars taken over te kunnen nemen indien nodig: ze trekken op veel terreinen samen op en er is een goede werkrelatie. Volgens geïnterviewden is de huidige formatie nodig om de werkzaamheden adequaat op te pakken. De afgelopen maanden hebben zij ervaren dat (tijdelijk) zelfs meer formatie benodigd is om bijvoorbeeld de vele vragen en adviesverzoeken vanuit de organisatie te kunnen behandelen. In diverse andere gemeenten is minder formatie beschikbaar. De geïnterviewden schatten in dat dit een weerslag heeft op het adequaat kunnen oppakken van privacy in de organisatie.

Periodiek overleg CISO en portefeuillehouder Bedrijfsvoering; niet met portefeuillehouders Sociaal Domein

De CISO is het vaste aanspreekpunt voor de wethouders bij vragen en opmerkingen over informatieveiligheid en privacy. De CISO van de gemeente Heerhugowaard is tevens Privacy Officer. Als CISO is hij aanspreekpunt voor het bestuur op het gebied van informatieveiligheid en als Privacy Officer is hij, evenals de FG, aanspreekpunt voor het bestuur op het gebied van privacy. De CISO heeft een periodiek overleg met de gemeentesecretaris. Daarnaast overleggen de CISO en de portefeuillehouder Bedrijfsvoering, waar ICT onder valt, maandelijks over informatieveiligheid en privacy. Met de andere portefeuillehouders heeft de CISO geen terugkerend overleg. Als er iets speelt met betrekking tot informatieveiligheid of privacy, informeert de CISO de wethouders uiteraard wel. De wethouders worden in het geval van een datalek zo geïnformeerd dat zij in staat zijn om inwoners, raad en media indien nodig te woord te staan. Details worden in de meeste gevallen niet gedeeld met de wethouders.

2.2 / Governance Sociaal Domein

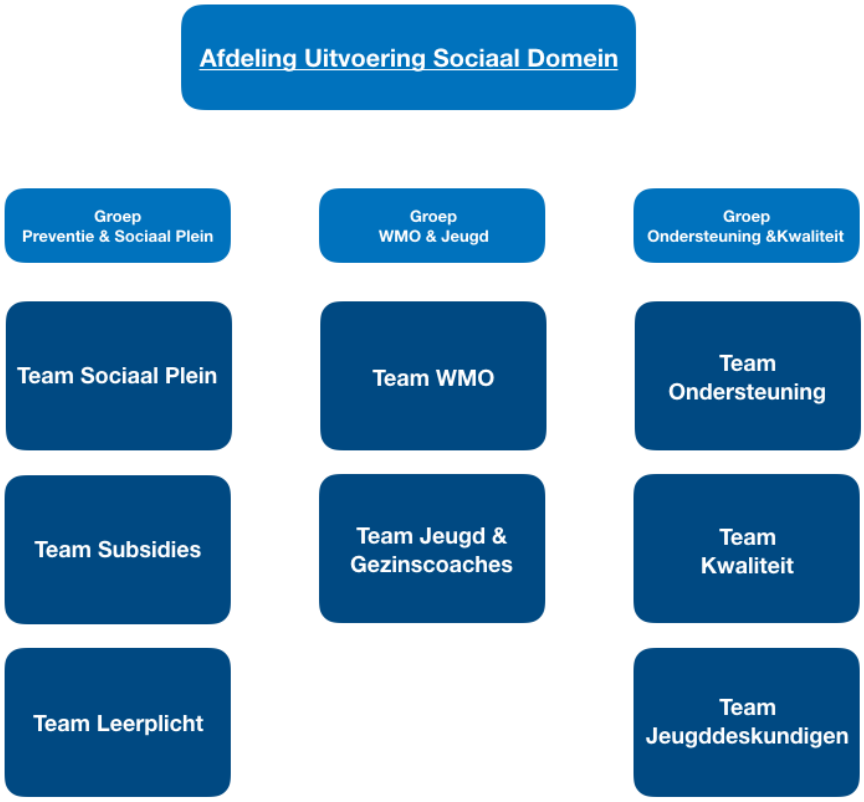
Het sociaal domein is verdeeld in drie basisgroepen

Het sociaal domein van de gemeente Heerhugowaard is ingedeeld in drie basisgroepen met ieder een eigen coördinator en onderliggende teams. Hierbij is het uitgangspunt dat de teams zodanig zijn ingedeeld, dat er meer recht wordt gedaan aan de zelfredzaamheid van de inwoners, dat er integraal gewerkt kan worden en dat er meer focus komt op de kerntaken van de verschillende basisgroepen.[24]

[23] Voordat de huidige CISO werd aangesteld op 1 december 2017, werden de taken van de CISO uitgevoerd door twee medewerkers, één uit de gemeente Heerhugowaard en één uit de gemeente Langedijk. De taakuitvoering door deze medewerkers stond onder druk, doordat de rol van CISO naast andere rollen diende te worden opgepakt.

[24] Basisgroepindeling dienstverlening Sociaal Domein.

Figuur 2 Organigram Sociaal Domein gemeente Heerhugowaard



Een continue functie voor privacy/informatieveiligheid, niet altijd bekend bij de medewerkers

In een addendum bij het informatiebeveiligingsbeleid is opgenomen dat er in het sociaal domein een privacy beheerder/informatieveiligheidsbeheerder actief is.[25]

Tijdens de interviews bleek dat deze persoon niet bij iedereen bekend is. Door een deel van de geïnterviewden werd wel aangegeven dat er een medewerker binnen het sociaal domein is die zich bezighoudt met dit thema, maar niet zozeer als privacy beheerder/informatieveiligheidsbeheerder.

Naar aanleiding van de genoemde privacy beheerder/informatieveiligheidsbeheerder gaven geïnterviewden aan dat er op een eerder moment een medewerker met de rol van privacy functionaris voor het sociaal domein in dienst was bij de gemeente Heerhugowaard. Deze heeft meegeholpen met de coördinatie van het privacybeleid. De geïnterviewden hebben geen concreet beeld van wat de taken van deze medewerker precies waren ten aanzien van de bescherming van privacy en informatieveiligheid in het sociaal domein.

2.3 / Informatievoorziening aan de gemeenteraad

Gemeenteraad wordt over informatieveiligheid geïnformeerd in de jaarstukken

Overeenkomstig de VNG-resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' van de VNG informeert de gemeente Heerhugowaard de raad volgens de methodiek van Eenduidige Normatiek Single Information Audit (ENSIA) over informatieveiligheid. ENSIA is in het leven geroepen om de verantwoordingslasten ten aanzien van informatieveiligheid te verminderen en de informatie toegankelijker te

[25] Governance Heerhugowaard concept – 21 november 2017.

maken. Het totale proces bestaat uit een voorbereiding, zelfevaluatie, horizontale verantwoording, verticale verantwoording en een evaluatie. In het jaarverslag van 2017 is in het kader van informatieveiligheid in de paragraaf dienstverlening onder andere opgenomen dat het Actieplan Informatieveiligheid is vastgesteld; dat er samen met de gemeente Langedijk twee functionarissen zijn aangesteld die de CISO-rol in beide gemeente vervullen en dat er maatregelen zijn genomen op het gebied van personele beveiliging, toegangsbeveiliging en het beheer van beveiligingsincidenten.[26] Naast doelen en resultatenvoortgang bevat de paragraaf in het jaarverslag informatie over incidenten in het afgelopen jaar. Tenslotte bevat de paragraaf in het jaarverslag de geselecteerde verbeteracties voor de komende jaren.[27]

Gemeenteraad stelt weinig vragen specifiek over informatieveiligheid en privacy

De geïnterviewden gaven aan dat de gemeenteraad niet veel aandacht heeft voor informatieveiligheid en privacy. In 2018 is er één vraag geweest over de twee thema's, gesteld door één partij.

