

Jaarverslag 2024

Functionaris Gegevensbescherming

Datum: 7-2-2025

Functionaris: Mr. N.J. Mookhoek CIPP/E

Deze rapportage is gebaseerd op het model “FG Jaarverslag (AVG en WPG)- Handleiding format” van de Informatie Beveiligings Dienst (IBD) van de VNG.

Het verslag wordt ter informatie aangeboden aan het College van Burgemeesters en Wethouders van de gemeente, in hun rol als verwerkingsverantwoordelijke voor de persoonsgegevens die de gemeente verwerkt.

Het verslag is opgesteld door de huidige FG die deze rol sinds 1 oktober jl. heeft. In het verslag zijn de bevindingen van de vorige FG meegenomen.

Versiebeheer

Versie	Datum	Beschrijving
1.0	22-1-2025	Eerste versie
1.1	6-2-2025	Tweede versie met input privacy team

1. Inhoudsopgave

2. Managementsamenvatting.....	4
3. Inleiding	
4. Deel A Jaarverslag AVG.....	5
3.1 Terugblik 2024	
3.2 Vooruitblik 2025	
5. Deel B Jaarverslag WPG.....	8
4.1 Terugblik 2024	
4.2 Vooruitblik 2025	
6. Ontwikkelingen.....	9

2. Managementsamenvatting

Het algemene beeld is dat de bescherming van persoonsgegevens binnen de Gemeente Gouda voldoende is. Medewerkers en Directie/ management zijn zich over het algemeen bewust van de persoonsgegevens waar ze mee om gaan en de vereisten die dat met zich meebrengt. Op enkele plekken bij management en proceseigenaren kan het bewustzijn nog (verder) worden vergroot. De inbreng van het privacy team in projecten vindt weliswaar plaats, maar vaak op ad hoc basis, er is geen gestructureerde werkwijze voor.

In 2024 is het privacy beleid vernieuwd. In 2025 kan dit als het herschreven is naar het IBD model naar het College ter vaststelling. Deze vaststelling kan als katalysator werken voor het bewustzijn over de bescherming van de persoonsgegevens.

De vereiste AVG documentatie die nodig is om de inspanningen aantoonbaar te maken, is aanwezig. Het register van verwerkingsactiviteiten is in 2024 gereed gekomen en zou in 2025 geopenbaard kunnen worden.

In 2024 is aan de hand van de lijst van “must have DPIA’s” van de VNG een planning gemaakt voor de uitvoering van DPIA’s. Daarin is de revisie van reeds uitgevoerde DPIA’s mee genomen.

Voor de stand van zaken met betrekking tot de implementatie van de Wpg en Bpgboa heeft een extern bureau aan het begin van het jaar een audit gehouden. Uit deze audit kwamen een aantal verbeterpunten, daarvoor is een verbeterplan opgesteld. Er is een begin gemaakt met de uitvoering van de verbeterpunten. Deze acties zullen in 2025 doorlopen.

Aanbevelingen

Op basis van het verslag doe ik als FG de volgende aanbevelingen:

- Overweeg om het register van verwerkingsactiviteiten te openbaren. Hierdoor zet de gemeente Gouda weer een stap in de transparantie over de gegevens die zij van haar inwoners verwerkt.
- Als dat er nog niet is: maak een meerjarenplan om de AI geletterdheid van medewerkers en organisatie te ontwikkelen en te borgen.
- Maak een aanpak om daar waar nodig het bewustzijn over gegevensverwerking bij management en proceseigenaren te vergroten.
- Zorg dat de betrokkenheid van het privacy team bij projecten waar gegevensverwerking plaats vindt, structureel georganiseerd wordt.

3. Deel A AVG

3.1 Terugblik 2024

3.1.1 Beleid

In 2024 is een start gemaakt met het updaten van het privacy beleid dat uit 2018 dateert. Dit beleid beschrijft hoe de Gemeente Gouda om gaat met de persoonsgegevens die zij verwerkt. Naast de principes en uitgangspunten die daarbij gehanteerd worden, zijn ook de rollen en verantwoordelijkheden beschreven in het Three Lines model. Dit model geeft aan wie voor welke taak met betrekking tot privacy verantwoordelijk is.

Het concept beleid is besproken in het privacy team en gereviewed door de FG. De conclusie hiervan is dat het beleid voor een efficiënt vervolg en implementatie omgezet moet worden naar het model van de IBD van de VNG.

3.1.2 Processen

Register verwerkingsactiviteiten

In 2024 zijn de werkzaamheden voor het Register van verwerkingsactiviteiten afgerond. Daarmee heeft de gemeente een volledig en up-to-date register en is op een belangrijk punt voldaan aan de vereisten van de AVG.

