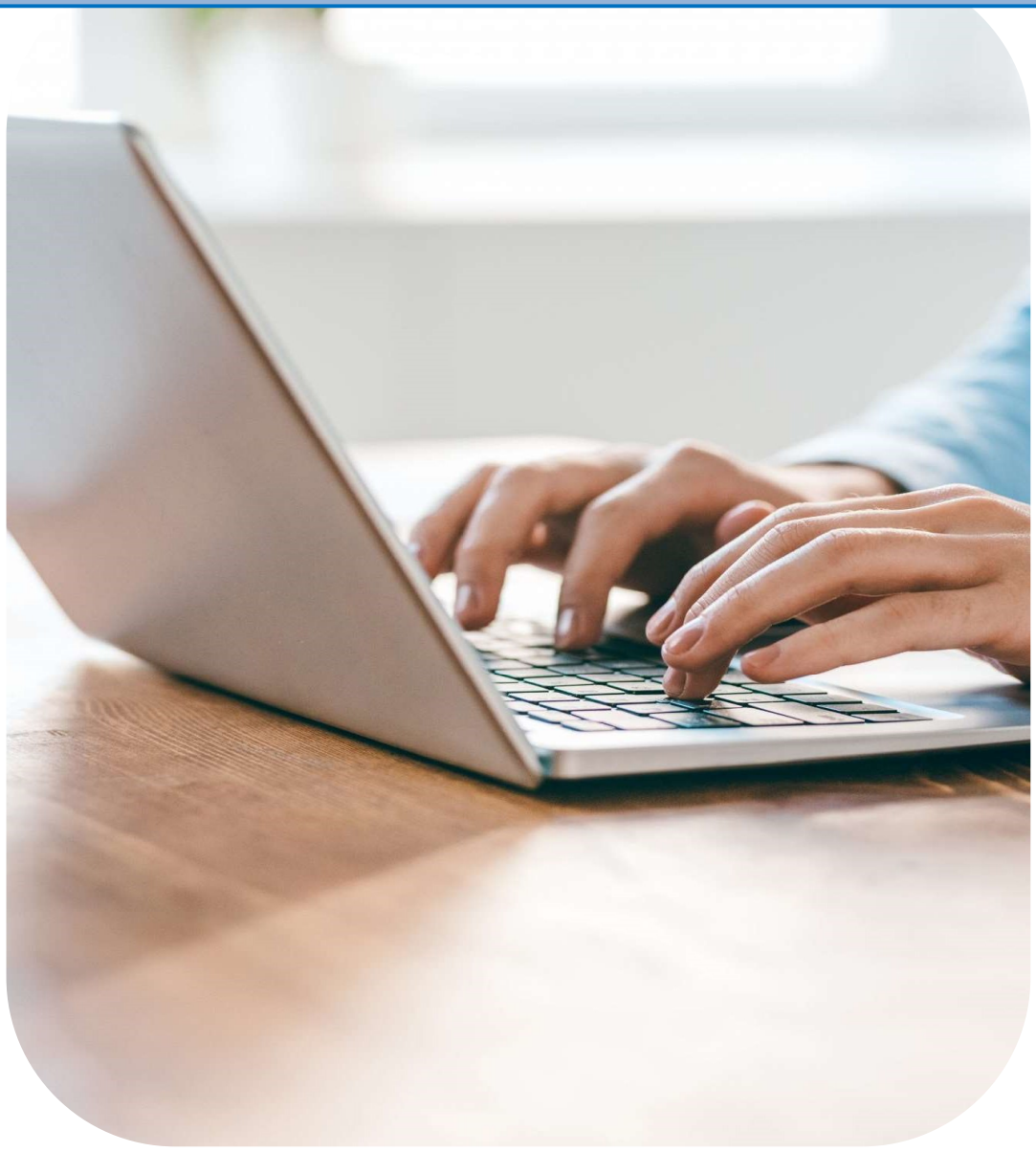
JAARRAPPORTAGE FUNCTIONARIS GEGEVENSBESCHERMING 2021



Verwerkingen colleges van burgemeester en wethouders
Gemeentes Deventer, Olst-Wijhe en Raalte
Lotte Schieving, Functionaris Gegevensbescherming
Maart 2022

