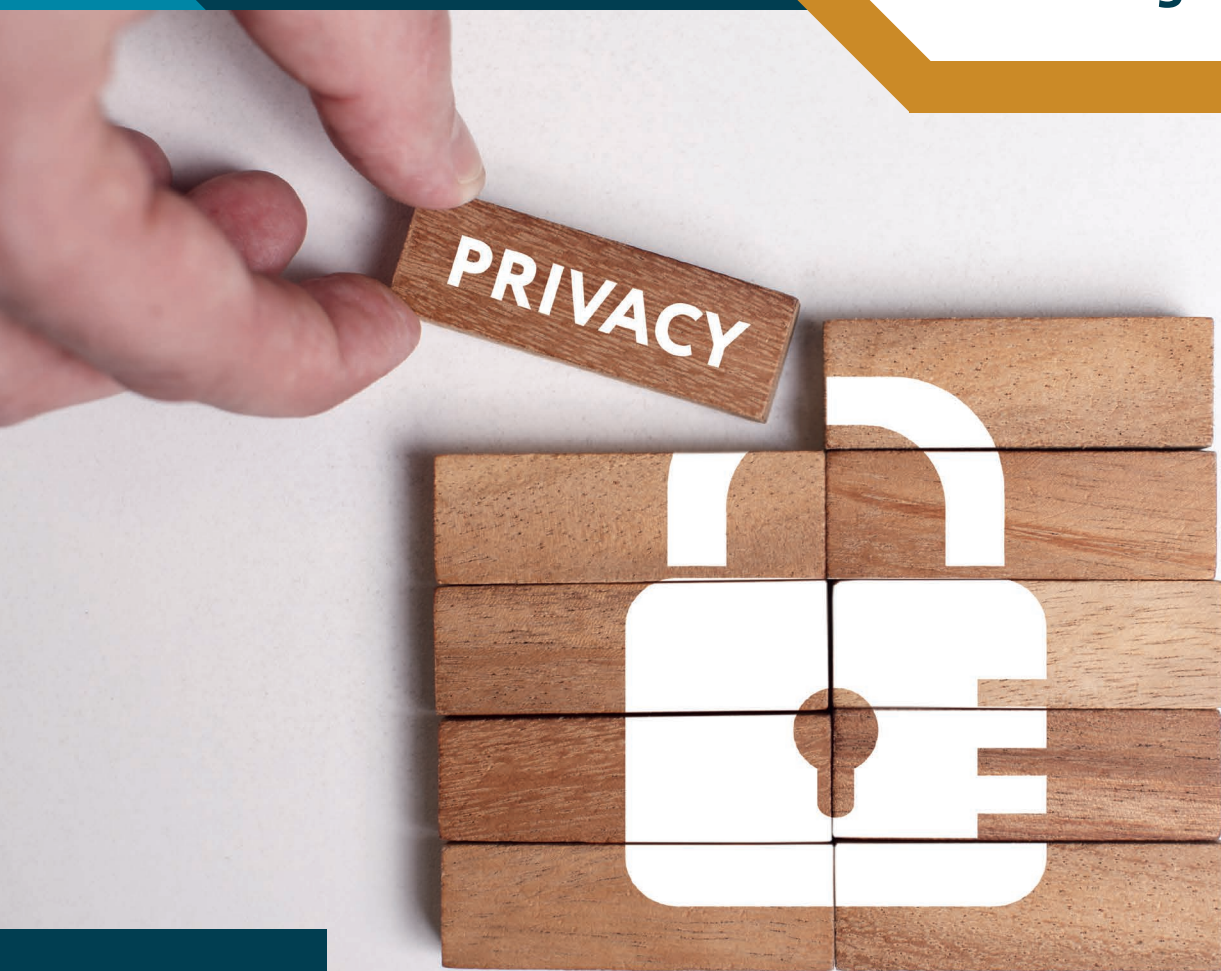


Functionaris voor de Gegevensbescherming gemeente Oss



Inhoud

Inleiding	2
1. Algemene indruk 2021	3
2. Status privacy	3
2.1 Beleid	3
2.2 Organisatorische inbedding	4
2.3 Risicomanagement	5
2.4 Samenwerking	6
2.5 Rechten van betrokkenen.....	7
2.6 Beveiliging	8
2.7 Verantwoording	9
3. Conclusie en aanbevelingen.....	10