Er zijn wel vragen gesteld die raakten aan informatieveiligheid en privacy, maar deze vragen vloeiden dan voort uit andere inhoudelijke terreinen (bijvoorbeeld het sociaal domein). Na een hack-incident in 2012 heeft de gemeenteraad wel specifieke vragen gesteld over die situatie.

[26] Jaarverslag 2017, paragraaf bedrijfsvoering.

[27] Jaarverslag 2017, paragraaf bedrijfsvoering.

3 Werkprocessen rondom gegevensverwerking

In dit hoofdstuk bespreken we de omgang met gegevens in de praktijk, en de maatregelen op het gebied van privacy en informatiebeveiliging waar medewerkers uit het sociaal domein dagelijks mee te maken hebben.

De volgende deelvragen staan centraal in dit hoofdstuk:

Governance en werkprocessen

- *Welke werkafspraken zijn er binnen de gemeente gemaakt rondom gegevensverwerking en –beveiliging en rondom beveiligingsincidenten in het sociaal domein?*
- *Hoe verloopt de omgang met persoonsgegevens in de praktijk?*

Beheer en opslag gegevens

- *Is er zicht op:*
  - *a) welke informatiesystemen er binnen de gemeente persoonsgegevens registreren;*
  - *b) hoe de toegang van medewerkers tot informatiesystemen is geregeld (autorisatieregisters);*
  - *c) hoe de verwerking van persoonsgegevens door samenwerkende partijen is geregeld (bewerkersovereenkomsten).*

3.1 / Werkprocessen - algemeen

Voorbereiding AVG planmatig uitgevoerd

Op 1 december 2017 is de huidige CISO benoemd als CISO en Privacy Officer. Samen met een tweede Privacy Officer heeft de CISO overlegd met relevante partners, bijvoorbeeld medewerkers van juridische zaken en HRM, over de voorbereidingen op de inwerkingtreding van de AVG. Tijdens deze overleggen is een stappenplan opgesteld. Dit stappenplan is gebaseerd op het stappenplan zoals opgesteld door de Autoriteit Persoonsgegevens (AP), bestaande uit tien stappen.[28]

Onderdelen van het stappenplan van de gemeente Heerhugowaard waren onder andere het voorbereiden op verzoeken om inzage in gegevensverwerkingen van betrokkenen, het opstellen van een register met gegevensverwerkingen en het aanstellen van een Functionaris voor de Gegevensbescherming (FG). Het aanstellen van een FG was de eerste stap die werd uitgevoerd door de gemeente Heerhugowaard. Per 1 februari 2018 werd er een FG (ad interim) aangesteld. Ten tijde van de interviews (juli 2018) zijn ook de stappen 'voorbereiding op verzoeken van betrokkenen' en het opstellen van een register van gegevensverwerking, afgerond. Ten aanzien van andere stappen uit het stappenplan, zoals het bewust maken van de organisatie, het

[28] AVG 10-stappenplan. Voor meer informatie zie: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-biedt-10-stappenplan-voorbereiding-nieuwe-privacywet.

uitvoeren van data protection impact assessments (PIA), het toepassen van privacy by design en privacy by default en het aanpassen van de voorwaarden van de huidige bewerkersovereenkomsten, zijn de werkzaamheden gestart.

In het register van gegevensverwerkingen zijn per afdeling de gegevensverwerkingen opgenomen. Op het moment van schrijven (september 2018) is nog niet voor alle verwerkingen de complete hoeveelheid informatie opgenomen: sommige kolommen zijn nog leeg. Gedurende 2018 wordt dit register verder aangevuld. In de interviews werd aangegeven dat het register ook daarna een 'levend' document blijft; nieuwe verwerkingen worden zo snel mogelijk in het register opgenomen. De categorieën van informatie die over de verwerkingen worden opgenomen komen overeen met de vereisten die hiervoor gelden.

Het voldoen aan de AVG is een voortdurend proces, dat constant aandacht vraagt. Dat zien ook de geïnterviewden. Zij gaven aan dat een gemeente niet kan voldoen aan de eisen uit de AVG door eenmalig een aantal stappen uit te voeren. De maatregelen moeten continue uitgevoerd en verbeterd worden, zodat het risico op normafwijkende gebeurtenissen wordt geminimaliseerd.

Procedure wijzigingsbeheer vastgelegd voor de gehele organisatie

Heerhugowaard kent een vastgestelde procedure en afspraken voor het doorvoeren van wijzigingen in de ICT-infrastructuur.[29] Voorbeelden van uitgangspunten die gehanteerd worden, zijn bijvoorbeeld dat wijzigingen eerst in een testomgeving plaatsvinden, en dat er tijdens vakanties standaard geen wijzigingen worden ingepland. Het document over wijzigingsbeheer beschrijft de taken en verantwoordelijkheden rondom de verschillende stappen die een wijziging kent, middels een RACI-matrix (Responsible, Accountable, Consulted, Informed–matrix). Verder beschrijft het document te nemen processtappen in het wijzigingsbeheerproces, wat er geregistreerd wordt met betrekking tot de wijzigingen en hoe er over de wijzigingen gecommuniceerd wordt.

Autorisaties voor applicaties niet altijd up-to-date, afdelingsmanagers verantwoordelijk

Per afdeling en applicatie bestaan verschillende werkwijzen rondom het inrichten en up-to-date houden van autorisaties. Autorisaties voor toegang tot dossiers en applicaties worden aangevraagd door de manager van een afdeling. De manager is ook verantwoordelijk voor het doorgeven van wijzigingen in autorisaties bij bijvoorbeeld een wijziging van functie en in- of uitdiensttreding. De afdelingsmanager geeft wijzigingen door aan de betreffende applicatiebeheerder. Dit gaat volgens de geïnterviewden over het algemeen goed, alhoewel het soms even kan duren voordat het geregeld is, omdat het up-to-date houden van de autorisaties vrij veel tijd vraagt van de afdelingsmanager. In het tweede kwartaal van 2018 is er daarom een inhaalslag uitgevoerd om alle autorisaties up-to-date te krijgen. Om een dergelijke inhaalslag niet nodig te hebben en de druk op de manager te verlichten, wordt de mogelijkheid verkend om de aanvraag van autorisaties te standaardiseren.

Werken op eigen *devices* kan alleen met een tweefactor-authenticatie

De gemeente stimuleert het werken op eigen devices (zie paragraaf 4.3). Om te kunnen werken via een eigen device is er een tweefactor-authenticatie methode vastgesteld die, ongeacht de locatie van werken, altijd doorlopen moet worden bij het inloggen op de virtuele werkplek. Een aantal applicaties werkt met SSO (Single Sign On, eenmalige inlog waarna automatisch toegang wordt verschaft tot meerdere applicaties), voor andere applicaties dient altijd ingelogd te worden met een combinatie van gebruikersnaam en wachtwoord.

