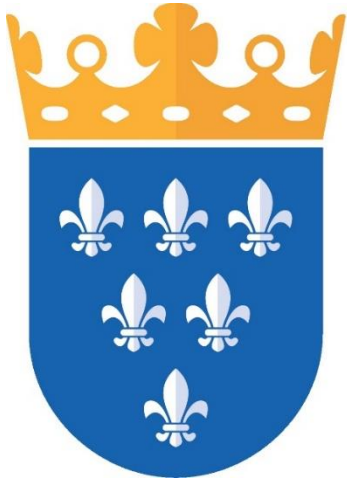




**Gemeente
Scherpenzeel**

Jaarverslag Gegevensbescherming

1 mei 2023 tot en met 31 december 2024

GEMEENTE SCHERPENZEEL

Datum: 6 februari 2025

Functionaris: M.M.S. ten Hoven-van de Waerd

1. Inhoudsopgave

2.	Managementsamenvatting	2
3.	Inleiding	5
	Leeswijzer jaarverslag	5
4.	Deel A: AVG	6
4.1.	AVG-dashboard	6
4.2.	Deel 1. Terugblik op 2023/2024.....	7
4.3.	Deel 2. Vooruitkijken naar 2025.....	10
5.	Deel B: Wpg	11
5.1.	Inleiding	11
5.2.	Wpg-dashboard	11
5.3.	Bevindingen en aanbevelingen jaar 2025	12
5.4.	Audit Wpg	12
5.5.	Vooruitblik jaar 2025	12
6.	Deel C: Ontwikkelingen.....	13

2. Managementsamenvatting

Dit jaarverslag maakt onderscheid tussen de periode 1 mei 2023 tot en met 31 mei 2024 en 1 juni 2024 tot en met 31 december 2024.

Periode 1 mei 2023 tot en met 31 mei 2024

Tot 1 juni 2024 bestond het privacyteam uit een Chief Information Security Officer (CISO), een externe Privacy Officer (PO) en een externe Functionaris Gegevensbescherming (FG).

Mede vanwege een beperkt aantal beschikbare werkuren in de week functioneert de gemeente Scherpenzeel niet op het gewenste volwassenheidsniveau volgens het borgingsproduct van de Informatiebeveiligingsdienst (IBD). Het is de wens van de gemeente Scherpenzeel om op volwassenheidsniveau 3 te werken waarbij de organisatie organisatiebreed aan privacy werkt en dit conform de wet- en regelgeving kan worden aangetoond.

De CISO en externe FG hebben zich tot 1 juni 2024 voornamelijk gericht op:

- * het afhandelen van inzageverzoeken, datalekken, informatieverzoeken jeugd;
- * het opstellen van verwerkersovereenkomsten;
- * het voeren van gesprekken namens de gemeente Scherpenzeel met de gemeente Oostzaan om kennis en ervaring te delen en mogelijk toe te passen binnen de eigen gemeente;
- * het voeren van gesprekken in verband met het formeren van een nieuw privacyteam (waaronder het analyseren van wensen, het opstellen van vacatureteksten, het voeren van sollicitatiegesprekken en het inwerken van het nieuwe privacyteam).

Ook is er aandacht geweest voor de Wet politiegegevens (Wpg). Met extern ingehuurd bureau BMC als PO hield de externe FG zich bezig met het analyseren van auditresultaten. Ook is er aandacht geschonken aan het bewustzijn binnen het team Wpg/OOV. In de praktijk bleek dit lastig vanwege het verloop in personeel binnen het team Wpg/OOV.

Periode 1 juni 2024 tot en met 31 december 2024

Op 1 juni 2024 is er een nieuw samengesteld privacyteam gestart in de gemeente Scherpenzeel. Dit team bestaat uit een Chief Information Security Officer (CISO), Privacy Officer (PO) en Functionaris Gegevensbescherming (FG).

Het nieuwe privacyteam startte met het invullen van het borgingsproduct van de IBD. Doel hiervan was bekijken hoe de gemeente Scherpenzeel er op privacyvlak voor stond. Er werd geconcludeerd dat de gemeente Scherpenzeel niet op volwassenheidsniveau 3 functioneert. Eind 2026 moeten rijksorganisaties echter een volwassenheidsniveau tussen 3 en 4 halen.

