Rapportage
Interne toetsing AVG 2018

Aan het College van burgemeester en wethouders
Gemeente Doetinchem
15 januari 2019

Verslagperiode juni – december 2018
Uitgevoerd door Anne-Marie Nas (FG)

Inleiding

Sinds 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Deze verordening zorgt ervoor dat in de hele EU dezelfde privacywetgeving geldt.

De AVG stelt nieuwe eisen aan het omgaan met en het verwerken van persoonsgegevens. Bestaande rechten en plichten van een betrokkene zijn uitgebreid.

Binnen de gemeente Doetinchem wordt veel gewerkt met persoonsgegevens van betrokkenen. Dit zijn persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke (wettelijke) taken. Het is belangrijk dat de burger erop kan vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

De AVG legt de verantwoordelijkheid bij uzelf om aantoonbaar te maken dat uw organisatie voldoet aan de privacyregels. Hiervoor is het belangrijk dat iedereen in de organisatie deze noodzaak voelt en hierin zelf een eigen verantwoordelijkheid neemt.

Om dit te bereiken is de bewustwording bij medewerkers een randvoorwaarde. Zonder bewuste medewerkers lukt het niet om privacyproof te werken. Door dit goed op te pakken leveren we met elkaar een belangrijke bijdrage aan de bescherming van het grondrecht op privacy.

Deze rapportage is bedoeld om u als college van B&W in mijn rol als functionaris gegevensbescherming (FG) te informeren en advies te geven. Door middel van deze interne toetsing krijgt u een beeld in hoeverre de AVG binnen uw organisatie wordt nageleefd.

Leeswijzer
Deze rapportage begint met een samenvatting gevolgd door de conclusies en aanbevelingen. Daarna wordt uiteengezet op welke wijze de interne toetsing is uitgevoerd. Gevolgd door hoofdstuk 3 waarin de borging van privacy organisatie is beschreven. In hoofdstuk 4 leest u over de bewustwording, een randvoorwaarde om als organisatie privacyproof te zijn. Hoofdstuk 5 is een uiteenzetting van de nakoming van de verplichting uit de AVG die goed aantoonbaar zijn. Tot slot hoofdstuk 6 waarin twee specifieke verplichtingen uit de AVG aan de orde komen.

Samenvatting
De gemeente Doetinchem verwerkt veel persoonsgegevens. Dit zijn persoonsgegevens van burgers, medewerkers en (keten)partners. In de huidige digitale en datagedreven samenleving zijn persoonsgegevens erg waardevol. Daarom is het belangrijk zorgvuldig om te gaan met de persoonsgegevens waarvoor de gemeente verantwoordelijk is.

De Algemene verordening gegevensbescherming (AVG) geeft de regels die gelden op het gebied van de privacy. In dit eerste rapport ligt de focus op het vergroten van de bewustwording, de naleving van de verantwoordingsplicht en de verplichte aanwezigheid van de FG. Deze 3 hoofdonderwerpen zijn vertaald naar de onderstaande 10 vragen.

- Heeft de organisatie een FG aangesteld en aangemeld;
- Zijn de contactgegevens van de FG bekend gemaakt op de eigen website;
- Is er een verwerkingsregister aanwezig en staan hierin de juiste onderwerpen;
- Kunnen de betrokkenen hun rechten uitoefenen (en is dit goed toegankelijk);
- Bewustwording, is hier expliciet aandacht aan besteed;
- Is er een incidenten/datalek register en wat is met de incidenten gedaan;
- Zijn er verwerkersovereenkomsten gesloten;
- Is er privacybeleid vastgesteld;
- Is er een DPIA uitgevoerd;
- Is er een privacyverklaring en staan hierin de juiste onderwerpen.

Op 7 januari 2019 heb ik als FG een interne toets uitgevoerd. Hiervoor is de privacy coördinator geïnterviewd. Met behulp van de 10 vragen wordt zichtbaar in hoeverre de gemeente Doetinchem haar verantwoordelijkheid neemt (zie hoofdstuk 2).

De bewustwording wordt gezien als het belangrijkste onderwerp om de organisatie privacyproof te krijgen. Hier is binnen de organisatie veel tijd aan besteed. Om de privacy te waarborgen is het van belang blijvend in te zetten op de bewustwording (zie hoofdstuk 4).

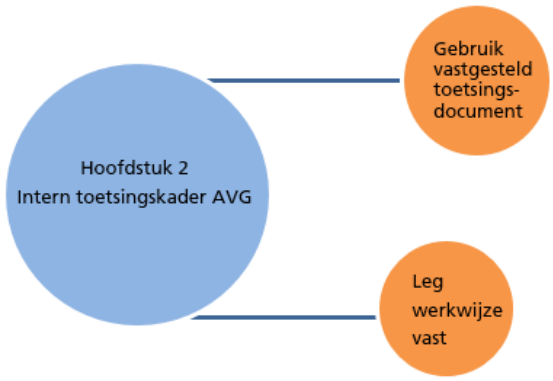
De privacy is organisatorisch geborgd door het inrichten van de ‘virtuele’ privacy organisatie. In de ‘virtuele’ privacy organisatie worden de taken, rollen en verantwoordelijkheden bij medewerkers belegd. Dit is gedaan op strategisch, tactisch en operationeel niveau. Om kennis breder te delen en van elkaar te leren werkt de gemeente Doetinchem op dit thema samen met de gemeente Aalten, Doesburg, Oost-Gelre, Oude-IJsseltreek en met ODA, Buha en Buurtplein (zie hoofdstuk 3).