[29] Document wijzigingsbeheer (februari 2018).

3.2 / Werkprocessen - sociaal domein

Bepalingen autorisaties sociaal domein opgenomen in Privacybeleid Sociaal Domein

In het privacybeleid van de afdeling Sociaal Domein is op hoofdlijnen opgenomen welke autorisaties en toegang tot dossiers en/of gegevens horen bij welke rollen van medewerkers. Daarbij worden vijf rollen herkend. Op hoofdlijnen worden autorisaties als volgt aan deze vijf rollen toegewezen:[30,31]

- **Vraagverkenner**: de medewerker die het eerste gesprek met de cliënt voert. Hij/zij heeft alleen zicht op de status van lopende aanvragen en voorzieningen. De inhoudelijke dossiers kan men niet zien.
- **Medewerker Intake**: de medewerker handelt de enkelvoudige zaken af. Van de zaak die aan hem/haar is toegewezen kan men de vraagverkenning (verslag) inzien en hij/zij heeft toegang tot het dossier van de cliënt voor wat betreft de enkelvoudige aanvraag (dus: gaat het om een WMO-voorziening, dan alleen inzage in WMO-dossier van de cliënt en geen toegang tot het dossier van de cliënt over jeugdhulp of werk & inkomen).
- **Regisseur**: de medewerker handelt de meervoudige zaken af. Van de zaak die aan hem/haar is toegewezen kan men de vraagverkenning (verslag) inzien en de status van lopende aanvragen en voorzieningen. De regisseur heeft toegang tot het plan dat in het kader van '1gezin, 1plan' door de regisseur en de cliënt is opgesteld en bewaakt de acties die hieruit voortkomen. De regisseur heeft geen inzage in de achterliggende dossiers bij de vakafdeling wat de uitvoering van genoemde acties betreft (ziet wel de status, maar niet de inhoud erachter).
- **Medewerker Toetsing**: bij de jeugdhulp is een splitsing gemaakt tussen de ingehuurde medewerker intake die in gesprek met de cliënt komt tot een advies en de toekenning van een voorziening. Indien een maatwerkvoorziening wordt geadviseerd, beoordeelt de medewerker toetsing deze. Hij/zij heeft toegang tot de vraagverkenning en het advies en niet tot het inhoudelijke dossier.
- **Administratief medewerker**: hier gaat het om opdrachtverstrekking aan een zorgaanbieder, het afhandelen van declaraties en betalingen en verkrijgen van managementinformatie. Administratief medewerkers hebben in de regel geen toegang tot inhoudelijke dossiers, maar alleen inzage in de afgegeven beschikkingen en/of acties (opdracht zonder beschikking) en kunnen geanonimiseerd managementinformatie genereren. In afwijking van dit beleid werd tijdens het onderzoek aangegeven dat binnen het team Jeugd zowel de financiële administratief medewerkers als de administratief medewerkers toegang hebben tot de inhoud van het dossier in Mens Centraal.

Inrichting werkplekken sociaal domein ontoereikend om privacy te waarborgen

In de interviews is aangegeven dat op de werkplekken voor het sociaal domein privacy en informatieveiligheid niet voldoende geborgd kan worden. Dat is terug te leiden tot twee aspecten: de open werkruimte en het onvoldoende beschermen van papieren informatie.

Gedeelde werkruimte: op het kantoorplein zitten veel verschillende medewerkers, variërend van vaste krachten en ingehuurde medewerkers tot stagiairs, en zowel medewerkers van de afdeling Sociaal Domein als medewerkers van andere afdelingen. In de interviews werd aangegeven dat medewerkers zich niet altijd bewust zijn van deze omgeving wanneer zij tijdens het overleg met collega's persoonlijke informatie van inwoners bespreken. Dit kan voorkomen worden door te bellen en te overleggen in afgesloten ruimtes, maar deze ruimtes zijn er maar beperkt.

Beschermen van papieren informatie: er wordt nog regelmatig met papieren dossiers of papieren aantekeningen gewerkt binnen het sociaal domein. Een deel van de medewerkers in het sociaal domein laat deze dossiers op 'hun' bureau liggen als zij naar een inwoner of een overleg gaan, om te voorkomen dat een collega aan het bureau gaat werken. Omdat alle medewerkers van de gemeente op de afdeling sociaal domein mogen komen, zijn de dossiers voor meer mensen toegankelijk dan noodzakelijk. Ook als de dossiers wel in een kast worden opgeborgen, kan het voorkomen dat ze nog breed toegankelijk zijn: niet alle kasten zijn voorzien van een slot.

[30] Privacybeleid Sociaal Domein Heerhugowaard.

[31] Dit betreft de vijf rollen zoals beschreven in het privacybeleid van de gemeente Heerhugowaard. Mogelijk verschillen de benamingen en precieze invullingen van de rollen voor specifieke teams binnen de afdeling Sociaal Domein.

In de overleggen wordt verschillend omgegaan met al dan niet anoniem bespreken van casussen

Bij het team WMO vinden in deelgroepen casuïstiekoverleggen plaats, waar casussen niet anoniem worden besproken. De casuïstiek overleggen van het team Inkomen worden in 2018 opnieuw ingericht, de organisatie geeft aan dat privacy hierbij een aandachtspunt zal zijn. Daarnaast vindt om de dag een startoverleg plaats, waar jeugd, WMO, en het Sociaalplein vertegenwoordigd zijn. Hier sluiten ook vertegenwoordigers van directe ketenpartners bij aan. In dit overleg worden casussen wel anoniem besproken. In het algemeen is volgens de geïnterviewden de regel dat casussen alleen niet anoniem worden besproken in het kleine gezelschap van de deelgroep.

De jeugddeskundigen hebben een eigen casuïstiekoverleg. De jeugddeskundigen overleggen daarnaast met de jeugdgezinscoaches over het advies van de jeugdgezinscoach. Dit draagt de naam 'adviestafel'. Uit deze overleggen volgen adviezen voor klanten. Deze adviezen worden teruggelegd bij de klant die vervolgens kan aangeven of en waarom hij of zij het al dan niet eens is met het advies. Hier worden casussen geanonimiseerd besproken.

Daarnaast zijn er overleggen tussen leden van verschillende teams en overlegstructuren met externe partners. Het 18-/18+ overleg is een overleg waarbij vertegenwoordigers van de teams Participatie, Jeugd en WMO en medewerkers van de regionale meld- en coördinatiefunctie vroegtijdig schoolverlaten (RMC) aanwezig zijn. Hier worden casussen anoniem besproken. Het overleg Veilig Thuis en het multidisciplinaire aanpak-overleg (MDA++-overleg) zijn overlegstructuren met externe partners. Tijdens deze overleggen werken de gesprekspartners volgens een speciaal privacy convenant dat door de overlegpartners is afgesproken. Het privacyconvenant voor het MDA++ overleg is overigens nog niet formeel door de betrokken colleges bekrachtigd. Hiervoor zijn de colleges in afwachting van de uitkomsten van een DPIA (data protection impact assessment).

Onderling sparren leidt tot risico's voor privacy

Naast de officiële werkoverleggen wordt er veel gespard door teamleden onderling. Dit heeft nadelen. Zo worden er tijdens deze (veelal openbare) overlegmomenten voor de rest van de afdeling hoorbaar persoonsgegevens besproken en zorgt het voor geluidsoverlast voor de andere medewerkers. Er wordt daarom op korte termijn met het team gesproken over het sparren. De gemeente is voornemens om hier een gedragscode voor op te stellen.