Op basis van de uitkomsten van het borgingsproduct is er een jaarplan samengesteld. Dit jaarplan is ingedeeld in een actielijst per kwartaal. Het herzien van het privacybeleid en het Wpg beleid is onder andere hierin opgenomen. Na het herzien van het beleid volgt het herzien van de procedures.

Wekelijks is er een IB&P overleg tussen de CISO, PO en FG. Het eerste half jaar sloot de teamleider van team Data en Control hierbij aan. In dit IB&P overleg spreken de CISO, PO en FG over de voortgang van genomen acties en over actualiteiten binnen de organisatie (casussen, datalekken, (pré-)DPIA's, verwerkersovereenkomst enzovoort).

Eén keer in de zes weken vindt er met het privacyteam en de teamleider een strategisch overleg plaats. In dit strategisch overleg praat team IB&P de teamleider bij over de voortgang van de geplande acties, de bevindingen van de genomen acties en over actualiteiten.

Het privacyteam constateerde dat bewustwording van de medewerkers van de gemeente Scherpenzeel aandacht nodig heeft. Zichtbaarheid en vindbaarheid van het team privacy is belangrijk.

Om het bewustzijn van de medewerkers van de gemeente Scherpenzeel te verhogen koos het privacyteam voor herinvoering van Sir Askalot (Recourse). Elke medewerker van de gemeente Scherpenzeel krijgt op dinsdag een email met vraag over privacy of beveiliging. Het privacyteam vraagt hiermee herhaaldelijk aandacht voor informatiebeveiliging en privacy. Dit is ook verplicht conform art. 7.2.2 van de Baseline Informatiebeveiliging Overheid (BIO).

Naast bovenstaande hield het privacyteam zich bezig met ad-hoc vragen vanuit de organisatie, datalekken, verwerkersovereenkomsten en (pré-)DPIA's.

Verwachting voor 2025

De ambitie van het privacyteam is het volwassenheidsniveau van de gemeente Scherpenzeel verhogen naar minimaal niveau 3. Hiervoor is medewerking nodig van het managementteam en het college van burgemeester en wethouders van de gemeente Scherpenzeel.

Het privacyteam zal in 2025 deelnemen aan een MT-overleg. Doel is het privacy bewustzijn van de MT-leden verhogen, zodat zij privacy bewustzijn kunnen uitdragen naar hun eigen team en binnen de organisatie.

Naast het volgen van het jaarplan zal het privacyteam onder andere aandacht besteden aan de dag van de privacy (28 januari 2025) en de dag van de informatiebeveiliging (30 november 2025).

Ook vindt in 2025 de externe Wpg audit plaats. Tot slot wordt er tijd geïnvesteerd in ad-hoc vragen vanuit de organisatie, datalekken, verwerkersovereenkomsten en (pré-)DPIA's. De FG dient daarnaast toezichtacties te houden.

3. Inleiding

De Algemene verordening gegevensbescherming (AVG) omschrijft de taken van de Functionaris Gegevensbescherming (FG):

- de verwerkingsverantwoordelijke of de verwerker en de werknemers die persoonsgegevens verwerken, informeren en adviseren over hun verplichtingen (bijvoorbeeld door middel van een data protection impact assessment (DPIA));
- toezien op de naleving van de AVG en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens (waaronder het toewijzen van verantwoordelijkheden, bewustmaking, opleiding van betrokken personeel en audits);
- advies verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan;
- samenwerken met de toezichthoudende autoriteit (AP);
- optreden als contactpunt voor het AP inzake met verwerking verband houdende aangelegenheden en overleg plegen over enige andere aangelegenheid.

Het is aan de FG om bij het uitvoeren van zijn taken rekening te houden met het aan verwerkingen verbonden risico en met de aard, de omvang, de context en de verwerkingsdoeleinden. De FG voert zijn werkzaamheden grotendeels uit met de Chief Information Security Officer (CISO) en de Privacy Officer (PO).

Doel van dit jaarverslag is om aan het gemeentebestuur van de gemeente Scherpenzeel inzicht te geven in de werkwijze van de FG. Het verslag laat zien hoe de FG de gemeente Scherpenzeel begeleidt in het voldoen aan de privacywetgeving. Ook wordt er met dit jaarverslag verantwoording afgelegd aan het gemeentebestuur aangezien het gemeentebestuur eindverantwoordelijk is voor het verwerken van persoonsgegevens binnen de gemeente Scherpenzeel.