Uit de toets blijkt dat aan alle elementen uit de AVG die goed zijn aan te tonen is voldaan. Zo werkt de gemeente met een register van verwerkingen, een register van incidenten/datalekken en sluit zij verwerkersovereenkomsten. Ook is er een FG aangesteld en aangemeld bij de externe toezichthouder. Dit is de Autoriteit Persoonsgegevens. Verder is er op de website een privacyverklaring gepubliceerd. Op sommige onderdelen zijn kleine verbeteringen nodig om volledig aan de wettelijke verplichting te voldoen. Ook is het belangrijk goed na te gaan hoe de registers actueel kunnen blijven (zie hoofdstuk 1 en hoofdstuk 5).

Tenslotte zijn er twee andere onderwerpen uit de AVG belicht. De rechten van betrokkenen en de gegevensbeschermingseffectbeoordeling. Dit wordt meestal de DPIA (data protection impact assessment) genoemd. Beide onderwerpen zijn ‘ingericht’ maar verdere professionalisering van de bestaande werkwijze/processen is aan te bevelen (zie hoofdstuk 1 en 6).

Hoofdstuk 1 – Conclusies en aanbevelingen
Per hoofdstuk worden hieronder de conclusies - en indien aanwezig mogelijke aanbevelingen – per onderwerp gedaan. De aanbeveling om de privacy verder te verbeteren staat cursief weergegeven. Elke aanbeveling is voorzien van een kleur om de prioriteit aan te geven.

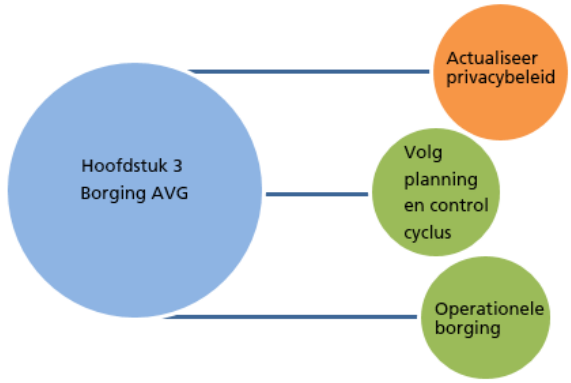
Op dit moment voldoende (groen)
Benodigd verbetering op (korte) termijn (oranje)
Urgente verbetering vereist (rood)



Op dit moment is er door de branche organisatie of de Autoriteit Persoonsgegevens (de externe toezichthouder) nog geen vastgesteld toetsingskader beschikbaar gesteld. Daarom is gewerkt met een door de FG zelf samengestelde vragenlijst.

- *Zodra er een vastgesteld toetsingsdocument beschikbaar wordt gesteld, dit toetsingsdocument volgen. Zo ontstaat meer eenduidigheid. Indien kan worden gekozen voor meerdere vastgestelde of goede toetsingsdocumenten bij voorkeur aansluiten bij een toetsingskader dat qua opzet aansluit bij andere audits (denk aan de High level structure bij ISO of de generieke en specifieke normenkaders bij informatieveiligheid).*

- *Leg de werkwijze waarop de interne toetsing wordt uitgevoerd vast in een procedure binnen de eigen organisatie (zie bijlage 1). Hierdoor zijn de verbeteringen ten opzichte van voorgaande jaren goed zichtbaar en meetbaar.*



Op dit moment is er privacybeleid, vastgesteld in 2017. Op het gebied van privacy wordt samengewerkt met 7 andere organisaties. Door de deelnemers zonder privacybeleid is de wens uitgesproken in 2019 beleid op te stellen.

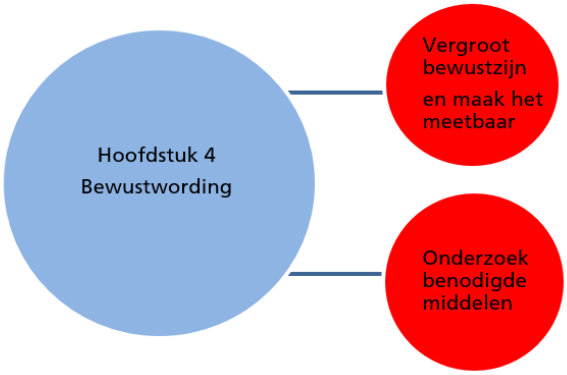
- *Om de kaders goed in beeld te hebben en houden is het aan te bevelen om het privacybeleid uit 2017 te actualiseren. Ga hierbij na of er verbinding kan worden gelegd met het informatie(be)veiligheidsbeleid en het informatiebeleid. Onderzoek - indien de organisatie hier klaar voor is - of privacy een pijler kan zijn van de governance, risk en compliance binnen de organisatie.*

De interne toetsing AVG is apart van andere toetsingen binnen de organisatie uitgevoerd.