Inleiding

We leven in een datagedreven wereld. Over nagenoeg iedereen worden doorlopend gegevens vastgelegd. Natuurlijk heeft dit voordelen, bijvoorbeeld doordat producten en diensten beter kunnen worden afgestemd op inwoners. Of doordat er onderzoeksgegevens kunnen worden gegenereerd voor het maken of bijsturen van beleid. Deze ontwikkeling brengt echter ook risico's met zich mee. Daarom is in Europa in 2016 de Algemene verordening gegevensbescherming (AVG) aangenomen. Dit is het algemene normenkader voor de bescherming van persoonsgegevens.

De AVG is een algemeen normenkader en regelt meer dan alleen 'een check achteraf' of iets wel of niet mag. Het gaat bijvoorbeeld over de vraag of gebruik van gegevens noodzakelijk is, waar en hoe lang deze bewaard worden, of ze voldoende beveiligd zijn en of we transparant kunnen zijn naar onze inwoners over het gebruik van hun gegevens.

Maar ook om alles wat we als organisatie moeten doen om ervoor te zorgen dat het naleven van die regels structureel wordt gewaarborgd en dat we daarover ook rekenschap kunnen afleggen. De (effectiviteit van de) maatregelen moeten aangetoond kunnen worden.

We vinden het als organisatie belangrijk om bij te dragen aan het verbeteren van de inwonersbeleving. Open en transparant zijn en verantwoording kunnen afleggen over het gebruik van gegevens van onze inwoners past binnen onze visie van een dienstverlenende organisatie.

Een goede omgang met privacy biedt daarnaast kansen processen te optimaliseren, data op te schonen en het risico op incidenten te verminderen.

Verwerking van persoonsgegevens vindt plaats onder de verantwoordelijkheid van zowel het college, de burgemeester als de gemeenteraad. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast moet de gemeente beschikken over een interne toezichthouder: de functionaris gegevensbescherming (FG).

De FG ziet toe op de naleving van het beleid en de privacy wet- en regelgeving in de brede zin en informeert de organisatie over verplichtingen die daaruit voortvloeien. In deze jaarrapportage brengt de FG in dat kader verslag uit over zijn bevindingen over 2021.

Dit jaarverslag bevat (bewust) een kritisch geluid. In lijn met de 'open en transparante' organisatie die we zijn, wordt zichtbaar gemaakt dat er nog de nodige stappen moeten worden gezet. Juist door je als organisatie bewust te zijn van de actuele stand van zaken, kun je leren en verbeteren en de kwaliteit rondom privacybescherming verhogen.

Functionaris voor gegevensbescherming

1. Algemene indruk

De afgelopen jaren is er in de organisatie een basis gelegd voor gegevensbescherming, waarbij urgente en wettelijke taken zijn opgepakt. Vanwege vele opgaven waar de gemeente voor aan de lat staat in relatie tot beperkte beschikbare capaciteit is er door het bestuur voor gekozen om vanaf 2020 minder prioriteit te geven aan gegevensbescherming. Aspecten als het evalueren en het verder borgen van processen rondom gegevensbescherming zijn daardoor naar de achtergrond verschoven.

In 2020 is er een onderzoek uitgevoerd naar de 'privacy-volwassenheid' van de organisatie. Hieruit bleek dat er nog onvoldoende geborgd was en dat er een hoop ontwikkelpunten waren. Sindsdien zijn er zeker stappen gezet, maar kan geconcludeerd worden dat de implementatie van de AVG nog niet is voltooid.

De aanpak van de bescherming van persoonsgegevens is nog vaak reactief en incident gedreven. De risico's zijn niet altijd voldoende in beeld en er is nog geen continue verbeterproces.