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Inhoud

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Inleiding en samenvatting

Gemeentes verwerken op grote schaal persoonsgegevens van inwoners. Zonder deze gegevens kunnen zij hun taken niet uitvoeren. Het gaat in de praktijk niet alleen om het verwerken van persoonlijke informatie van inwoners, maar ook om de gegevens van medewerkers en relaties van de gemeente. De Europese Algemene Verordening Gegevensbescherming (AVG) biedt waarborgen voor het beschermen van deze persoonsgegevens. De AVG verplicht tot het aantoonbaar treffen van beheersmaatregelen binnen organisaties om privacy en gegevensbescherming te borgen. Het onjuist en onzorgvuldig gebruik van persoonsgegevens kan grote gevolgen hebben voor mensen, zoals identiteitsfraude. Onvoldoende naleving van de AVG kan verder leiden tot forse boetes van de Autoriteit Persoonsgegevens (AP), tot reputatie- en imagoschade bij organisaties en tot schadeclaims van gedupeerde betrokkenen.

In deze rapportage geeft de Functionaris voor gegevensbescherming (FG) een beeld van de stand van zaken bij de gemeentes Deventer, Olst-Wijhe en Raalte als het gaat om het naleven van de AVG in 2021. De uitvoering van de AVG heeft een blijvende grote invloed op bijna alle werkprocessen van deze gemeentes. De gemeentes moeten werkprocessen waarin persoonsgegevens worden verwerkt inrichten volgens de uitgangspunten van de AVG. In 2021 hebben de drie samenwerkende organisaties de in vorige jaren ontwikkelde aanpak bij privacy en neergelegde basis verder uitgebouwd. De uitvoeringspraktijk in 2021 heeft laten zien dat er de afgelopen jaren op het gebied van privacy flink wat werk is verzet, maar dat er ook nog veel onderhanden werk is te doen. De AVG is een veelomvattende en gecompliceerde wet, die om structurele aandacht blijft vragen van bestuur, management en medewerkers. Dit vraagt om een gedegen planning, maar ook om een goed ingerichte organisatorische verbeteringscyclus. Daarnaast heeft de praktijk in 2021 opnieuw aangetoond dat het voor het voldoen aan de privacyverplichtingen cruciaal is dat er voldoende capaciteit beschikbaar is in de vorm van mensen en middelen om de daarbij horende werkzaamheden ook daadwerkelijk te kunnen uitvoeren. Dat blijkt lastig, waardoor werkzaamheden in de tijd uitlopen. Bijvoorbeeld als het gaat om het uitvoeren van risicoassessments (DPIA's).

In deze rapportage brengt de FG verslag uit aan de colleges van burgemeester en wethouders van de gemeentes Deventer, Olst-Wijhe en Raalte als het gaat om de naleving van de AVG bij verwerkingen van persoonsgegevens die onder de verantwoordelijkheid van deze colleges worden uitgevoerd. Het rapport vangt aan met de bevindingen van de FG bij de verschillende onderdelen van de AVG. De FG geeft per aandachtsgebied aan wat haar aanbevelingen zijn voor 2022. Vervolgens gaat de FG in op twee belangrijke ontwikkelingen die in 2022 extra aandacht van de organisaties vragen. De rapportage sluit af met een conclusie.

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

AVG aandachtsgebieden

Governance

De huidige privacyfunctionarissen voeren sinds eind 2020 samen de privacy werkzaamheden uit voor de gemeentes Deventer, Olst-Wijhe en Raalte. De Privacy Officer adviseert over de naleving van de AVG en fungeert als eerste aanspreekpunt voor de gemeentelijke organisaties. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. In 2021 werden zowel de Privacy Officer als de FG in toenemende mate betrokken bij vraagstukken die verband houden met privacy en het uitvoeren van risicoassessments. Daarbij is een discrepantie geconstateerd tussen het aantal uren wat de FG ter beschikking heeft voor de uitvoer van haar wettelijke taken voor de drie gemeentes en het aantal uren dat zij feitelijk nodig heeft om deze taken uit te kunnen voeren. Als tijdelijke oplossing heeft de FG inmiddels haar andere juridische werkzaamheden voor de gemeente Deventer neergelegd en deze benodigde uren ter beschikking gekregen voor het vervullen van haar FG-taken. Het verdient aanbeveling om hier als gemeentes in 2022 samen een structurele oplossing voor te vinden.