- *Laat de interne toetsing AVG onderdeel zijn van de reeds bestaande toetsingsmomenten in de organisatie. Borg de interne AVG toets in de bestaande planning- en control cyclus.*

De operationele borging van de virtuele privacy organisatie gaat over de privacy beheerder. Deze rol is vaak belegd bij de functioneel applicatiebeheerder. De invulling van de operationele borging is in dit eerste toetsingsjaar niet besproken.

- *De operationele borging in de 'virtuele' privacy organisatie meer aandacht geven en indien nodig hier de rollen, taken en verantwoordelijkheden beleggen.*

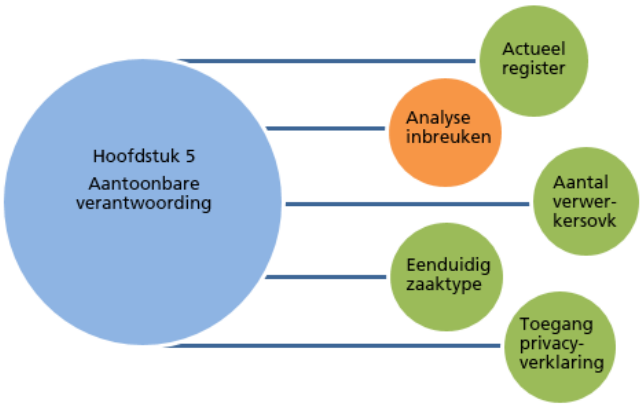


De bewustwording is een randvoorwaarde voor een organisatie die privacyproof wil zijn. Het is belangrijk dat de gemeente en haar medewerkers de noodzaak voelen en zelf hun verantwoordelijkheid nemen om zorgvuldig met persoonsgegevens om te gaan. Bewustwording is een blijvende activiteit.

- *Zorg ervoor dat het bewustzijn bij de medewerkers in ieder geval gelijk blijft maar bij voorkeur omhoog gaat. Om te meten of het bewustzijnsniveau omhoog is gegaan is het goed vooraf te bepalen hoe dit wordt gemeten. Om het levend te houden neem de privacy op in beleid en jaarplannen. Beoordeel bij het aantrekken van nieuwe medewerkers of zij beschikken over de vaardigheden om het gewenste gedrag te vertonen.*

Door de raad en het college zijn geen financiële middelen begroot om de bewustwording bij de medewerkers verder te vergroten.

- *Onderzoek hoeveel middelen er nodig zijn om de bewustwording bij medewerkers in ieder geval van vergelijkbaar niveau te houden en bij voorkeur te vergroten.*



De coördinatie van het register van verwerkingen ligt nu bij de privacy coördinator. Het register is voor iedereen beschikbaar op SharePoint. De integraal leidinggevende is zelf verantwoordelijk het register actueel te houden.

- *Een register actueel houden is lastig. Denk na hoe de organisatie volgt dat het register actueel blijft. Mogelijk kan het register worden gekoppeld aan een reeds bestaande (GEMMA) structuur en ga door met het vergroten van de privacy.*

Om te kunnen leren van inbreuken is een analyse van inbreuken belangrijk.

- *Denk na over een verbetering van het bestaande systeem om de inbreuken en datalekken eenvoudig te analyseren. Zo kan met 1 muisklik worden achterhaald hoeveel inbreuken een datalek zijn. Wat de aard is en hoeveel datalekken aan betrokkenen zijn gemeld.*

Bij een deel van de hoofdovereenkomsten die door de gemeente wordt gesloten is de afdeling contractmanagement/inkoop betrokken. Zij gaan dan na of een verwerkersovereenkomst nodig is. Het is niet zichtbaar of alle benodigde verwerkersovereenkomsten zijn afgesloten.

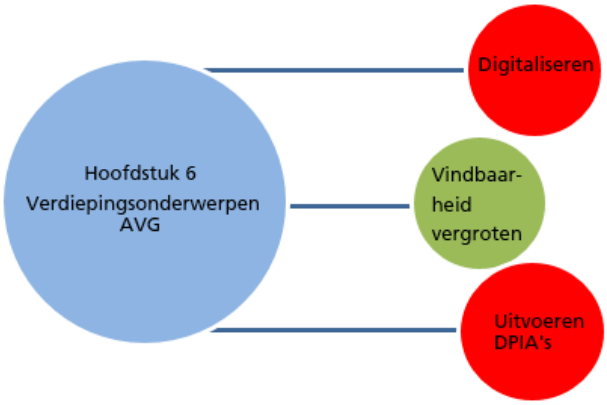
- *Nagaan of het mogelijk is de zichtbaarheid te vergroten waardoor kan worden aangetoond dat het juiste aantal verwerkersovereenkomsten is afgesloten. Denk na over de mogelijkheid om alle hoofdovereenkomsten via de afdeling contractmanagement/inkoop te laten lopen.*

De verwerkersovereenkomsten worden opgeslagen in het zaaksysteem. Hiervoor worden verschillende zaaktypen gehanteerd.

- *Hanteer een eenduidig zaaktype om dit document op te slaan in het zaaksysteem.*

De privacyverklaring is opgenomen op de website. De verklaring is niet in 1 muisklik te vinden. De toegankelijkheid is hiermee gewaardeerd op redelijk toegankelijk. De bronnen van de verkregen persoonsgegevens zijn niet opgenomen.