Opgemerkt moet wel worden dat er verschillen zijn tussen afdelingen. Enkele afdelingen hebben zichtbaar meer aandacht voor privacy. Dat vertaalt zich in meer kennis, vaardigheden en borging van gegevensbescherming.

Vanuit de programmabegroting 2022-2025 is er capaciteit beschikbaar gesteld voor de invulling van twee privacy-functies, waardoor er de komende jaren verder gebouwd kan worden aan het fundament voor gegevensbescherming.

2. Status privacy

Er bestaat geen alomvattend normenkader waaraan getoetst kan worden of een organisatie aan de AVG voldoet. Een organisatie volledig op detailniveau toetsen is dan ook onmogelijk. Waar wel naar gekeken kan worden is of de verplichte beheersmaatregelen die de AVG voorschrijft gebruikt worden om risico's te beheersen. In deze jaarrapportage is het onderwerp 'privacy' opgesplitst in 7 thema's, welke gezamenlijk alle aspecten van gegevensbescherming bevatten. Er is geen volgorde: de criteria dienen in onderlinge samenhang te worden gelezen. Van een aantal cruciale basisuitgangspunten wordt de status weergegeven. Bij het in beeld brengen van de stand van zaken wordende volgende kleuren gebruikt:

-  managementaandacht nodig
-  gedeeltelijk op orde
-  in control

2.1 Beleid

Het privacybeleid geeft aan op welke wijze - door het treffen van maatregelen - voldaan wordt aan de van toepassing zijnde privacywet- en regelgeving. Het geeft op organisatie- en strategisch niveau duidelijkheid over de inrichtingskeuzes van privacy en waarborgt dat de verwerking van gegevens op een rechtmatige wijze plaatsvindt.

Er is een algemeen privacybeleid met vastgestelde kaders



Het privacybeleid komt tot stand langs een cyclisch proces



Bestuur, directie en management laten zien dat privacy belangrijk is en zijn actief betrokken



Het privacybeleid is leidend bij ontwerp en ontwikkelingen van (nieuwe) verwerkingen



Bevindingen

In 2016 is het 'Privacybeleidskader Gemeente Oss' vastgesteld. Omdat wet- en regelgeving externe factoren zijn, is periodieke review nodig om vast te stellen of het beleid nog voldoet. Eenmalig beleid opstellen is niet voldoende. Daarnaast kunnen ook interne factoren, zoals onvoldoende effectiviteit van het beleid en gewijzigde missie of visie, bepalend zijn om het beleid te actualiseren. Door het beleid periodiek te evalueren en bij te stellen wordt bereikt dat het op de ontwikkelingen en de uitvoering afgestemd blijft. Ook kunnen daar de benodigde middelen aan gekoppeld worden en kan deze meegenomen worden in de planningscyclus van de organisatie.

De directie en het management vinden privacy en een zorgvuldige omgang met gegevens belangrijk. Privacy wordt echter niet altijd tijdig en naar behoren betrokken bij (nieuwe) ontwikkelingen. Risico's worden daardoor (onbewust) geaccepteerd. Het is belangrijk dat privacymaatregelen in het ontwerpproces van nieuwe producten, diensten en processen (bij voorkeur al bij de beleidsontwikkeling) aan de orde komen. Gegevensbescherming kan er namelijk aan het eind van het proces niet nog even 'aangeplakt' worden. Het speelt daarnaast ook een belangrijke rol bij beoordeling van de rechtmatigheid van een verwerking door bijvoorbeeld de AP.

2.2 Organisatorische inbedding

Het waarborgen van gegevensbescherming ligt niet bij één persoon. Veel medewerkers hebben in hun werk te maken met de privacy wet- en regelgeving. Het is daarom van belang dat deze medewerkers op de hoogte zijn van het belang van een goede omgang met persoonsgegevens. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en het creëren van bewustzijn.