Dossiervorming rondom inwoners

De Jeugdgezinscoaches en jeugddeskundigen delen informatie via een systeem van de gemeente: MensCentraal. De medewerkers van het team WMO werken met het systeem CiVision Samenlevingszaken. Binnen deze systemen wordt gewerkt met verschillende autorisatieniveaus. Medewerkers van WMO hebben geen toegang tot de inhoud van de dossiers van Jeugd en medewerkers van Jeugd hebben geen toegang tot de inhoud van de dossiers van WMO. De medewerkers kunnen wel zien welke medewerker er betrokken is bij een klant. Binnen de teams WMO en Jeugd hebben de gezinscoaches en WMO-consulenten binnen de eigen groep wel toegang tot elkaars dossiers. Dit zorgt ervoor dat medewerkers elkaar makkelijk kunnen vervangen. Naast de verantwoordelijk coaches hebben leden van het crisisteam die ook een directe werkverbinding hebben met het team Jeugd of WMO, toegang tot de dossiers.

Het dossier van een klant wordt afgesloten als er een antwoord wordt gegeven op de vraag die is opgesteld. Verdere monitoring van de klant volgt meestal via aparte stappen in het systeem.

De dossiers worden uiteindelijk digitaal gearchiveerd in het archiefsysteem Corsa. In Corsa is op basis van autorisatie een splitsing gemaakt, zodat alleen de coaches van de betrokken afdeling toegang hebben tot de eigen archiefdossiers. De gezinsplannen worden niet gearchiveerd in Corsa. Deze worden in MensCentraal bewaard volgens de wettelijk bepaalde bewaartermijn. Deze termijnen zijn geautomatiseerd in het systeem van MensCentraal.

Contact met klanten/inwoners via de mail; gevoelig voor fouten

De medewerkers van de afdelingen Jeugd en WMO hebben veel contact met hun klanten via de mail. Informatie wordt ook via de mail gedeeld. Recent ontstond een datalek. Er werd een document, bestemd voor een klant, naar een verkeerd e-mailadres verstuurd. Dit gebeuren is geëscaleerd naar de teamleider en er is concrete actie ondernomen. De betrokkenen zijn geïnformeerd, en er is gesproken met de betreffende medewerker. Ook de wethouder is direct geïnformeerd over het datalek. Om een dergelijk voorval in de toekomst te voorkomen, is aan medewerkers gecommuniceerd om in het vervolg alleen nog met een wachtwoord beveiligde bestanden naar de klant te mailen. De geïnterviewden geven aan dat dit geen ideale oplossing is, maar de beste optie binnen de

huidige mogelijkheden. Binnen de organisatie leeft het beeld dat nog niet alle medewerkers weten hoe zij op deze manier kunnen mailen.

Overleg tussen CISO en medewerkers sociaal domein bij datalek

Er is geen vast afstemmingsmoment tussen uitvoerend medewerkers van het sociaal domein en de Chief Information Security Officer (CISO). Er is incidenteel contact wanneer er sprake is van een datalek, of als er vragen leven ten aanzien van informatieveiligheid. Niet alle medewerkers van het sociaal domein zijn bekend met de CISO, ditzelfde geldt voor de Functionaris Gegevensbescherming (FG).

3.3 / Inrichting samenwerkingsverbanden

Samenwerking met externen alleen via Zorgring

De afdeling Sociaal Domein is aangesloten bij Zorgring[32] en werkt alleen samen met externe partners die ook zijn aangesloten bij en werken via Zorgring. Zorgring zorgt ervoor dat gegevens veilig gedeeld kunnen worden. Via Zorgring worden zowel onderling gegevens gedeeld als met gecontracteerde externe partners. Met externe partners worden ook verwerkersovereenkomsten afgesloten. In het kader van dit onderzoek heeft de rekenkamer een dergelijke verwerkersovereenkomst ingezien. Deze komt overeen met de gebruikelijke standaard voor verwerkersovereenkomsten.

Samenwerking gemeenten, instellingen en inwoners in het Sociaalplein

Op 1 januari 2015 is het Sociaalplein in Heerhugowaard geopend. Hierbinnen werken de gemeente Heerhugowaard, instellingen uit het sociaal domein[33] en inwoners samen als één netwerk. Dit netwerk heeft als doel de toegang tot zorg en gemeentelijke voorzieningen in goede banen te leiden.[34] Bij het Sociaalplein kunnen inwoners van de gemeente Heerhugowaard die vragen hebben over opvoeden & opgroeien, zorg & ondersteuning en werk & inkomen terecht. De professionals die actief zijn bij het Sociaalplein richten zich op de kwetsbaarheden én krachten van zowel de inwoners als hun sociale netwerken.

In september 2015 is door het college van de gemeente Heerhugowaard besloten dat het Sociaalplein op een buurtgerichte wijze georganiseerd zal worden, met centrale toegang en bedrijfsvoering in het Huis van Heerhugowaard.[35] Buurgericht werken zorgt ervoor dat er efficiënter en sneller kan worden ingespeeld op de vragen van inwoners. Betrokkenen voegen hieraan toe dat er ten tijde van het onderzoek, medio 2018, voornamelijk samen wordt gewerkt rondom een aantal thema's, en niet (meer) zo duidelijk buurtgericht.

De gemeente Heerhugowaard heeft het werken met convenanten in het privacybeleid opgenomen

In het privacybeleid van de afdeling Sociaal Domein is opgenomen welke afspraken er moeten worden gemaakt en vastgelegd wat betreft de omgang met privacy door alle partijen die samenwerken in/met de buurt- en wijkteams.[36] Betrokkenen geven aan dat de gemeente Heerhugowaard niet werkt met wijk-of buurtteams, maar dat er sprake is van een netwerksamenwerking op doelgroep-niveau. Het beleid, het privacybeleid, spreekt juist wel van buurt- en wijkteams, waaraan de convenanten gekoppeld zijn.

In een convenant met een samenwerkingspartner dienen onder andere de wijze van verwerking van bijzondere persoonsgegevens overeengekomen te worden, dient te worden vastgelegd hoe betrokken burgers worden geïnformeerd over het gebruik van hun persoonsgegevens en in het convenant dient een beschrijving te worden vastgelegd van een procedure in verband met escalatie bij spoed- en/of noodgevallen. Voor het volledige

[32] Voor meer informatie over Zorgring, zie: https://www.zorgring.nl/

[33] Onder andere Halte Werk, Wijkverpleegkundigen S1, MET, J&G coaches (B&W besluit Buurtgericht Sociaalplein).

[34] Werkdocument het Sociaalplein.

[35] B&W besluit Buurtgericht Sociaalplein.