- *Maak de privacyverklaring beter toegankelijk op de website. Om de bronnen van de verkregen persoonsgegevens inzichtelijk te maken kan het verwerkingsregister op de website worden gepubliceerd.*



Een betrokkene die zijn of haar rechten wil uitoefenen kan naar het gemeentehuis komen om zich te legitimeren. Er bestaat ook de mogelijkheid om een gewaarmerkte kopie ID op te sturen. Er bestaat op dit moment geen volledige digitale toegang om rechten uit te oefenen.

- *De toegankelijkheid om voor de betrokkene zijn of haar rechten uit te oefenen verder uitbreiden door te werken met digitale mogelijkheden. Denk bijvoorbeeld aan de mogelijkheid om in te loggen met DigiD.*

- *De uitoefening van rechten door betrokkenen betekent voor de medewerkers extra (uitzoek)werk. In welke systemen zijn de persoonsgegevens 'verwerkt'. Denk bij het inrichten van systemen na over de vindbaarheid.*

Bij de gemeente Doetinchem is 2x een DPIA uitgevoerd. Onduidelijk is of er niet meer processen voorbij zijn gekomen waarbij dit wettelijk verplicht is. Mogelijk is de onbekendheid van het uitvoeren van de DPIA hier de oorzaak van.

- *Maak de medewerkers bewust over het uitvoeren van een DPIA. Op die manier zullen meer processen – zo vroeg mogelijk - zichtbaar worden waarbij het uitvoeren van een DPIA verplicht is gesteld. Neem het uitvoeren van een DPIA op in bestaande processen zodat over de uitvoering wordt nagedacht. Betrek de afdeling contactmanagement/inkoop hierbij.*

Hoofdstuk 2 – Intern toetsingskader AVG
Op dit moment is er geen vastgesteld AVG toetsingsdocument beschikbaar. Zowel de branche als de toezichthoudende autoriteit (Autoriteit Persoonsgegevens) bieden dit nog niet aan. Om de toetsing voor 2018 wel uit te kunnen voeren is eerst bepaald welke onderwerpen uit de AVG inhoudelijk het meest relevant zijn en daardoor voor toetsing in aanmerking komen. Tijdens het gezamenlijke privacy overleg op 21 augustus 2018 met de andere gemeenten en daaraan gelieerde organisaties is een top 5 van onderwerpen opgesteld. Dit is aangevuld met 5 onderwerpen uit het document 'AVG 10 stappenplan' uitgebracht door de Autoriteit Persoonsgegevens. Zo is een vragenlijst van 10 vragen opgesteld.

Deze 10 onderwerpen zijn in de vorm van een interview door de FG voorgelegd aan de privacy coördinator. De privacy coördinator heeft de vragen beantwoord en betrekt hierbij andere collega's.

Bij het opstellen van deze rapportage is deels aansluiting gezocht bij het Privacy Control Framework van NOREA (Nederlandse Vereniging van erkende IT-auditors) en voor zover mogelijk bij het document 'Borging AVG' van december 2018 opgesteld door VNG Realisatie en de Informatiebeveiligingsdienst (IBD).

Procedure
Om de interne toetsing jaarlijks op vergelijkbare wijze uit te voeren is beschreven welke werkwijze is gevolgd. Deze werkwijze is opgenomen in bijlage 1. Deze werkwijze kan door de organisatie worden vastgelegd.

Hoofdstuk 3 – Borging AVG
In dit hoofdstuk staat de voortgang ten aanzien van de borging van privacy binnen de gemeente centraal. Hierbij wordt onderscheid gemaakt in strategisch, tactisch en operationeel niveau.

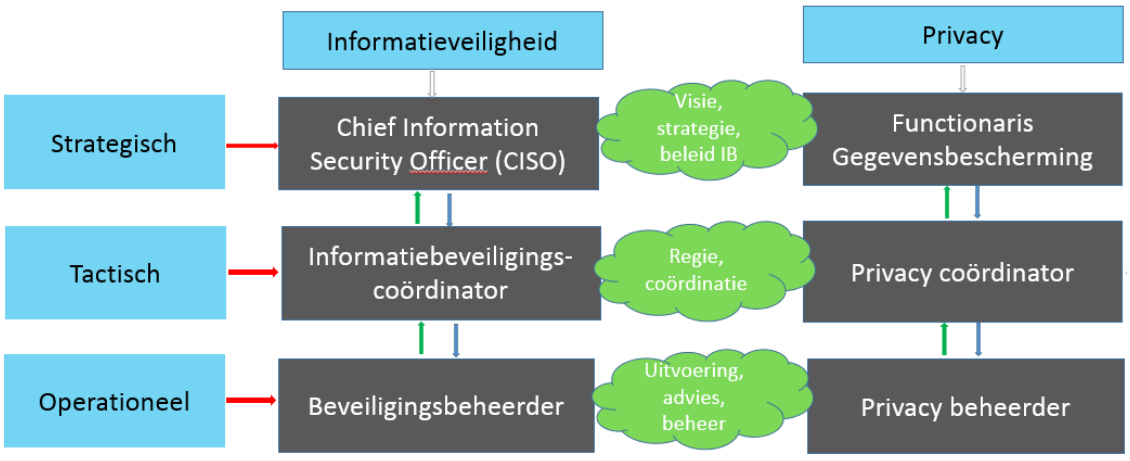
Strategie en beleid
De AVG stelt (deels) nieuwe eisen aan het omgaan met en het verwerken van persoonsgegevens. Bestaande rechten en plichten van een betrokkene, maar ook van de verwerkingsverantwoordelijke zijn uitgebreid. De gemeente heeft de taak de AVG juist te implementeren in de bedrijfsvoering.