De taken, verantwoordelijkheden en bevoegdheden zijn duidelijk belegd



Er is ruime (juridische) kennis en ervaring over privacy en relevante wet- en regelgeving



Er is een vastgesteld jaarplan waarin prioriteiten worden bepaald



Bevindingen

In het 'Privacybeleidskader Gemeente Oss' is de privacy-organisatie beschreven. Deze beschrijving is verouderd. De privacyorganisatie is bij de implementatie van de AVG voor een deel anders vormgegeven. Met de komst van twee privacy officers in 2022 verdient het aanbeveling taken, verantwoordelijkheden, bevoegdheden en rapportagelijnen te beschrijven en formeel vast te stellen. Denk hierbij aan alle functies/rollen in de organisatie, zoals bijvoorbeeld ook die van privacyaccenthouder.

Beleid is pas effectief als medewerkers daarvan op de hoogte zijn. Taken en bevoegdheden rondom de bescherming van persoonsgegevens zijn niet voor iedereen duidelijk. Zo maakt het bijvoorbeeld geen onderdeel uit van het inwerkprogramma. Er is meer aandacht nodig voor interne bewustwording en doelgroepgerichte training van medewerkers op privacybestendig werken. In 2021 is daar al wel een start mee gemaakt door de uitrol van een e-learning privacy en AVG.

Er wordt in de organisatie nog niet gewerkt aan de hand van een jaarplan. Op basis van de organisatiebrede volwassenheidsmeting uit 2020 en deze jaarrapportage kunnen daarvoor de prioriteiten worden bepaald. Ook lessen voortvloeiend uit incidenten en risico's uit DPIA's kunnen daar in meegenomen worden.

2.3 Risicomanagement

Om grip te hebben en houden op het gebruik van persoonsgegevens is het noodzakelijk voor organisaties om een actueel privacymanagement te voeren. Dit betekent bijvoorbeeld dat organisaties moeten kunnen aantonen welke persoonsgegevens ze in huis hebben, voor welke doeleinden ze deze gebruiken en welke maatregelen er zijn genomen om de gegevens te beschermen. Pas als je weet welke data je in huis hebt kun je deze ook goed beschermen. Dat verkleint bijvoorbeeld het risico op datalekken of op onrechtmatig gebruik van gegevens door de organisatie zelf en het vergroot de mogelijkheden om naar inwoners en medewerkers toe transparant te zijn.

Vanwege deze verantwoordingsplicht moet de organisatie een (actueel) register bijhouden van alle verwerkingsactiviteiten die onder haar verantwoordelijkheid plaatsvinden.

Daarnaast moet de organisatie 'Data Protection Impact Assessment' (DPIA's) uitvoeren voor verwerkingen met een hoog risico. Hierbij worden vooraf privacy risico's in kaart gebracht om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen of weg te nemen. Voorbeelden van 'hoog risico verwerkingen' zijn cameratoezicht of gegevensuitwisseling binnen het zorg- en veiligheidsdomein.

Het verwerkingsregister is actueel en het beheer is intern belegd



Werkprocessen of verwerkingen met een hoog risico zijn vastgesteld.



Voor verwerkingen met hoge privacyrisico's worden DPIA's uitgevoerd en mitigerende maatregelen worden doorgevoerd.



Bevindingen

Het verwerkingsregister bestaat uit verschillende Excel-bestanden verspreid over de teams in de organisatie. Ondanks het feit dat er veel verwerkingen staan opgenomen in het register, is bij de meeste teams de registratie niet volledig op orde. De overzichten zijn niet volledig/actueel. Er is ook een team waar nog geen register is opgesteld, waar dit wel zeer wenselijk is. Het gaat hier namelijk om processen waarbij hoge privacyrisico's een rol spelen, bijvoorbeeld door het uitwisselen van (gevoelige) persoonsgegevens met externe partijen.

De aanschaf en implementatie van een Privacy Management Systeem en een proces rondom het beheer van het verwerkingsregister zijn maatregelen die kunnen bijdragen aan het volledig en actueel houden van het register.

Een ander aandachtspunt is 'eigenaarschap' van verwerkingen. Niet alle verwerkingen/systemen/procedures hebben een 'eigenaar'. Gevolg daarvan is dat deze verwerkingen niet in het register worden opgenomen en er geen verbetercyclus wordt uitgevoerd.