DPIA's

Volgens opgave zijn sinds 2018 32 DPIA's uitgevoerd. De FG heeft maar op 10 hiervan advies gegeven. Van de uitgevoerde DPIA's zijn 24 niet meer herzien sinds ze zijn opgesteld. Afhankelijk van de gesignaleerde risico's, zouden de uitgevoerde DPIA's binnen 1, 2 of 4 jaar herzien moeten worden.

In het najaar heeft de VNG een lijst met zogenaamde "must have DPIA's" uitgebracht. Deze lijst is onder de aandacht gebracht van de senior juristen privacy met het doel deze te delen met de organisatie, management en proceseigenaren.

Eind 2024 is een planning gemaakt voor het uitvoeren van de DPIA's op deze lijst en het uitvoeren van de benodigde revisies. Er is een start gemaakt met de uitvoering daarvan.

Rechten betrokken

In 2024 hebben 14 betrokkenen (degene van wie gegevens worden gebruikt) een beroep gedaan op zijn/ haar rechten uit de AVG.

In alle gevallen betrof het een beroep op het recht van inzage. In 1 geval is ook een beroep gedaan op het recht van verwijdering van de persoonsgegevens.

Deze verzoeken zijn afgehandeld, een enkele loopt nog door in 2025.

Datalekken

In 2024 zijn 45 meldingen van een datalek geregistreerd.

In 8 gevallen werd de impact op de privacy van de betrokkenen dermate groot geacht dat er melding bij de Autoriteit Persoonsgegevens is gedaan. In 1 geval was dit in de vorm van een voorlopige melding. Voorzover bekend is deze inmiddels ingetrokken.

3.1.3 Organisatorische inbedding

Voor een goede bescherming van de persoonsgegevens is het noodzakelijk dat alle medewerkers van de Gemeente bekend zijn met het belang van het beschermen van persoonsgegevens van de inwoners en de beginselen van de AVG.

In 2024 is aan alle medewerkers een online training van studytube op het gebied van privacy en informatiebeveiliging aangeboden.

Nieuwe medewerkers worden in hun onboarding programma getraind op het gebied van de AVG. Deze sessies vinden elke maand plaats.

Daarnaast worden met regelmaat afdelingen bezocht om de algemene vereisten van de AVG praktisch te koppelen aan hun praktijk en de materie waarmee zij werken.

Tevens is samen met de CISO besloten een online bewustwordingsprogramma aan te gaan bieden. De selectie van het programma heeft inmiddels plaats gevonden. In 2025 zal hiermee gestart worden. Het programma loopt 1 jaar en zal dan worden geëvalueerd.

Naast bewustzijn bij medewerkers is kennis en bewustzijn bij Directie, Management en procesverantwoordelijken van belang. De AVG vereist dat het gemeentebestuur en in mandaat de managers/ procesverantwoordelijken aan kunnen tonen in control te zijn over de persoonsgegevens die de gemeente van haar inwoners verwerkt.

Dat betekent dat zij zicht moeten hebben op de processen met persoonsgegevens en moeten weten of die aangepast moeten worden omdat ze niet voldoen aan de AVG.

De Directie onderkent het belang van een goede bescherming van persoonsgegevens en de noodzaak te voldoen aan de AVG.

Het beeld met betrekking tot het management/procesverantwoordelijken is meer wisselend: sommigen zijn doordrongen van de noodzaak op andere plekken kan dit verbeterd worden.

In 2024 zijn medewerkers van het privacy team regelmatig aan geschoven bij projecten waar aspecten van de bescherming van persoonsgegevens een rol speelden. Hoewel dit een mooie eerste stap is, gebeurde dit vaak ad hoc. Hier kan nog verbetering plaatsvinden door te komen tot een meer gestructureerde werkwijze.

3.2 Vooruitblik 2025

3.2.1 Beleid

Op het moment van schrijven van dit verslag is er een concept versie van het beleid aangeboden aan het privacy team. Als dit herschreven is naar het IBD model is het voornemen het herijkte beleid in Q2 voor te leggen aan de directie. De volgende stap moet dan zijn dat het beleid wordt vastgesteld door het College van B&W in haar rol als verwerkingsverantwoordelijke.

3.2.2 Processen

Register verwerkingsactiviteiten

Nu het Register afgerond is, zou overwogen kunnen worden dit te publiceren op de website. Met publicatie maakt de gemeente Gouda een stap op het gebied van transparantie van de verwerking van persoonsgegevens.

DPIA's

In 2025 zal verder gewerkt worden aan het uitvoeren van DPIA's dan wel reviseren van bestaande DPIA's volgens de opgestelde uitvoeringsplanning. De planning zal in Q1 ook worden gedeeld met de Directie.