Het privacybeleid is een kader waarin wordt aangegeven aan welke principes de gemeente zich houdt, het laat zien hoe de gemeente met persoonsgegevens omgaat en welke maatregelen de gemeente treft om te voldoen aan de bestaande wet- en regelgeving.

Op dit moment is er privacybeleid, vastgesteld in 2017. Op het gebied van privacy wordt samengewerkt met 7 andere organisaties. Door de deelnemers zonder privacybeleid is de wens uitgesproken in 2019 beleid op te stellen. Voor de gemeente Doetinchem betekent dit mogelijk een actualisatie van het bestaande beleid.

Tactische borging
Op tactisch niveau is er aandacht voor de inrichting van de privacy organisatie, de inzet van medewerkers en de toewijzing van benodigde middelen.

Om privacy goed in de organisatie in te bedden wordt gewerkt op basis van een 'virtuele' privacy organisatie (zie figuur 1). Hier is ook de onderverdeling gemaakt tussen strategisch, tactisch en operationeel niveau. Gekoppeld aan de functies/rollen die hierin een verantwoordelijkheid hebben.



Figuur 1 – 'Virtuele' privacy organisatie

De privacy coördinator werkt binnen de eigen organisatie en coördineert de privacy onderwerpen die relevant zijn. De privacy coördinator verbindt de strategische onderwerpen met de onderwerpen die op operationeel niveau spelen.
Hiervoor sluit de privacy coördinator aan bij het overleg dat door de FG wordt georganiseerd. De FG werkt voor 7 andere organisaties en nodigt alle privacy coördinatoren elke maand uit voor een gezamenlijk privacy overleg.

Zo wordt de privacy kennis breder gedeeld en kunnen de privacy coördinatoren van elkaar leren. Aan de privacy samenwerking nemen de gemeente Aalten, Doesburg, Oost-Gelre, Oude-IJsseltreek, ODA, Buha en Buurtplein deel.

Inzet van medewerkers
Voor een goede en juiste uitvoering is het van belang dat medewerkers binnen de organisatie op de hoogte zijn van de beginselen van de AVG en het belang inzien van privacy.

Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden. Daarnaast is het belangrijk dat het voor medewerkers duidelijk is bij wie zij terecht kunnen bij vragen over gegevensbescherming of de uitvoering en interpretatie van de wet- en regelgeving.

Toewijzen van middelen
De gemeente Doetinchem heeft voor een goede inbedding van de privacy in de eigen organisatie een coördinator informatiebeveiliging/privacy in dienst voor 36 uur per week.

Operationele borging
De operationele borging van de 'virtuele' privacy organisatie gaat over de privacy beheerder. Vaak een rol die wordt belegd bij de functioneel applicatiebeheerder.

De invulling van de operationele borging is in dit eerste toetsingsjaar niet besproken.

Hoofdstuk 4 – Bewustwording

Bewustwording! Misschien wel het belangrijkste onderwerp als het gaat om privacy. Ook al is de 'virtuele' privacy organisatie ingericht, zonder de medewerkers lukt het niet om de organisatie privacyproof te krijgen. Qua inrichting en op papier is de privacy dan mogelijk op orde, zolang medewerkers niet weten hoe te handelen is een datalek zo gemaakt. Bewuste medewerkers kunnen meehelpen de privacy van de burger, de klant en henzelf te beschermen en 'vervelende' krantenkoppen te voorkomen.

Figuur 2 - Krantenkoppen

Vergroten van bewustwording

De bewustwording is een randvoorwaarde voor een organisatie die privacyproof wil zijn. Het is belangrijk dat de gemeente en haar medewerkers de noodzaak voelen en zelf hun verantwoordelijkheid nemen.

Door de raad en het college zijn geen financiële middelen begroot om de bewustwording verder te vergroten. Wel is privacy opgenomen als onderdeel van de begroting. Binnen de samenwerking wordt de bewustwording in 2019 vergroot door middel van e-learning, apps, fysieke veiligheid, security en privacy.

Bewustwording wordt binnen de gemeente Doetinchem gezien als een doorlopende activiteit. Er wordt blijvend ingezet op bewustwording bij medewerkers op het gebied van privacy. Door aandacht te blijven hebben voor bewustwording zal het bewustwordingsniveau in ieder geval gelijk blijven aan het bestaande niveau.

Wat is er aan bewustwording gedaan

In 2018 is aandacht besteed aan het vergroten van de bewustwording bij medewerkers. Hieronder is opgesomd wat er is gedaan om de bewustwording te vergroten.