Een groot deel van de teams heeft geen volledig overzicht van de verwerkingen met een hoog privacy risico. DPIA's worden bijna nog niet uitgevoerd. Een aantal teams is er inmiddels mee gestart. Daar worden nu voor nieuwe of bij wijzigingen van verwerkingen DPIA's uitgevoerd.

Het is wenselijk dat er een inventarisatie plaatsvindt waar DPIA's nodig zijn en dat er een planning wordt opgesteld voor de uitvoering daarvan.

Hieronder een overzicht van de DPIA's die in 2021 zijn uitgevoerd of waarmee is gestart:

Onderwerp DPIA	Status
Datawarehouse/Dashboard sociaal domein	Afgerond. Aanvullend nog een keer in 2022
Proces tegemoetkoming kinderopvang	Afgerond
Mobile Device Management	In behandeling
Signalenoverleg/Maasland Interventie Team	In behandeling
HRM-proces/applicatie	In behandeling

2.4 Samenwerking

De organisatie werkt op meerdere beleidsterreinen samen met (mede-)overheden, ketenpartners en private organisaties. Juiste afspraken over de omgang met persoonsgegevens met samenwerkende partijen zijn nodig. Organisaties die persoonsgegevens onder verantwoordelijkheid van de gemeente verwerken worden 'verwerker' genoemd. Een voorbeeld daarvan is het uitbesteden van de boekhouding of het gebruiken van een clouddienst. In dat geval is het verplicht een verwerkersovereenkomst af te sluiten. Een verwerkersovereenkomst bevat bijvoorbeeld afspraken over de verwerkingen die de verwerker mag uitvoeren en de beveiligingsmaatregelen.

Omdat de risico's rondom verwerkingen niet statisch zijn, is het nodig een overeenkomst met een verwerker periodiek te evalueren en de verwerker te controleren. Het is een belangrijk controlemechanisme. Als verwerkingsverantwoordelijke is de gemeente verantwoordelijk voor de gehele verwerking en keten van (sub)verwerkers. Actief toezicht op het nakomen van de gemaakte afspraken, waaronder de naleving van de beveiligingsmaatregelen, is daarom belangrijk.

De organisatie heeft een overzicht van partijen waarmee een (verwerkers)overeenkomst is gesloten



Bij het inschakelen van externe partijen wordt voorafgaand getoetst of er sprake is van het verwerken van persoonsgegevens en wanneer dit het geval is, worden voorafgaand aan de inschakeling afspraken gemaakt over de verwerking



Bevindingen

Een volledig overzicht van partijen waarmee een (verwerkers)overeenkomst is gesloten ontbreekt. Enkele teams hebben wel een eigen overzicht.

Om uitbesteding, samenwerking en uitwisseling van gegevens met externe partijen goed te borgen is het aan te bevelen om overzicht te houden op deze partijen. Welke organisaties hebben we ingeschakeld of werken we mee samen? Welke verwerkingen voeren zij uit? Wie heeft welke rol? En wat zijn de risico's? Als verantwoordelijke is het belangrijk om te blijven monitoren of partijen zich aan de (beveiligings)afspraken houden. Richt daarom het toezicht op de naleving van (verwerkers)overeenkomsten in. Stel regelmatig vast of partijen zich nog aan de afspraken houden.

2.5 Rechten van betrokkenen

Inwoners, medewerkers en andere betrokkenen moeten zowel actief als passief geïnformeerd worden over de omgang met hun persoonsgegevens. Daarnaast stelt de AVG betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

Er is een werkend proces om het recht van inzage van betrokkenen te faciliteren



Er is een communicatieplan over privacy om invulling te geven aan de AVG-transparantieplichtingen.



Bevindingen

De organisatie heeft in 2018 een procedure voor de afwikkeling van inzageverzoeken van betrokkenen geïmplementeerd. Deze procedure wordt consequent toegepast. De juridische ontwikkelingen op dit gebied gaan echter snel. Het is daarom aan te bevelen om deze procedure te evalueren en te actualiseren.