In 2018 hebben de gemeentes alle drie een eigen privacyoverlegorgaan ingericht, het Privacy Implementatie Team (PIT). Dit team bestond bij elke gemeente uit een directeur met in zijn portefeuille AVG/privacy, een Privacy Officer, een Information Security Officer, een Chief Information Security Officer (CISO) en een FG. Een aantal keer per jaar behandelde dit team een verscheidenheid aan strategische vraagstukken op het gebied van privacy en informatieveiligheid. In 2021 is ervoor gekozen deze organen samen te voegen tot het Privacy en Informatieveiligheid Toezichtsorgaan DOWR (PIT DOWR). De reden daarvoor is dat de drie gemeentes uitdrukkelijk de wens hebben om bij de aanpak van privacy en informatieveiligheid zo veel mogelijk samen te doen. De managers van de drie gemeentes die verantwoordelijk zijn voor informatiemanagement- en beheer zijn aan het PIT DOWR toegevoegd. Dit ter vervanging van enkele incidentele werkoverleggen met deze managers en de andere leden van het PIT DOWR. Ook nemen de FG en de CISO inmiddels standaard deel aan het strategisch informatieoverleg in de drie gemeentes. Op deze manier probeert men de individuele gemeentes aangesloten te houden bij de uitvoering van de aanpak van privacy en informatieveiligheid door de voornamelijk in DOWR-verband opererende functionarissen. Om ook de andere managers en medewerkers van de individuele gemeentes aangesloten te houden, wordt bij het verspreiden van de notulen van het PIT DOWR gemeentebrede aandacht gevraagd voor de daarin besloten liggende vraagstukken. Het advies is om bij het opstellen van de formele agenda van het kwartaaloverleg PIT DOWR in 2022 de deelnemers van de verschillende gemeentes de mogelijkheid te bieden agendapunten aan te dragen, zodat er een breder gedragen agenda ontstaat. Op dit moment vindt deze input namelijk slechts plaats vanuit het wekelijks samenkomen van de in DOWR-verband opererende privacy- en informatieveiligheidsfunctionarissen.

Register van verwerkingen

De AVG geeft aan dat organisaties moeten kunnen aantonen dat zij handelen in overeenstemming met de wet- en regelgeving. Dat betekent onder meer dat gemeentes een register van verwerkingsactiviteiten moeten bijhouden met daarin alle structurele verwerkingen waar persoonsgegevens bij worden gebruikt. Het register vormt de basis van waaruit andere AVG onderdelen, zoals het uitvoeren van risicoassessments, kunnen worden opgepakt. Alle drie de gemeentes hebben hun verwerkingen van persoonsgegevens inmiddels in een register van verwerkingsactiviteiten opgenomen. Er stond een actualisatie van de registers gepland voor 2021. Managers zou gevraagd worden om de verwerkingen in het register die onder hun verantwoordelijkheid vallen na te gaan en daarbij aan te geven of zij nog up-to-date waren. Ondanks dat er een begin is gemaakt met het betrekken van de managers bij deze plannen, heeft de daadwerkelijke actualisatie nog niet plaatsgevonden. Vanwege het belang van een actueel verwerkingsregister verdient het aanbeveling om in 2022 deze actualisatie alsnog uit te voeren. Aangezien een dergelijke actualisatie daarna periodiek dient plaats te vinden, is het aan te raden daarnaast een proces te ontwikkelen en vast te stellen voor het tijdig nalopen van wijzigingen in de registers van verwerkingen van de drie gemeentes. Dit om achterstanden of vervuiling in de geregistreerde structurele verwerkingen zoveel mogelijk te voorkomen.