[36] Privacybeleid Sociaal Domein Heerhugowaard, Bijlage 1 Convenant met (keten)partners.

overzicht van afspraken en informatie die moet worden opgenomen in een convenant, verwijzen wij u naar het privacybeleid van de gemeente.[37]

Gemeente Heerhugowaard werkt met bewerkers- en raamovereenkomsten

De gemeente Heerhugowaard heeft voorbeelden van bewerkers- en raamovereenkomsten gedeeld met de rekenkamer. De gemeente Heerhugowaard heeft (in ieder geval) voor beschermd wonen en de uitvoering van de WMO zowel een raamovereenkomst als een bewerkersovereenkomst samen met de gemeenten Alkmaar, Bergen, Castricum, Heiloo, Heerhugowaard en Langedijk.[38]

In deze documenten is bijvoorbeeld de loopduur van de overeenkomst vastgesteld. Ook is vastgesteld aan welke eisen de bewerkers van informatie dienen te voldoen en hoe zowel de verantwoordelijke (degene van wie de informatie is) als de bewerker (degene die de informatie verwerkt) aan de wettelijke eisen voldoet.[39] De bewerkers- en raamovereenkomst komen overeen met dit type overeenkomsten in andere gemeenten.

Bewaartermijnen

De gemeente Heerhugowaard heeft in het privacybeleid de – ten tijde van het opstellen van het beleid geldende - maximale wettelijke bewaartermijn opgenomen. Deze is 15 jaar. Voor verwerking van gegevens in verband met zorgcoördinatie geldt een bewaartermijn van vijf jaar nadat het actieve dossier is afgesloten.

In de systemen van de gemeente wordt vastgelegd welke gegevens hoe lang bewaard mogen en moeten worden. Ook wanneer bewaartermijnen veranderen wordt dit in de systemen verwerkt. Soms kan of moet een hulpverlener gegevens toch langer bewaren “indien dat redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit” .

3.4 / (Zelf)evaluaties

Beperkt aantal zelfevaluaties

In Heerhugowaard zijn er maar een beperkt aantal zelfevaluaties die worden uitgevoerd voor privacy en informatieveiligheid. In het kader van de ENSIA wordt jaarlijks een zelfevaluatie uitgevoerd (zie paragraaf 2.3). Verder zijn in het kader van dit onderzoek geen gegevens over zelfevaluaties aangeleverd, anders dan de evaluatie in het kader van de Basisregistratie personen (BRP).
Gemeenten voeren jaarlijks een zelfevaluatie uit naar de inrichting, de werking en de beveiliging van de basisregistratie, alsmede naar de verwerking van gegevens in de BRP, voor zover het de gemeentelijke voorziening betreft of het college verantwoordelijk is voor het bijhouden hiervan (Wet basisregistratie personen, artikel 4.3). Hiervoor maken de gemeenten gebruik van een kwaliteitsmonitor. In 2017 scoorde de gemeente overwegend voldoende op het onderdeel ‘bestandscontrole’: alleen in de categorie ‘verwerking van **relaties** in de basisregistratie’ scoorde Heerhugowaard onder de norm. In het kader van de toetsing van processen scoorde Heerhugowaard voldoende op de inrichting, werking en beveiliging van de basisregistratie. Hierbij werd wel aangegeven dat de gemeente de kwaliteit van de gegevens en de bescherming van de vertrouwelijkheid onvoldoende waarborgt. Ook werden de beveiligingsaspecten op het gebied van personeel als onvoldoende beoordeeld.

[37] Privacybeleid Sociaal Domein Heerhugowaard, Bijlage 1 Convenant met (keten)partners.

[38] BW Raamovereenkomst 2017, BW Verwerkersovereenkomst 2017, WMO Raamovereenkomst 2017, WMO Verwerkersovereenkomst.

[39] BW Raamovereenkomst 2017, BW Verwerkersovereenkomst 2017, WMO Raamovereenkomst 2017, WMO Verwerkersovereenkomst.

3.5 / Incidenten

Procedure beveiligingsincidenten en datalekken behoeft actualisatie

Op 23 december 2015 is de procedure beveiligingsincidenten vastgesteld door het managementteam.[40] Hierin wordt onderscheid gemaakt tussen beveiligingsincidenten en datalekken. Een **beveiligingsincident** is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden zoals tijdelijke onderbreking van bedrijfsactiviteiten, discontinuïteit, reputatieschade en financiële schade. Er is sprake van een **datalek** als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs is uit te sluiten.

De verantwoordelijkheden rondom een beveiligingsincident zijn in de **procedure beveiligingsincidenten** als volgt beschreven:

- Iedere medewerker die direct of indirect kennis draagt of krijgt van een beveiligingsincident, is verplicht dit direct te melden aan de verantwoordelijk manager en/of het CISO team.
- Meldingen van de Informatiebeveiligingsdienst voor gemeenten (IBD) worden beoordeeld en zo nodig ook via de servicedesk geregistreerd.
- De servicedesk zorgt voor routering van het incident via het registratiesysteem.
- Het CISO team bepaalt, in overleg met betrokkenen, wie bij de afhandeling van het incident betrokken moeten worden.
- Het CISO team is verantwoordelijk voor onderzoek en rapportage naar aanleiding van een beveiligingsincident.
- De Privacy Officer is verantwoordelijk voor de advisering van het betrokken management en het bestuur over de mogelijke gevolgen van een beveiligingsincident voor de privacy van de betrokkene.
- De verantwoordelijk manager verleent alle medewerking aan het onderzoek en is verantwoordelijk voor:
    - het ondernemen van preventieve en repressieve beveiligingsacties
    - het al dan niet melden van het incident aan de AP[41]
    - het informeren van de gedupeerde
    - de communicatie met de AP en betrokkenen naar aanleiding van de meldingen.

Deze beschrijving laat goed zien dat de procedure nog geüpdatet moet worden. De gemeente heeft weliswaar privacy officers, maar de CISO is verantwoordelijk voor de afhandeling van een datalek. Meldingen van incidenten bij de AP worden volgens geïnterviewden gedaan door de FG of de CISO, niet door de verantwoordelijk manager.

Beschreven procedure wijkt af van de procedure uit het informatiebeveiligingsbeleid

In het informatiebeveiligingsbeleid, uit 2015, is informatie opgenomen over de afhandeling van een beveiligingsincident. Deze informatie komt niet geheel overeen met de informatie uit de procedure beveiligingsincidenten. In het informatiebeveiligingsbeleid is opgenomen dat niet de verantwoordelijk manager een melding doet bij de AP, maar de informatiebeveiligingsfunctionaris of de FG. Daarbij wordt ook nog verwezen naar het College Bescherming Persoonsgegevens (CBP) in plaats van de AP. De procedure rondom een beveiligingsincident lijkt hiermee aan actualisatie toe. Als de procedure rondom een beveiligingsincident wordt geactualiseerd, kunnen verschillen tussen de twee procedures recht worden getrokken.

Afdelingsmanagers of team privacy en informatieveiligheid eerste aanspreekpunt bij datalek

De afdelingsmanager of leden van het team privacy en informatieveiligheid vormen het eerste aanspreekpunt voor medewerkers die een datalek opmerken.[42] Zij kunnen vervolgens besluiten om contact op te nemen met de wethouder. Dit is niet standaard opgenomen in het protocol, maar uit ervaring blijkt dat dit wel gebeurt. In het nieuwe protocol, dat in de tweede helft van 2018 wordt opgesteld, kan dit mogelijk worden opgenomen.

[40] Procedure beveiligingsincidenten, vastgesteld 23 december 2015.