Transparantie is een van de belangrijkste uitgangspunten van de AVG. Op de gemeentelijke website is een algemene privacyverklaring opgenomen. Betrokkenen worden echter nog niet altijd geïnformeerd over verwerkingen van hun persoonsgegevens. Evaluatie van bestaande werkwijzen en een gemeentebreed communicatieplan voor privacy is daarom wenselijk. In een dergelijk plan kan invulling worden gegeven aan diverse transparantieplichtingen, zoals via welke kanalen inwoners en personeel worden geïnformeerd over de verwerking en bescherming van hun persoonsgegevens en hun rechten.

Hieronder een overzicht van het aantal inzageverzoeken de afgelopen jaren:

	2019	2020	2021
Inzageverzoeken	9	4	11

2.6 Beveiliging

Passende technische en organisatorische maatregelen zijn essentieel om persoonsgegevens te beschermen. De basis voor passende beveiliging ligt in de Baseline Informatiebeveiliging Overheid (BIO), de beveiligingsstandaard voor alle overheidsorganisaties.

Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten waar persoonsgegevens bij betrokken zijn gedocumenteerd moeten worden en onder omstandigheden gemeld dienen te worden aan de Autoriteit Persoonsgegevens en/of betrokkenen.

De gemeente stelt organisatiebreed een informatiebeveiligingsplan formeel vast, waarbij de bescherming van persoonsgegevens als aandachtspunt is meegenomen



De gemeente heeft een datalekprocedure



De medewerkers zijn bekend met de datalekprocedure en passen deze consequent toe



Bevindingen

Informatiebeveiliging

De ontwikkelingen op het gebied van informatiebeveiliging gaan snel. De organisatie zet stappen in de goede richting om de informatiebeveiliging op orde te krijgen. Er worden organisatorische maatregelen genomen om gegevens te beveiligen en om dat te kunnen aantonen. Zo wordt de laatste hand momenteel gelegd aan het nieuwe informatiebeveiligingsbeleid, waarin richting wordt geven aan de invulling van informatiebeveiliging binnen de organisatie. Vervolgens wordt in 2022 een informatiebeveiligingsplan opgesteld. De organisatie is echter nog niet volledig in control met de BIO. Zo moet de organisatie bijvoorbeeld aan de slag met 'logische toegangscontrole' (maatregelen welke de toegang tot gegevens en informatiesystemen beheersen).

Door het uitvoeren van DPIA's krijgt de organisatie meer zicht op (bestaande) informatiebeveiligingsrisico's. Een aanbeveling is om de nog te nemen beveiligingsmaatregelen af te stemmen op de uitkomsten van de DPIA's.

Datalekken

De organisatie heeft een datalekprocedure. Er is nog veel onbekendheid over deze procedure onder medewerkers en hoe datalekken moeten worden afgehandeld. In 2021 zijn er 15 datalekken geregistreerd, waarvan er 2 bij de Autoriteit Persoonsgegevens zijn gemeld. Gezien het lage aantal geregistreerde datalekken afgezet tegen de grootte van de organisatie is het mogelijk dat niet alle datalekken als dusdanig worden herkend. Naarmate de bewustwording over dit onderwerp wordt vergroot en er een positieve cultuur wordt gecreëerd rondom het intern melden van datalekken, is de verwachting dat het aantal geregistreerde datalekken toeneemt. Mijn aanbeveling is daarom om in 2022 meer organisatiebrede training en bewustwording op te zetten.

Hieronder een overzicht van het aantal geregistreerde datalekken:

	2019	2020	2021
Geregistreerde datalekken	19	7	15
Gemeld bij de AP	3	3	2

2.7 Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht levert de gemeente een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat de gemeente aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en andere relevante wet en regelgeving.

De gemeente heeft inzichtelijk welke acties en maatregelen genomen moeten worden om het niveau van gegevensbescherming en de zorgvuldige omgang met persoonsgegevens naar een hoger niveau te brengen



Verantwoording is structureel ingericht, zodat naleving is geborgd



Bevindingen

In 2020 is er een onderzoek uitgevoerd naar de 'privacy-volwassenheid' van de organisatie. Daar kwamen ontwikkelpunten uit naar voren om naar een hoger volwassenheidsniveau toe te kunnen werken. Binnen gemeentelijke organisaties zijn er aanzienlijke verschillen tussen teams voor wat betreft de aard en de omvang van verwerking van persoonsgegevens en de risico's die dat met zich mee brengt. Het zou goed zijn om voor teams apart een onderzoek naar volwassenheid uit te voeren en een plan van aanpak op te stellen.