DPIA’s

De AVG kent de verplichting om een risicoassessment, een DPIA (Data Protection Impact Assessment), uit te voeren voor verwerkingen met een hoog risico. Daarvan is bijvoorbeeld sprake wanneer een organisatie op grote schaal bijzondere persoonsgegevens gaat verwerken. Met een DPIA worden de privacyrisico’s voor de betrokkenen bij een verwerking van persoonsgegevens in kaart gebracht, evenals de maatregelen om deze risico’s te ondervangen. Wanneer bepaalde privacyrisico’s niet kunnen worden ondervangen is er sprake van een hoog restrisico. In dat geval moet de verwerking voor de start van het werkproces in de lijn of de ingebruikname van een nieuw systeem aan de toezichthouder, de AP, worden voorgelegd.

In 2021 hebben de drie organisaties ervaring opgedaan met het uitvoeren van DPIA’s. Nieuwe verwerkingen of wijzigingen van bestaande verwerkingen zijn actief aangemeld bij de Privacy Officer. Daarbij is er aandacht besteed aan het hergebruik van kennis en het uitwisselen van DPIA’s tussen de drie gemeentes onderling. De Privacy Officer heeft de verschillende wijzen waarop de gemeentes DPIA’s uitvoeren geïnventariseerd en er is uiteindelijk één werkwijze ontwikkeld voor de DOWR met een daarbij horend DPIA-format wat inmiddels bij alle drie de gemeentes in gebruik is. Met het vaststellen van het risicoanalyseproces informatieveiligheid en privacy in DOWR-verband is in 2021 het proces voor het uitvoeren en actualiseren van DPIA’s vastgesteld, hoe intern verantwoordelijken er zorg voor dragen dat relevante verwerkingen in beeld komen bij de Privacy Officer en hoe de te nemen maatregelen opvolging krijgen. Om te borgen dat dit proces ook daadwerkelijk in de drie gemeentes gevolgd gaat worden, is het aan te raden als organisaties in 2022 te kijken naar de verdere implementatie van dit proces.

Het uitvoeren van DPIA’s, met alle activiteiten die daaraan verbonden zijn, resulteert in veel documentatie. Aandacht voor het aantoonbaar vastleggen van bevindingen maakt dat de resultaten

van een DPIA verifieerbaar en vindbaar blijven. Om dit te waarborgen is er in 2021 door de organisaties een DOWR omgeving ingericht op SharePoint, genaamd Informatieveiligheid en Privacy Centraal, waar de ingevulde vragenlijsten, rapportages en adviezen van de FG per gemeente worden gedocumenteerd. In deze nieuwe omgeving is verder een overzicht te vinden van de voor de drie gemeentes geplande DPIA's, hetzij zonder uitvoerdata.

In 2021 is gebleken dat er een steeds groter beroep gedaan wordt op de Privacy Officer door de drie gemeentes als het gaat om het coördineren en adviseren bij DPIA's. Managers en medewerkers weten de Privacy Officer steeds beter te vinden wanneer zij een werkproces of de ingebruikname van een systeem volgens de AVG voorwaarden willen inrichten. Zij lijken zich ook steeds beter bewust van deze verantwoordelijkheid bij risicovolle verwerkingen. Dat daarbij keuzes gemaakt dienen te worden over het prioriteren van werkzaamheden is duidelijk geworden. Op basis van de AVG geldt dat er voor alle nieuwe risicovolle verwerkingen een DPIA moet worden uitgevoerd, vóórdat er begonnen wordt met deze verwerking. Op basis van de richtlijnen van de Autoriteit Persoonsgegevens moet ook voor bestaande risicovolle verwerkingen, namelijk risicovolle verwerkingen die al operationeel waren bij de inwerkingtreding van de AVG in 2018, uiterlijk in mei 2021 een DPIA uitgevoerd zijn. Geen van de drie gemeentes heeft deze doelstelling gehaald. Hier ligt dus nog een grote opgave voor 2022. Bij het eventueel prioriteren van het uitvoeren van DPIA's gaat het enerzijds om de beantwoording van de vraag of deze werkzaamheden voorrang moeten krijgen ten opzichte van de andere werkzaamheden van de Privacy Officer. Anderzijds gaat het om de vraag of nieuwe dan wel gewijzigde verwerkingen voorrang krijgen ten opzichte van reeds geplande DPIA's. Vervolgens zal gekeken moeten worden of er tijdig budget gereserveerd kan worden voor het uitvoeren van wettelijk verplichte DPIA's waarvoor geen capaciteit voorhanden is. Het verdient aanbeveling in 2022 als organisaties hier keuzes in te maken, eventueel in samenhang met het implementatievraagstuk rondom het risicoanalyseproces, en dit kader vervolgens toe te passen op de planning van DPIA's voor 2022 en verder.