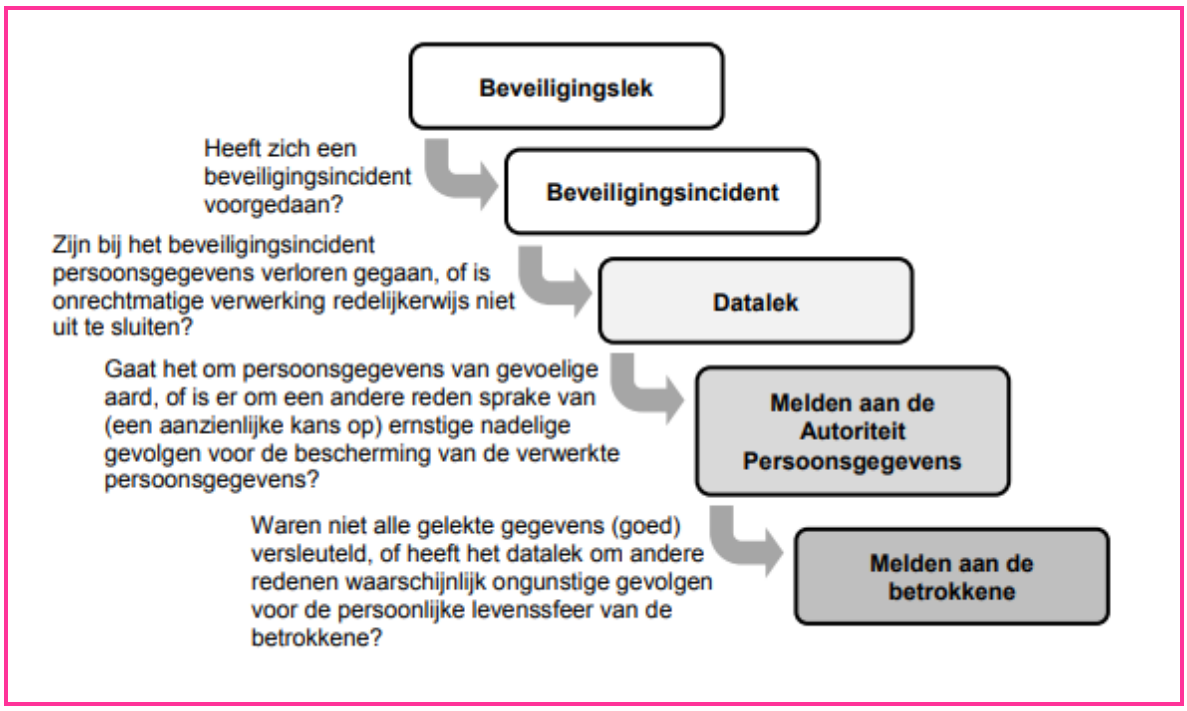
[41] Wordt bedoeld: Autoriteit Persoonsgegevens.

[42] Procedure beveiligingsincidenten.

Afwegingskader voor het melden van incidenten

Voor de afweging of een incident gemeld moet worden of niet, is het volgende hulpschema ingericht door de AP.[43] De gemeente Heerhugowaard gebruikt dit hulpschema aan de hand waarvan medewerkers hun route kunnen bepalen op het moment dat sprake is van een beveiligingslek. Volgens betrokkenen is het hulpschema bij veel medewerkers nog onbekend.

Figuur 3 Hulpschema melden beveiligingsincidenten



Aantal incidenten licht toegenomen sinds 2016

In het kader van dit onderzoek is een overzicht van de beveiligingsincidenten van de afgelopen drie jaar aangeleverd. Hieruit blijkt dat er in 2016 15 incidenten waren, in 2017 20 incidenten en in 2018 tot aan juni 10 incidenten. Niet alle incidenten hoeven gemeld te worden bij de AP; dat is afhankelijk van de aard van het incident. In 2016 zijn er twee incidenten gemeld bij de AP, in 2017 0 en in 2018 tot aan juni, drie.
De gemeente maakt ook inzichtelijk wat de oorzaak van het incident was. Zonder op de individuele aard van incidenten in te gaan kan worden aangegeven of de oorzaak van een incident lag in menselijk handelen, in ICT, in een procedure of extern. Voor de incidenten in 2018 is in het overzicht nog niet aangegeven in welke categorie de oorzaak van het incident lag. Voor de jaren 2016 en 2017 zien die gegevens er als volgt uit:

Oorzaak incident	2016	2017
Menselijk	60%	50%
ICT	20%	30%
Procedure	20%	15%
Extern	-	5%

Voor ieder incident is vervolgens een te nemen maatregel geformuleerd.

[43] De meldplicht datalekken in de Wbp (2015), p.4.

4 Bewustzijn

In dit hoofdstuk wordt ingegaan op bewustzijn omtrent informatieveiligheid en privacy en hoe de gemeente Heerhugowaard dit stimuleert. De verschillende middelen om bewustzijn te creëren en de bijbehorende opleidingsmogelijkheden worden besproken.

De volgende deelvraag staat centraal in dit hoofdstuk:

Bewustzijn

- *Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers in het sociaal domein op het gebied van privacy en informatieveiligheid?*

4.1 / Bewustzijn in de ambtelijke organisatie

Algemeen niveau bewustzijn door medewerkers zelf ervaren als hoog en stijgend, in de praktijk komen kwetsbaarheden naar voren

Over het algemeen ervaren de geïnterviewden dat de mate van bewustzijn hoog is bij medewerkers van de ambtelijke organisatie. Binnen het sociaal domein ziet men vaak dat het bewustzijn van medewerkers ten aanzien van privacy en informatieveiligheid al sterk ontwikkeld is. De wettelijke kaders die binnen het domein gelden en het feit dat medewerkers gewend zijn om met veel gegevens om te gaan, vormt hier de aanleiding voor. De geïnterviewden geven hierover ook aan dat de gemeente professionals met een zorgverleningsachtergrond inhuurt. Deze hebben vanuit hun ervaring en opleiding al een sterk bewustzijn voor informatieveiligheid en privacy ontwikkeld.

Hoewel volgens de geïnterviewden medewerkers binnen het Sociaal Domein zich in grote lijnen bewust zijn van privacy en informatieveiligheid, zijn er voorbeelden van gesprekken waarin medewerkers privacygevoelige gegevens bespreken op ongeschikte locaties. Wanneer medewerkers hierop worden aangesproken komen ze volgens de geïnterviewden snel tot inzicht van de nadelen die deze overleggen met zich meebrengen. Andere kwetsbaarheden worden onder andere gezien in de fysieke werkomgeving van de medewerkers (zie paragraaf 3.2).

Privacy en informatieveiligheid worden niet vaak als apart onderwerp besproken tijdens werkoverleggen. In de afgelopen periode spraken de aanwezigen wel meer over privacy. Dit werd gestimuleerd door de inwerkingtreding van de AVG. De geïnterviewden gaven aan dat het goed zou zijn om het bespreken van privacy en informatieveiligheid periodiek te herhalen om het bewustzijn te vergroten en te behouden.

Beantwoording vragen kost tijd en aandacht van verantwoordelijken

Door het toegenomen aandacht voor het thema privacy krijgen de CISO, de coördinator informatieveiligheid en FG meer vragen. Medewerkers van de ambtelijke organisatie stellen met regelmaat vragen over óf zij informatie mogen delen, en hoe zij dit mogen delen. De geïnterviewden geven aan dat de medewerkers vervolgens handelen naar het gegeven antwoord, ook als dat betekent dat ze bepaalde informatie niet kunnen delen.