Er wordt nog weinig gerapporteerd over de (voortgang van) verbeteracties en relevante ontwikkelingen op het gebied van privacy. Met de komst van twee privacyfunctionarissen in 2022 kan een continue verbetercyclus opgezet gaan worden.

Daarnaast wordt nog niet voldoende gezorgd voor aantoonbare naleving van wet- en regelgeving doordat er weinig DPIA's zijn uitgevoerd. Deze verantwoording is vooral een verantwoordelijkheid van de primaire afdelingen.

Een ander aandachtspunt rond de verantwoording is dat, wanneer de organisatie afwijkt van het advies van de FG, de motivering daarvan vastgelegd moet worden.

3. Conclusie en aanbevelingen

Het inbedden van gegevensbescherming in de dienstverlening, werkprocessen en planning- en control-cyclus kost tijd, energie en geld. Dat gaat niet vanzelf. Belangrijk is dat de organisatie blijft bouwen aan een fundament dat als basis dient voor een betrouwbare overheid.

Specifieke aandacht zal in 2022 moeten uitgaan naar het gestructureerd integreren van gegevensbescherming in de organisatie en het verhogen van het privacy bewustzijn. Belangrijke aspecten daarbij zijn:

1. Het actualiseren van het privacybeleid, met inbegrip van de 'privacyorganisatie' en deze communiceren.
2. Het tijdig betrekken van privacy bij nieuwe ontwikkelingen: in het ontwerpproces van nieuwe producten, diensten en processen. Bij voorkeur al bij de beleidsontwikkeling.
3. Gaan werken met een vastgesteld jaarplan waarin (organisatiebrede) prioriteiten worden bepaald.
4. Het voeren van een actueel privacymanagement o.a. ten aanzien van het verwerkingsregister, hoog risico verwerkingen/processen en (verwerkers)overeenkomsten.
5. Het plannen en uitvoeren van DPIA's voor risicovolle verwerkingen/processen om risico's en mitigerende maatregelen in beeld te krijgen en deze te kunnen uitvoeren.
6. Interne bewustwording en doelgroepgerichte training van medewerkers.
7. Het opstellen van een gemeentebreed communicatieplan voor privacy.

Prioriteiten verwerkingen met een hoog risico

Op basis van de nu beschikbare informatie is bekend dat zeker 100 verwerkingen/processen waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van personen. Hoog risico verwerkingen/processen die in het bijzonder prioriteit moeten krijgen zijn¹:

- Verwerkingen in samenwerkingsverbanden zoals RIEC, Zorg- en veiligheidshuis, sociale wijkteams en domein overstijgende overleg(tafels).
- (Uitbestede) processen rondom kwetsbare groepen zoals schuldhulpverlening en jeugdhulp.
- Verwerkingen waarmee burgers of medewerkers bedoeld of onbedoeld gecontroleerd of geobserveerd (kunnen) worden, zoals cameratoezicht, locatiebepaling van voertuigen en gedragsanalyse via ICT-systemen.
- 'Zwarte lijsten': waarbij persoonsgegevens over strafrechtelijke veroordelingen, strafbare feiten en gegevens over onrechtmatig of hinderlijk gedrag worden verwerkt.
- Verwerkingen waarbij gebruik gemaakt wordt van cloudoplossingen.
- Verwerkingen waarbij gebruik gemaakt wordt van 'big data', kunstmatige intelligentie, algoritmen of analysesystemen.

¹ Hiervoor is o.a. aansluiting gezocht bij de focusgebieden van de AP die voor de periode 2020 tot en met 2023 zijn aangewezen in het visiedocument 'Dataproductie in een digitale samenleving': <https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/focus-ap-2020-2023>.