In 2021 hebben de drie gemeentes ervaring opgedaan met de vastlegging van DPIA's, het uiteindelijke doorvoeren van de resultaten van een DPIA in het werkproces in de lijn en het nemen van beheersmaatregelen. Ondanks dat er tooling is aangeschaft voor het bijhouden van de mate van AVG-compliance op werkprocesniveau wordt de voortgang als het gaat om opvolging van beheersmaatregelen nog niet standaard gedocumenteerd voor geregistreerde verwerkingen. Dit komt mede doordat deze tooling achteraf niet aan de verwachtingen en wensen van de Privacy Officer blijkt te voldoen. Het gebrek aan registratie zorgt voor onvoldoende overzicht als het gaat om de waarborgen op werkprocesniveau en bemoeilijkt het afwikkelen en monitoren van de resultaten van DPIA's. Het advies is om in 2022 een werkwijze te ontwikkelen waarmee veranderingen in de AVG-compliance ten gevolge van adviezen en risicoassessments overzichtelijk kunnen worden geregistreerd.

Datalekken

Bij datalekken gaat het om het vrijkomen, wijzigen of vernietigen van persoonsgegevens zonder dat dit de bedoeling is. Datalekken zijn niet alleen een risico voor de gemeente die het betreft, maar ook vooral voor de personen waar de gegevens van zijn. De meeste datalekken die zich in de drie gemeentes voordeden in 2021 vielen in de categorie 'persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger'. Het betreft meestal een verkeerde adressering van e-mail of post. Bijvoorbeeld

stukken van een andere persoon die in een verkeerde envelop belanden en zo worden verzonden. Dit kan vervelende gevolgen hebben, zeker als het gaat om gevoelige informatie of kwetsbare personen. Mede om die reden is en blijft het van belang dat medewerkers op de risico's bij het versturen van persoonsgegevens worden gewezen en goed worden geïnstrueerd.

Om het afhandelen van een incident zo goed en zo adequaat mogelijk te kunnen doen hebben de drie gemeentes in 2018 een geactualiseerde procedure meldplicht datalekken vastgesteld. Deze procedure beschrijft de stappen die voor en na het melden van een datalek door de verschillende actoren moeten worden doorlopen. Het omvat het nemen van maatregelen om het datalek te dichten om de schade zo beperkt mogelijk te houden, maar ook het nemen van preventieve maatregelen om datalekken in de toekomst te voorkomen. In 2021 is het formulier voor incidentmeldingen geactualiseerd en is er een Cybercrisisplan voor de drie gemeentes opgesteld. Het verdient aanbeveling bij het vaststellen en oefenen met dit plan in 2022 de doelmatigheid en doeltreffendheid van de procedure meldplicht datalekken te betrekken en deze procedure te evalueren. Daar waar nodig is het raadzaam deze procedure opnieuw te actualiseren.

Bewustwording

De afgelopen jaren is er in de drie gemeentes door middel van de inzet van verschillende communicatiekanalen aandacht geschonken aan hoe medewerkers om moeten gaan met de persoonsgegevens waar zij dagelijks mee werken. Eenmalige acties zijn echter niet voldoende om gedragsverandering op dit gebied te borgen. In 2021 is daarom een start gemaakt met het uitvoeren van een plan voor communicatie en bewustzijn rondom privacy en gegevensbescherming in DOWR-verband. Structurele aandacht voor communicatie en bewustzijn dient het reeds opgebouwde kennisniveau te verbreden, bijvoorbeeld daar waar het herkennen van AVG-verzoeken betreft, maar ook nieuwe kennis te introduceren. Denk daarbij bijvoorbeeld aan kennis over de toepassing van bepaalde algoritmes nu er steeds meer nieuwe technologieën beschikbaar komen. Er is in 2021 voor gekozen om in DOWR-verband gebruik te gaan maken van NanoLearning. Inmiddels krijgen alle medewerkers van Deventer, Olst-Wijhe en Raalte om de drie weken een minicursus van 1-3 minuten toegestuurd waarbij ze door middel van een stukje tekst, een video, een afbeelding of een korte opdracht iets leren over privacy en informatieveiligheid. Aangezien dit slechts een basisniveau van bewustzijn stimuleert, bij reeds ingewerkte medewerkers, en niet alle medewerkers even gevoelig zullen zijn voor deze vorm van leren, is het advies om naast het gebruik van dit programma in 2022 ook op andere manieren planmatig het bewustzijn rondom deze onderwerpen te vergroten dan wel te verstevigen.