Het beantwoorden van deze, extra, vragen met aandacht vraagt veel tijd. Dit heeft gevolgen voor de tijd die de CISO, de coördinator informatieveiligheid en FG aan andere zaken kunnen besteden, bijvoorbeeld het opstellen van nieuw beleid of het houden van toezicht op de naleving van dit beleid.

4.2 / Acties om het bewustzijn van medewerkers te bevorderen

(Risico's van) Menselijk handelen krijgt expliciet de aandacht

In het informatieveiligheidsbeleid van de gemeente Heerhugowaard is aandacht voor menselijke handelen in relatie tot informatieveiligheid en privacy. De ambtelijke organisatie herkent namelijk risico's in menselijk handelen (vergeetachtigheid, emotie, nieuwsgierigheid) en onduidelijkheid over gemaakte afspraken tussen mensen. Om deze reden is de doelstelling dat werknemers, ingehuurd personeel en (externe) gebruikers hun verantwoordelijkheden en de gemaakte afspraken inzake informatiebeveiliging begrijpen en geschikt zijn voor de rollen die zij vervullen.[44]

Om dit te bewerkstelligen speelt de gemeente naast formele maatregelen (VOG's, afleggen van de eed of ondertekenen van verklaring) in op bewustwording. Dit doet de gemeente door algehele communicatie (bijvoorbeeld cursussen of besprekingen per afdeling) en het toepassen van lijnmanagement waardoor de communicatie (ook over informatiebeveiliging) makkelijker verloopt.

Aandacht voor privacy en informatieveiligheid bij indiensttreding

Iedere medewerker tekent bij indiensttreding een verklaring waarin onder andere is opgenomen dat zij op de hoogte zijn van het actuele beleid van de gemeente. Een aandachtspunt hierbij is dat op het gebied van privacy geen gemeentebreed beleid is opgesteld. De afdeling Sociaal Domein heeft op het gebied van privacy wel een eigen beleid.

Privacy en informatieveiligheid krijgen bij het inwerken van nieuwe medewerkers in het sociaal domein niet als zelfstandig thema de aandacht. Voorafgaand aan de aanstelling wordt wel gelet op het bewustzijn van mogelijk nieuwe medewerkers. Jeugdwerkers moeten bijvoorbeeld allemaal een Stichting Kwaliteitsregister Jeugd (SKJ) registratie hebben. Dit betekent dat zij staan ingeschreven bij een landelijke organisatie voor jeugdwerkers en zich conformeren aan de regels en normen van die stichting (vastgelegd in het kwaliteitskader Jeugd). Bij het team WMO is er nog geen landelijke organisatie voor de medewerkers. Er is wel een landelijke beweging om dit van de grond te tillen.

Stimuleren van bewustzijn staat hoog in het vaandel

In het jaarverslag 2017 is opgenomen dat het bewustmaken van het management en de medewerkers van hun verantwoordelijkheid ten aanzien van informatieveiligheid binnen de gemeentelijke organisatie een belangrijke beheersmaatregel voor het bewerkstelligen van een stevig bewustzijn is.[45]

Alle geïnterviewden gaven aan zelf ook actief bezig te zijn met het stimuleren van bewustzijn. Dit geeft aan dat betrokkenen uit verschillende lagen van de gemeente bij het bewustmakingsproces betrokken zijn. De geïnterviewden stelden bovendien dat in het nieuwe beleid naar verwachting meer aandacht wordt geschonken aan het uitdragen van kennis over privacy en informatieveiligheid via bijvoorbeeld trainingen en cursussen. Dit zou vervolgens moeten bijdragen aan het bewustzijn in de ambtelijke organisatie.

[44] Informatieveiligheidsbeleid gemeente Heerhugowaard.

[45] Jaarverslag 2017, paragraaf bedrijfsvoering.

Gemeente Heerhugowaard gebruikt iBewust nieuwsbrief om bewustzijn te creëren

Ter bevordering van het bewustzijn omtrent informatieveiligheid en privacy is de campagne iBewust gevoerd. Deze campagne is op medewerkers gericht. De campagne iBewust houdt in dat er regelmatig updates en/of nieuwtjes worden gedeeld met de medewerkers in de vorm van een speciale nieuwsbrief: iBewust. Iedere editie van deze nieuwsbrief behandelt een thema onderliggend aan informatiebeveiliging. Voorbeelden van thema's die aangestipt worden in de nieuwsbrief zijn: het voorkomen van virussen (editie 5); veilig e-mailen (editie 13); het informatiebeveiligingsbeleid (editie 14) en de invoering van de AVG als nieuwsbericht. Inmiddels zijn er al meer dan 20 iBewust nieuwsbrieven verspreid. De bekendheid van de campagne onder medewerkers wordt niet gemonitord.

Bewustzijn bestuurders en management bijhouden door presentaties en overleg

Het feit dat er in Heerhugowaard bijna 3 fte beschikbaar is voor het bevorderen van privacy en informatieveiligheid toont volgens geïnterviewden aan dat het college van Heerhugowaard het belang van de thema's ziet.

Aangezien de iBewust campagne en de bijbehorende nieuwsbrief met name zijn gericht op medewerkers van de ambtelijke organisatie, worden de collegeleden en leden van het managementteam ook via alternatieve manieren bewustgemaakt van privacy en informatieveiligheid. De CISO heeft een gesprek gehad met het management en het college over informatieveiligheid en privacy in hun werkzaamheden, waarbij ook de AVG aan bod kwam. Deze presentatie volgde op een reeks presentaties over de meldplicht datalekken. Daarnaast is er, zoals eerder vermeld, maandelijks overleg tussen de CISO en de gemeentesecretaris en tussen de CISO en portefeuillehouder.

4.3 / Opleiding

BYOD en cursus *Veilig Digitaal Werken*

De gemeente Heerhugowaard verplicht medewerkers om hun eigen device mee te brengen; *Bring Your Own Device (BYOD)*. Medewerkers kunnen een vergoeding krijgen voor het aanschaffen van een eigen device waarop hij of zij bij de gemeente kan werken.

Alvorens medewerkers in aanmerking komen voor een vergoeding voor het device wat is aangeschaft in het kader van BYOD, moeten medewerkers eerst een cursus *Veilig Digitaal Werken* afronden. De ambtelijke organisatie biedt deze cursus aan al haar medewerkers aan. In het kader van informatiebeveiliging moet de cursus worden afgerond vóór een medeweker een vergoeding krijgt voor het aanschaffen van een device waar hij of zij kan werken. Dit geldt voor alle medewerkers; van stagiairs tot wethouders.

De cursus behandelt met name hoe medewerkers met gegevens om kunnen gaan die op verschillende locaties, op verschillende devices en in verschillende vormen bewaard worden, de gevaren die daarbij komen kijken en het bewust handelen in die omstandigheden.[46] Thema's die worden besproken in de cursus zijn bijvoorbeeld wachtwoorden, virussen, openbare Wifi, e-mail en social media.[47] De cursus *Veilig Digitaal Werken* wordt afgerond door middel van een meerkeuze-examen.[48]

E-learning module over privacy en informatieveiligheid

De gemeente Heerhugowaard is bezig met het instellen van een bewustwordingsprogramma, o.a. via E-learning. Dit leerprogramma gaat uitgebreid in op privacy en informatieveiligheid. De geïnterviewden geven aan dat het leerprogramma, in de huidige planning, cyclisch over meerdere jaren wordt uitgevoerd. De start van het traject staat gepland voor het najaar van 2018. De gemeentesecretaris en portefeuillehouder zijn akkoord met uitvoeren van een bewustwordingsprogramma. Het MT is over het programma geïnformeerd en zal betrokken worden bij de uitvoering.