Wat	Wie	Wanneer
Intranetpagina privacy	Alle medewerkers	februari
Presentatie AVG	Afdelingshoofden	maart
Presentatie AVG	Klankbordoverleg Jeugdbeschermingstafel	maart
Presentatie AVG met verbinding met informatiebeveiliging	Functioneel applicatiebeheerders	april (3x)
Toelichting AVG sociaal domein	Sociale Raad	april
Uitleg gevolgen AVG	Team Financiële Administratie	april
Diverse berichten op intranet	Alle medewerkers	april en mei
Posters op koffiezetapparaten	Alle medewerkers	mei
Toelichting AVG sociaal domein	Zorgplein, Maatschappij, Bedrijfsvoering en Buurtplein	mei
Informatiebijeenkomsten AVG	Alle medewerkers	mei (3x)
Kruiswoordpuzzel AVG en banner	Alle medewerker werkcafé	mei
AVG en Meedoen arrangement	Medewerkers maatschappij	juni
AVG en Statushouders	Medewerkers maatschappij en Sité Woondiensten	juli
AVG en communicatie	Medewerkers communicatie	augustus
Flyer Eerste hulp bij Privacy	Alle medewerkers	september
Bijpraten Ondernemingsraad AVG	OR	september
AVG en digitaal kladblok Omgevingswet	Betrokkenen	oktober
AVG en Gehandicaptenparkeerkaart	Medewerkers gemeentewinkel	oktober
AVG en Leren Werkt	Leren Werkt afdeling maatschappij	oktober
AVG en persoonsgebonden overgangsrecht	Medewerkers afdeling ruimte	november
AVG en postregistratie/archivering	Medewerkers documentaire informatie	november
AVG en leerlingenvervoer	Medewerkers bedrijfsvoering	december
Zaaksysteem en AVG	Coördinatoren, teamleider en FG	maandelijks
Onderdeel van het beoordelingsgesprek	Alle medewerkers	Q4

Hoofdstuk 5 - Aantoonbare verantwoording
In dit hoofdstuk staat de operationele uitvoering van de AVG centraal. Bij een aantal onderwerpen uit de AVG is goed aan te tonen of de organisatie voldoet aan de AVG.

Dit geldt voor het register van verwerkingen, het register van beveiligingsincidenten/datalekken, de verwerkersovereenkomsten, het aanstellen van de FG en de privacyverklaring.

Hieronder wordt per onderdeel toegelicht in hoeverre aan deze waarborgen wordt voldaan.

Register van verwerkingen
De gemeente heeft taken waarvoor zij persoonsgegevens gebruikt. In het register van verwerkingen wordt vastgelegd hoe deze gegevens worden 'verwerkt'. In het register kan worden opgezocht welke persoonsgegevens voor welk doel worden gebruikt.

De gemeente Doetinchem heeft een verwerkingsregister opgesteld. Het register is toegankelijk voor alle medewerkers. Het register is te vinden via het intranet onder kennisplein en vervolgens het kopje privacy. In figuur 3 is te zien of aan alle wettelijke eisen is voldaan.

Register van verwerkingen	Aanwezigheid
Naam verwerkingsverantwoordelijke	nee
Contactgegevens verwerkingsverantwoordelijke	nee
Naam FG	nee, wel in privacy verklaring
Contactgegevens FG	nee, wel in privacy verklaring
Doel van verwerking	ja
Categorie van betrokkenen	ja
Categorie van persoonsgegevens	ja
Bewaartermijn	ja
Beveiligingsmaatregelen	nee, wel vastgesteld informatiebeveiligingsbeleid

Figuur 3 – Register van verwerkingen

Van de 500 beschreven processen zijn op dit moment 155 hoofdprocessen opgenomen in het register. Elke leidinggevende is integraal verantwoordelijk voor het actueel houden van het register. Het register kan worden bijgewerkt in SharePoint. De privacy coördinator heeft hierin een coördinerende rol en wijst medewerkers op het bestaan van dit register.

In 2019 wordt verder nagedacht over het actueel houden van het register. Mogelijk kan het register worden gekoppeld aan een reeds bestaande (GEMMA) structuur en medewerkers nog bewuster te maken. Zodat aan de 'voorkant' wordt nagedacht over dit onderwerp.

Beveiligingsinbreuk en datalekken
Een mail met (bijzondere) persoonsgegevens versturen naar een onjuist mailadres kan elke medewerker gebeuren. We communiceren door middel van diverse apparaten en via verschillende kanalen. Wat doe je als dit gebeurt? Kun je aantonen welke maatregelen je als organisatie hebt genomen zodat je zorgvuldig omgaat met persoonsgegevens.

Ieder datalek is een beveiligingsinbreuk in de zin van de AVG. Bij een datalek moet er sprake zijn van een daadwerkelijk lek van persoonsgegevens. Soms is er enkel een tekortkoming in de beveiliging, bijvoorbeeld wanneer de software niet up-to-date is. Dan is er sprake van een beveiligingslek, maar niet van een datalek.

Een datalek ontstaat als persoonsgegevens terechtkomen op een plek waar deze niet horen te zijn, vaak veroorzaakt door menselijke handelen.

De landelijke top 3 bestaat uit de onderstaande oorzaken:
- E-mailbericht verzonden aan een onjuist persoon;
- Verkeerd geadresseerde envelop of onjuiste bijlage;
- Verloren apparaat (mobiele telefoon of laptop).