Rechten betrokken

Voor 2025 worden hier geen bijzonderheden verwacht. Een groot inzageverzoek uit 2024 zal door het team in overleg met de Directie in 2025 verder afgehandeld worden. Dit zal net als in 2024 de nodige capaciteit kosten. Daarnaast zullen nieuwe inzageverzoeken worden afgehandeld.

Datalekken

In 2025 staan geen extra acties gepland om het onderwerp datalekken onder de aandacht van de organisatie te brengen. Vanzelfsprekend zullen de gemelde datalekken door het team worden afgehandeld.

3.2.3 Organisatorische inbedding

De sessies in het kader van het onboardingsprogramma van nieuwe medewerkers zullen in 2025 worden gecontinueerd. Hetzelfde geldt voor de online studie mogelijkheden. Daarnaast zal een nieuw programma worden gestart over privacy en informatiebeveiliging.

In de terugblik over 2024 is geconstateerd dat de relevantie van de bescherming van persoonsgegevens bij management en proceseigenaren nog wisselend is. Het verdient het aanbeveling om in 2025 te kijken in hoeverre het bewustzijn bij deze doelgroep naar een hoger niveau kan worden gebracht.

Daarnaast is geconstateerd dat het privacy team op ad hoc basis regelmatig wordt betrokken bij projecten. Het verdient aanbeveling in 2025 hiervoor tot een meer gestructureerde aanpak te komen.

4. Deel B WPG

4.1 Terugblik 2024

In 2024 is op basis van de heraudit WPG in 2023 een verbeterplan opgesteld. Per domein waar Boa's werkzaam zijn en politiegegevens worden verwerkt (leerlingzaken, sociaal domein (sociaal rechercheurs) en stadstoezicht) zijn de noodzakelijke acties gepland. Uit de audit volgen ook een aantal acties voor het privacy team.

Het verbeterplan strekt zich uit over 2025 en 2026. Bij het opstellen van het plan zijn de punten die nog beschreven moeten worden in de jaren gepland.

De punten waarvan alleen de werking dus de implementatie en de toepassing moet worden aangetoond zijn niet in de planning mee genomen.

4.2 Vooruitblik 2025

Het jaar 2025 zal vooral in het teken staan van het uitvoeren van de punten uit het verbeterplan.

5. Ontwikkelingen

Artificial Intelligence

Een van de belangrijkste ontwikkelingen op dit moment is onmiskenbaar de rol van Artificial Intelligence (AI). De ontwikkeling van applicaties met AI heeft een grote vlucht genomen. De Europese AI Act beoogt een juridisch kader te geven om de ontwikkeling en het gebruik van AI te faciliteren. De Act stelt onder andere verplicht dat organisaties met ingang van 2 februari 2025 aan de slag gaan met AI-geletterdheid.

AI-geletterdheid betekent dat medewerkers een basiskennis hebben van wat AI is, hoe het werkt en welke toepassingen relevant zijn voor hun werk. Het gaat dus niet om de (technische) werking van AI-systemen, maar om inzicht in hoe AI gebruikt kan worden om problemen op te lossen en processen te verbeteren. Medewerkers moeten ook kritisch kunnen nadenken over de ethische implicaties van AI, zoals privacy, bias en transparantie.

De gemeente Gouda is momenteel aan het onderzoeken of er binnen een afgesloten AI kader met één of meerdere pilots kan worden gestart. Het privacy team is hier nauw bij betrokken. Daarnaast mogen medewerkers AI toepassingen zoals ChatGPT en Microsoft 365 Copilot gebruiken om hen te ondersteunen bij hun werk.

De gemeente kan ook nog op een andere manier te maken krijgen met AI: veel leveranciers van applicaties gebruiken AI in hun toepassingen. Als de Gemeente applicatie met AI gebruikt, zal zij ook aan de AI Act moeten voldoen. De AI Act kent immers een breed werkingsgebied: niet alleen ontwikkelaars, maar ook gebruikers vallen onder deze wetgeving.

Data ethiek: de AVG voorbij

Data-ethiek houdt in dat de organisatie nadenkt over hoe ze wil dat er met data wordt omgegaan. Data-ethiek geeft dus geen regels en voorschriften, maar bevordert dat de organisatie zelf kritisch nadenkt over wat goed is om te doen met data.

Data-ethiek is dus breder dan alleen persoonsgegevens, maar zal daar in de gemeente Gouda wel vaak betrekking op hebben. De AVG biedt vanzelfsprekend een kader dat

helpt om goed met persoonsgegevens om te gaan. Echter, de AVG kent veel open normen en bovendien gaan de technologische ontwikkelingen, zoals de boven beschreven AI, dermate snel dat niet alles met regelgeving kan worden opgelost. Data-ethiek komt daarbij te hulp door na te denken en met elkaar te bespreken hoe de gemeente om wil gaan met de enorme hoeveelheid data die zij heeft.