Rechten van betrokkenen

Onder de AVG zijn de zogenoemde rechten van betrokkenen versterkt. Dit recht houdt onder meer in dat burgers inzage kunnen krijgen in hun eigen persoonsgegevens. De AVG schrijft voor dat dit per ommegaande moet gebeuren, doch uiterlijk binnen één maand. Het besluit op een verzoek kan in complexe gevallen met twee maanden worden verdaagd. In 2021 werden er in Deventer 12 aanvragen, in Olst-Wijhe 3 aanvragen en in Raalte 1 aanvraag ingediend in het kader van 'rechten van betrokkenen'. Al deze AVG-verzoeken zijn binnen de wettelijke termijnen afgewikkeld.

Medewerkers van de drie gemeentes die aan de behandeling van een dergelijk verzoek hebben meegewerkt weten inmiddels hoe zij een verzoek kunnen herkennen en wat zij moeten doen op het moment waarop zij een dergelijk verzoek ontvangen. Het is raadzaam om in 2022 structureel aandacht te vragen voor dit soort verzoeken door dit onderwerp in de drie inwerkprogramma's en binnen NanoLearning op te nemen. Zo wordt geborgd dat ook nieuwe medewerkers, managers en medewerkers die nog geen ervaring hebben met dit soort verzoeken kennis opdoen over de rechten die het daarbij betreft, de termijnen die moeten worden bewaakt en de manier van afhandeling.

Klachten

De AVG verplicht de gemeentes om de naam en contactgegevens van de FG te publiceren zodat de inwoners van Deventer, Olst-Wijhe en Raalte contact met deze functionaris kunnen opnemen. In 2021 hebben 11 personen van deze mogelijkheid gebruik gemaakt. Al deze vragen en klachten over de AVG zijn door de FG onderzocht en afgehandeld. De meeste van de vragen en klachten gaan over:

- Het toepassen van de AVG door de betreffende gemeente (bijvoorbeeld: 'ik heb een brief gekregen van een bepaalde partij, heeft deze partij mijn gegevens van de gemeente gekregen? En mag dat zomaar?')
- De wijze waarop de betreffende gemeente bepaalde persoonsgegevens gebruikt (bijvoorbeeld: 'wordt er wel veilig met mijn gegevens omgegaan?');
- Zorgen over de gevolgen van (mogelijke) datalekken (bijvoorbeeld: 'ik heb het idee dat er misbruik is gemaakt van mijn gegevens, zijn deze wellicht afkomstig van een lek bij de gemeente?').

De aard van de vragen en klachten ten opzichte van eerdere jaren laat zien dat mensen zich steeds meer bewust zijn van het datagebruik van gemeentes en zich vaker afvragen wat de gemeente met hun persoonsgegevens doet.