De gemeente Doetinchem heeft 5 datalekken gemeld bij de externe toezichthouder.
Een datalek hoeft alleen te worden gemeld bij de externe toezichthouder als dit leidt tot een risico voor de rechten en vrijheden van betrokkenen (degene van wie de persoonsgegevens zijn). De specificatie hiervan is als volgt:
- 3 datalekken gaan over het verkeerd adresseren van post;
- 1 datalek gaat over het onjuist inrichten van een digitaal formulier op de website;
- 1 datalek gaat over het versturen van diverse e-mailadressen.

Melden van inbreuken en cijfers
Elke medewerker kan een melding maken van een beveiligingsinbreuk. Dit wordt geregistreerd in TopDesk (register). Daarnaast is er op intranet een formulier beschikbaar voor medewerkers om een datalek te melden.

De privacy coördinator beoordeelt vervolgens of de inbreuk ook daadwerkelijk een datalek is. De leidinggevende van de afdeling waar het datalek is ontstaan is verantwoordelijk om hiervoor de juiste gegevens aan te leveren. Of een datalek moet worden gemeld bij de toezichthouder overlegt de privacy coördinator met de CISO en/of de FG. De privacy coördinator is namens het college gemandateerd om te melden bij de toezichthouder. Het betrokken afdelingshoofd informeert de directie en de portefeuillehouder.

De bij de toezichthouder gemelde datalakken worden geregistreerd in het zaaksysteem van de organisatie.

Een datalek dat waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van betrokkenen moet ook aan de betrokkenen worden gemeld. De procedure hiervoor is gelijk aan die bij het melden aan de Autoriteit Persoonsgegevens. Het afdelingshoofd van de afdeling waar het datalek is ontstaan meldt het veroorzaakte datalek aan betrokkenen.

Figuur 4 – Cijfers

Bovenstaande werkwijze is vastgelegd in de handleiding melden datalek.

Leren van inbreuken
Bij 1 van de gemelde datalekken zijn technische maatregelen doorgevoerd. Hiermee is het datalek gedicht en wordt herhaling in de toekomst voorkomen. Bij de overige gemelde datalekken is de leidinggevende in gesprek gegaan met de betrokken medewerker om de bewustwording te vergroten.

Verwerkersovereenkomsten
De gemeente werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in verschillende rollen en hoedanigheden samen met publieke en private organisaties. Hierbij worden vaak persoonsgegevens 'verwerkt' zoals het ontvangen van persoonsgegevens, het verzenden van persoonsgegevens, het opslaan van en inzage hebben in persoonsgegevens.

Over deze verwerkingen worden afspraken gemaakt die worden vastgelegd in een verwerkersovereenkomst. De gemeente Doetinchem hanteert hiervoor de standaard verwerkersovereenkomst die is verstrekt door de Informatiebeveiligingsdienst (IBD).

Contractmanagement
De afdeling contactmanagement/inkoop ziet de hoofdovereenkomst en gaat na of er een verwerkersovereenkomst nodig is. Er is een format opgenomen in de aanbestedingsprocedure. De verwerkersovereenkomsten worden opgeslagen in het zaaksysteem. Hierbij wordt geen eenduidige categorie gekozen.

Ook andere medewerkers zijn via berichten op intranet op de hoogte gebracht van de verwerkersovereenkomst. Er is een flyer beschikbaar om informatie terug te lezen.

Het is niet zichtbaar voor de privacy coördinator of bij alle hoofdovereenkomsten waarbij een verwerkersovereenkomst nodig is, dit ook is of wordt afgesloten.

Aanstellen FG (functionaris gegevensbescherming)
De gemeente heeft een FG aangesteld en aangemeld bij de Autoriteit persoonsgegevens. De FG geeft advies en houdt intern toezicht op de naleving van de privacy wet- en regelgeving. De FG is rechtstreeks aanspreekpunt voor burgers en de Autoriteit persoonsgegevens. De contactgegevens van de FG staan op de website van de organisatie. Hierbij is de naam, het algemene telefoonnummer en een rechtstreeks e-mailadres vermeld. Volgens het standpunt van de Autoriteit persoonsgegevens is hiermee voldaan aan de eis van 'rechtstreekse' benadering van de FG.

Privacyverklaring
Op de website van de gemeente is een privacyverklaring opgenomen. Het is verplicht burgers, medewerkers en (keten)partners duidelijk en transparant te informeren over welke privacygevoelige gegevens u verzamelt en met welk doel u dit doet.
De privacyverklaring behoort diverse elementen te bevatten. In onderstaande figuur 5 is zichtbaar of hieraan is voldaan.

Privacyverklaring bevat	Aanwezigheid
Verkregen persoonsgegevens	ja, niet limitatief
De bronnen van verkregen persoonsgegevens	nee, wel in verwerkingsregister
Doeleinden van verwerking	ja, niet limitatief
Consequentie bij niet verstrekken van gevraagde informatie	mogelijkheid om klacht in te dienen
Verdere verwerking (indien van toepassing)	n.v.t.
Gemakkelijk toegankelijk en beschikbaar	redelijk en ja
Tijdig wordt verstrekt	ja, gemeente heeft wel bijzondere rol
Duidelijk is gedateerd	ja

Figuur 5 - Privacyverklaring

Hoofdstuk 6 - Verdiepingsonderwerpen AVG
Naast de onderwerpen uit hoofdstuk 5 kent de AVG diverse andere onderwerpen die van belang zijn om te privacy goed te waarborgen. Deze onderwerpen gaan verder dan de basiskennis van de AVG. Dit hoofdstuk kent in dit eerste toetsingsjaar 2 onderwerpen. In 2019 worden hier andere verdiepingsonderwerpen aan toegevoegd.