[46] Theorie BYOD 2

[47] Theorie BYOD 2

[48] Toetsvragen BYOD 2

Gepland is om het programma na afronding te evalueren te evalueren. Er is daarom voorafgaand aan de training een nulmeting, gevolgd door de training en tenslotte een effectmeting. De resultaten van deze evaluatie worden meegenomen in de vaste P&C-cyclus.

Bijlage I - Bronnen

Documenten

Op basis van een informatie-uitvraag heeft de gemeente Heerhugowaard het volgende bronmateriaal aangeleverd:[49]

/ B&W besluit buurtgericht Sociaalplein
/ Basisgroepindeling dienstverlening Sociaal Domein
/ Beschermd Wonen Bewerkersovereenkomst 2017
/ Beschermd Wonen Raamovereenkomst 2017
/ Cursus BYOD Theorie
/ Cursus BYOD Toetsvragen
/ Format Verwerkersovereenkomst HHW
/ Governance Heerhugowaard concept – 21 november 2017
/ Handreiking Toegang en Declaratie 2018 v1
/ iBewust in Heerhugowaard (delen 4 tot en met 21, delen 15 en 19 uitgezonderd)
/ iBewust nieuwsbericht: De AVG geldt
/ Informatieveiligheidsbeleid Heerhugowaard
/ Jaarrekening Heerhugowaard 2017 - paragraaf bedrijfsvoering
/ Organigram uitvoering Sociaal Domein
/ Overzicht beveiligingsincidenten
/ Procedure beveiligingsincidenten
/ Rapportage zelfevaluatie BRP
/ Register van gegevensverwerking HHW: Bestuur
/ Register van gegevensverwerking HHW: Generiek
/ Register van gegevensverwerking HHW: Ondersteuning
/ Register van gegevensverwerking HHW: Publieksdiensten
/ Register van gegevensverwerking HHW: Ruimtelijk Domein
/ Register van gegevensverwerking HHW: Sociaal Domein
/ Werkdocument het Sociaalplein
/ Wijzigingsbeheer
/ WMO Bewerkersovereenkomst 2017
/ WMO Raamovereenkomst 2017

[49] Dit zijn de namen zoals aan de documenten gekoppeld tijdens aanlevering bij de onderzoekers. De namen zijn alleen aangepast of aangevuld indien onderzoekers opheldering nodig achtten.

Open Bronnen

Ter verdieping van het onderzoek zijn er aanvullende gegevens gebruikt uit de volgende open bronnen en documenten:

/ Website gemeente Heerhugowaard (https://www.heerhugowaard.nl/inwoners-en-ondernemers/)
/ Website van Nederlandse Gemeenten (https://vng.nl/)
/ Website IBD (https://www.informatiebeveiligingsdienst.nl/)
/ Tactische Baseline Informatiebeveiliging Nederlandse gemeenten – V.1.02
/ Strategische Baseline Informatiebeveiliging Nederlandse gemeenten – V.1.02

Gesprekspartners

Ter verdieping van dit onderzoek zijn drie gesprekken gehouden. De gespreksverslagen van deze interviews zijn ter verificatie aan de gesprekspartners voorgelegd en geaccordeerd. De verslagen dienen als achtergrondinformatie voor de Nota van bevindingen.

Datum	Naam	Functie
5 juli 2018	de heer T. Quist	CISO en Privacy Officer
5 juli 2018	de heer A. Lensen	FG
5 juli 2018	de heer P. Korremans	FG (ad interim)
12 juli 2018	de heer J. Does	Wethouder (o.a. portefeuilles Jeugdhulp en Onderwijs)
12 juli 2018	de heer J. van der Sarre	Wethouder (o.a. portefeuilles WMO en Zorg & Gezondheid)
12 juli 2018	mevrouw P. van Dooijeweerd	Coördinator WMO consulenten en gezinscoaches
12 juli 2018	mevrouw M. Smith	Kwaliteitsadviseur bij team Jeugd

Bijlage II – Begrippen- en verklaringenlijst

AP – Autoriteit Persoonsgegevens (tot 1 januari 2016 College bescherming persoonsgegevens). De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

AVG – Algemene Verordening Gegevensbescherming: een Europese verordening (dus met rechtstreekse werking) die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.

BAG – Basisregistratie Adressen en Gebouwen.

BIG – Baseline Informatiebeveiliging Nederlandse Gemeenten; gemeentelijke basisnormenkader voor informatieveiligheid.

BRP – Basisregistratie personen.

CBP – College Bescherming Persoonsgegevens.

CISO – Chief Information Security Officer; specialist op het gebied van de Informatie Beveiligingsfunctie, genoemd in de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

DigiD - Een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren.

ENSIA – Eenduidige Normatiek Single Information Audit: Systematiek voor verantwoording over informatieveiligheid. Het proces bestaat uit een voorbereiding, zelfevaluatie, horizontale verantwoording, verticale verantwoording en een evaluatie.

FG – Functionaris voor de Gegevensbescherming. Functionaris die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG).

GBA – Gemeentelijke basisadministratie persoonsgegevens.

IBD – Informatiebeveiligingsdienst voor gemeenten.

IBF – Informatie Beveiligingsfunctionaris.

P&C Cyclus - Cyclus van planning en control.

PIA – Privacy Impact Assessment: Een instrument waarmee de risico's op het gebied van privacy in kaart kunnen worden gebracht.

SSO - Single Sign On: eenmalige inlog waarna automatisch toegang wordt verschaft tot meerdere applicaties.

Suwinet – Registratiesysteem; systeem van informatie-uitwisseling in de keten van werk en inkomen. Uitvloeisel van de Wet structuur uitvoeringsorganisatie werk en inkomen.

Suwi – Wet Structuur uitvoeringsorganisatie werk en inkomen.

Register van gegevensverwerking - Het register van gegevensverwerking bevat informatie over de persoonsgegevens die worden verwerkt. Het vervangt de bestaande verplichting uit de Wet bescherming persoonsgegevens om gegevensverwerkingen bij de Autoriteit Persoonsgegevens te melden.

RMC – Regionale Meld- en Coördinatiefunctie Voortijdig Schoolverlaten.

VNG – Vereniging van Nederlandse Gemeenten.

Wbp – Wet bescherming persoonsgegevens. Deze wet is na de invoering van de Algemene Verordening Gegevensbescherming op 25 mei 2018 niet meer van toepassing.

Whitelisten – Het opstellen van een lijst met IP-adressen of servers waarvan email altijd wordt geaccepteerd. In het geval van Suwinet betreft dit het (dagelijkst) vaststellen van een lijst burgerservicenummers die in Suwinet door medewerkers van de gemeente Heerhugowaard geraadpleegd mogen worden

WMO – Wet maatschappelijke ondersteuning; Gemeenten moeten ervoor zorgen dat mensen zo lang mogelijk thuis kunnen blijven wonen. De gemeente geeft ondersteuning thuis via de Wmo. Officieel heet deze wet Wmo 2015.