Privacy by design

In 2021 is er een eerste stap gemaakt als het gaat om het verder integreren van privacy bij de inkoop van een product of dienst, het toepassen van de inkoopstrategie in DOWR-verband en het eventueel doorlopen van aanbestedingsprocedures. Het is inmiddels gebruikelijk om bij projecten die buiten de i-uitvoeringsplannen om in de regiegroep DOWR worden besproken een businesscase mét een advies van de Privacy Officer en Information Security Officer te overleggen. Omdat deze projecten zich dikwijls nog in de opstartfase bevinden, kan er in sommige gevallen op dat moment nog niet beoordeeld worden of de ingekochte producten en diensten ook daadwerkelijk in de naleving van de AVG voorzien. Het gestructureerd beoordelen van nieuwe initiatieven zorgt er wel voor dat nieuwe projecten op tijd in het vizier van de Privacy Officer en Information Security Officer komen. Verder zijn de standaard privacy passages die opgenomen worden in het programma van eisen bij aanbestedingen in DOWR-verband in 2021 geactualiseerd. Het verdient aanbeveling om in 2022 te blijven monitoren of deze bij inkoop gehanteerde waarborgen er ook daadwerkelijk voor zorgen dat er bij de ontwikkeling van nieuwe producten en diensten voldoende rekening wordt gehouden met de naleving van de AVG.

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Ontwikkelingen

Digitale overheid

In de gemeentes Deventer, Olst-Wijhe en Raalte groeit het besef dat persoonsgegevens en andere gegevens nuttig zijn voor een brede(re) inzet, bijvoorbeeld als het gaat om data gedreven werken en het monitoren van het realiseren van beleidsdoelstellingen. Hiermee groeit ook de ambitie van de drie organisaties om deze data slimmer in te gaan zetten om het beleid en de dienstverlening te verbeteren. Zij het ieder in zijn eigen tempo.

Daar is niets op tegen. Als overheid wil je niet achterblijven in digitalisering. Randvoorwaarde vanuit de AVG is wel dat de drie gemeentes daarbij verantwoord omgaan met persoonsgegevens en de daarbij gekozen technologie toepassen op een wijze die uitlegbaar is. Dat betekent ook dat de AVG bij dergelijke trajecten van begin af aan moet worden meegenomen. Privacy mag daarbij niet als sluitstuk worden gezien. Toepassingen dienen eerlijk, transparant en rechtvaardig te zijn. Dit zal ook door de organisaties moeten kunnen worden aangetoond. Vanuit de functie van FG wordt deze ontwikkeling nauwgezet gevolgd. Het advies is de in DOWR-verband opererende privacy- en informatieveiligheidsfunctionarissen in 2022 zo veel mogelijk te betrekken bij dit soort voorgenomen verwerkingen. Naast dat het verplicht is bij de ontwikkeling of wijziging van producten en diensten privacy mee te nemen, vergt het doen van aanpassingen achteraf vaak meer kosten en inspanning dan wanneer privacy waarborgen al tijdens de ontwikkelfase zijn geïmplementeerd en toegepast.

Wet politiegegevens

De auditverplichting die organisaties als werkgever onder de Wet politiegegevens hebben (Wpg) is met ingang van 1 januari 2019 van kracht geworden. Deze wet verplicht de drie gemeentes vanaf 2021 elke vier jaar een externe Wpg-audit te laten uitvoeren en de resultaten daarvan naar de toezichthouder, de AP, te sturen. De controle ziet toe op hoe het verwerken van politiegegevens door buitengewoon opsporingsambtenaren (boa's) is georganiseerd, de maatregelen die daarop van toepassing zijn en de werking van deze maatregelen. De drie organisaties hebben in 2021 een externe auditor ingeschakeld die een preaudit heeft uitgevoerd. De AP heeft de aanleveringstermijn van het eerste Wpg-auditrapport inmiddels verlengd tot en met 31 december 2022. De echte audit staat voor 2022 gepland.

Met de extra tijd die de AP heeft gegeven, hoopt zij organisaties de kans te geven om verbeterplannen op te stellen en hercontroles uit te voeren. Mocht er uit de audit volgen dat er bij (één van) de drie gemeentes niet (volledig) wordt voldaan aan de Wpg dan moet er binnen één jaar een hercontrole worden uitgevoerd. Zorgvuldigheid is dus van groter belang dan snelheid. De extra tijd wijzigt de onderzoeksperiode echter niet. Dit blijft de periode tot en met het jaar 2021. Ontwikkelingen die zich daarna hebben voorgedaan kunnen in het auditrapport in een afzonderlijke paragraaf opgenomen worden, maar deze veranderen niets aan het wel of niet voldoen aan de Wpg. Het is aan

te bevelen in 2022 als organisaties aan de hand van de auditrapporten keuzes te maken over de inzet van de huidige privacyfunctionarissen bij het verder implementeren van de Wpg en het wel of niet prioriteren van deze werkzaamheden ten opzichte van de werkzaamheden onder de AVG. Het is raadzaam de vraagstukken die hierboven genoemd zijn omtrent de inzet van deze functionarissen onder de AVG daarbij te betrekken.