In dit eerste toetsingsjaar worden de rechten van betrokkenen en de Gegevensbeschermingseffectbeoordeling, ook wel de DPIA (data protection impact assessment), getoetst.

Rechten van betrokkenen
Organisaties dienen betrokkenen zowel actief als passief te informeren over de persoonsgegevens die zij verwerken en welke rechten zij kunnen uitoefenen om zelf controle uit te oefenen over de eigen persoonsgegevens. Informatie hierover is goed te vinden op de website, onder het kopje 'privacy' in de privacyverklaring. De toegang tot de rechten is basic ingericht.

Bij de gemeente Doetinchem kunnen alle rechten voor betrokkenen worden uitgeoefend. Dit kan per e-mail of telefoon. Het is ook mogelijk een e-mailbericht te sturen voorzien van een gewaarmerkte kopie ID. De identiteit van elke verzoeker wordt vastgesteld. Een kopie ID is onvoldoende bewijs om de identiteit vast te stellen. De afdeling juridische zaken wordt bij deze verzoeken betrokken indien dit nodig wordt geacht door de privacy coördinator. Bij een verzoek wordt nagegaan waar de betreffende persoonsgegevens zijn verwerkt. Dit levert extra uitzoekwerk op voor medewerkers.

Van alle verzoeken wordt een zaak aangemaakt in het zaaksysteem.

Er wordt over nagedacht om de toegang tot het uitoefenen van de rechten van betrokkene in de toekomst verder uit te breiden. Dit kan door gebruik te maken van een digitaal verzoek via DigiD.

DPIA (data protection impact assessment)
Als organisatie kun je verplicht zijn om een DPIA uit te voeren. Voorafgaand aan iedere nieuwe verwerking van persoonsgegevens dienen de privacy risico's in kaart te worden gebracht. Een DPIA is in ieder geval verplicht als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de mensen van wie de gemeente persoonsgegevens verwerkt.

Bij de gemeente Doetinchem is 2x een DPIA uitgevoerd. Deze processen komen voorbij omdat in het voortraject de adviseurs van informatiemanagement deelnemen. Zij hebben privacy en de DPIA opgenomen in hun checklist zodat hierover wordt nagedacht.

Het proces rondom de DPIA kan beter worden ingericht. Dit kan worden bereikt door de afdeling contactmanagement/inkoop meer bij dit onderwerp te betrekken. Maar belangrijker om bij het opkomen van ideeën en het doorvertalen naar plannen direct rekening te houden met de bescherming van persoonsgegevens.

Bijlage 1 - Taken, verantwoordelijkheden en bevoegdheden interne toetsing AVG

Taken, verantwoordelijkheden en bevoegdheden zijn binnen deze procedure als volgt georganiseerd:

- Een interne toetsing AVG wordt uitgevoerd door de functionaris gegevensbescherming.
- Het initiëren en coördineren van de interne toetsing AVG is een primaire verantwoordelijkheid van de functionaris gegevensbescherming.
- De functionaris gegevensbescherming is verantwoordelijk voor de actualiteit van deze procedure

Uitvoering
De uitvoering van de interne toetsing AVG kent de volgende stappen:
Verzamelen gegevens

- De privacy coördinator levert de gevraagde privacygegevens aan en maakt hierbij indien nodig gebruik van andere betrokken collega's binnen de organisatie.

Opzet normenkader

- De functionaris gegevensbescherming stelt aan de hand van de eisen van de AVG een normenkader en controleplan op, hierbij wordt bij voorkeur aansluiting gezocht bij het normenkader geldend in de branche.

Uitvoeren interne toetsing

- De functionaris gegevensbescherming maakt een afspraak met de privacy coördinator voor een controle, bij de organisatie waar de privacy coördinator werkzaam is.
- De functionaris gegevensbescherming stelt een onderzoek in, waarbij het normenkader en controleplan wordt gehanteerd.
- De functionaris gegevensbescherming verzamelt per norm bewijs (documenten, interviewverslagen) en beoordeeld deze. Per norm leidt dit tot een oordeel. De bevindingen worden vastgelegd in de rapportage AVG.

Rapporteren

- De rapportage wordt afgestemd met de privacy coördinator. Het verslag wordt aan de hand van aanvullend materiaal eventueel aangepast en definitief gemaakt.
- Op basis van de definitieve rapportage wordt door de functionaris gegevensbescherming geadviseerd over de mate waarin de organisatie voldoet aan de gestelde eisen.
- Het college van B&W beslist vervolgens wat er met de adviezen wordt gedaan. De rapportage wordt ondertekend en ter beschikking gesteld aan de privacy coördinator.
- De controller en de functionaris gegevensbescherming besluiten hoe de rapportage onderdeel uitmaakt van de managementrapportage.

Interne toetsing AVG
Minimaal jaarlijks beoordeelt de FG of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien dit niet het geval is, wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden omtrent een juiste toepassing van de procedure.