Conclusie

De AVG is een omvangrijke en gecompliceerde wet, die om structurele inzet vraagt van bestuur, management en medewerkers. Uit de rapportage komt naar voren dat de afgelopen jaren en in 2021 flinke stappen zijn gezet, maar ook dat er nog veel onderhanden werk is. Het is daarbij cruciaal dat er voldoende capaciteit beschikbaar is om de benodigde werkzaamheden ook daadwerkelijk te kunnen uitvoeren. Ondanks dat de organisaties zich in 2021 hebben ingespannen, bleek dit laatste bij de huidige capaciteit toch lastiger te zijn dan verwacht waardoor was te zien dat werkzaamheden in de tijd uitliepen.

Het doel zou dan ook moeten zijn in 2022 als organisaties tot een accentverschuiving te komen van een grotendeels reactieve naar een meer proactieve houding ten opzichte van de aanpak bij privacy. Hierbij wordt ingezet op privacy als belangrijke randvoorwaarde en kans voor succesvolle innovatie. Voldoen aan de AVG vraagt om een verandering in het denken en handelen van iedereen die met persoonsgegevens werkt. Dit is een ontwikkeltraject binnen de drie organisaties dat nog niet is afgerond. Er liggen nog flinke uitdagingen voor de komende jaren.

Verklarende woordenlijst

Autoriteit Persoonsgegevens (AP)
Dit is de externe toezichthouder binnen Nederland met betrekking tot de uitvoering van de AVG.

Betrokkene
De persoon waarvan persoonsgegevens worden verwerkt.

Data Protection Impact Assessment (DPIA)
Een instrument om privacy risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is verplicht voor 'risicovolle verwerkingen'. De AVG geeft aan voor welke categorieën van verwerkingen een DPIA verplicht is. Daarnaast heeft de Autoriteit Persoonsgegevens een aanvullend overzicht opgesteld waarin is geconcretiseerd in welke gevallen de organisatie verplicht is een DPIA uit te voeren.

Meldplicht datalekken
Als een datalek ernstige nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkenen moet het datalek binnen 72 uur na ontdekking worden gemeld bij de Autoriteit Persoonsgegevens. Dit wordt de meldplicht van datalekken genoemd.

Persoonsgegevens
Een persoonsgegeven is alle informatie, op wat voor manier ook, die iets zegt over een persoon. Bijvoorbeeld een naam, (mail)adres, woonplaats of geboortedatum, maar ook een loginnaam of een IP-adres.

Rechten van betrokkenen
Onder de AVG hebben mensen mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Het gaat om het recht op inzage, het recht op rectificatie en aanvulling, het recht op verwijdering, het recht op vergetelheid, het recht op beperking van de verwerking, het recht op een menselijke blik bij besluiten, het recht op dataportabiliteit, het recht om bezwaar te maken tegen de gegevensverwerking en het recht op duidelijke informatie over wat de gemeente met persoonsgegevens doet.

Verwerken van persoonsgegevens
Dit is in feite alles wat de gemeente doet met persoonsgegevens. Bijvoorbeeld het verzamelen, vastleggen, structureren, opslaan, wijzigen, opvragen of bekijken van persoonsgegevens.

Verwerkingsverantwoordelijke
Het gaat bij dit begrip om een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In deze rapportage gaat het bij de verwerkingsverantwoordelijke om het college van burgemeester en wethouders van de drie gemeentes.

Verwerkingsregister
Een gemeente is verplicht een register bij te houden van alle verwerkingen van persoonsgegevens. Dit register moet continu actueel worden gehouden. In het verwerkingsregister staan onder meer per structurele verwerking de verwerkingsdoeleinden, een beschrijving van de categorieën persoonsgegevens en de beoogde bewaartermijnen van persoonsgegevens.