Leeswijzer jaarverslag

Dit jaarverslag bestaat uit 3 onderdelen:

Deel A: betreft het verslag over de AVG;

Deel B: gaat over de bevindingen over de Wpg;

Deel C: relevante ontwikkelingen op het gebied van gegevensbescherming.

Aangezien zowel de AVG als de Wpg gaan over het beschermen van persoonsgegevens is er één jaarverslag. De opbouw van het verslag is grotendeels hetzelfde:

- Dashboard: stoplichtrapportage op basis van de thema's uit AVG en Wpg. Voor de AVG wordt hierbij verwezen naar de thema's uit het AVG borgingsproduct.
- Vervolgens worden per thema de bevindingen en aanbevelingen beschreven.

4. Deel A: AVG

4.1. AVG-dashboard

Onderstaand dashboard geeft het gemeentebestuur in één opslag een beeld van de stand van zaken rondom de naleving van de AVG binnen de gemeente Scherpenzeel.

Thema:	2022/2023	2024	2025
Borging AVG	Jaarverslag	Resultaat	Verwacht
 Beleid			
 Processen			
 Organisatorische inbedding			
 Rechten van betrokkenen			
 Samenwerking			
 Gegevensbescherming			
 Verantwoording			

Legenda:

	AANDACHT VEREIST VAN MANAGEMENT
	IN TE HALEN ACHTERSTAND
	OP SCHEMA

4.2. Deel 1. Terugblik op 2023/2024

Dit deel van de rapportage blikt terug op hetgeen de gemeente Scherpenzeel in 2023/2024 heeft bereikt. Ook vindt er een opsomming plaats van de werkzaamheden en bevindingen in deze periode door de FG.

4.2.1. Beleid

Het privacybeleid is een kader waarin de gemeente Scherpenzeel aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe de gemeente wenst om te gaan met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving.

In de formatie van een team privacy is geïnvesteerd door het gemeentebestuur. Het nieuwe privacyteam is gestart met het uitvoeren van het borgingsproduct. Naar aanleiding van het uitvoeren van het borgingsproduct is besloten om te starten met het herzien van het privacybeleid. Na het gereedkomen van het privacybeleid staat het herzien van de procedures op de planning.

4.2.2. Processen

De verwerkingen van persoonsgegevens door de gemeente Scherpenzeel dienen te voldoen aan de AVG. Dit houdt in dat de gemeente de werkprocessen waarin persoonsgegevens verwerkt worden moet toetsen en inrichten volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast kan de gemeente in bepaalde gevallen verplicht zijn om een (pré-) data protection impact assessment (DPIA) uit te voeren.

Het privacyteam heeft in 2024 acht (8) keer een pré-DPIA uitgevoerd. Eén van deze pré-DPIA's gaf aanleiding voor het uitvoeren van een DPIA.

4.2.3. Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat eenieder binnen de gemeentelijke organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en het creëren van bewustzijn.

Het privacyteam constateerde dat bewustwording van de medewerkers van de gemeente Scherpenzeel aandacht nodig heeft. Zichtbaarheid en vindbaarheid van het team privacy is belangrijk. Allereerst is er een algemeen mailadres voor het privacyteam gemaakt (privacy@scherpenzeel.nl) om zo de vindbaarheid van de medewerkers privacy te vergroten. Ten tweede investeerde de PO en FG tijd in kennismakingen met teamleiders en beleidsmedewerkers om zo beter zichtbaar te zijn en houden de CISO en PO voorlichtingsbijeenkomsten voor nieuwe medewerkers.

Om het bewustzijn van de medewerkers van de gemeente Scherpenzeel te verhogen koos het privacyteam voor herinvoering van Sir Askalot (Recourse). Elke medewerker van de gemeente Scherpenzeel krijgt op dinsdag een email met vraag over privacy of beveiliging. De medewerkers kunnen met het correct beantwoorden van de vraag punten verdienen en bij het behalen van een vastgesteld aantal punten een kleine traktatie ophalen bij het privacyteam. Het privacyteam vraagt hiermee herhaaldelijk aandacht voor informatiebeveiliging en privacy. Dit is ook verplicht conform art. 7.2.2 van de Baseline Informatiebeveiliging Overheid (BIO) waarin woordelijk staat: "Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie."

4.2.4. Rechten van betrokkenen

De gemeente Scherpenzeel dient degene van wie zij de persoonsgegevens verwerkt (betrokkene) zowel actief als passief te informeren over (de wijze van) het verwerken, de grondslag op grond waarvan dat gebeurt en de maatregelen die de gemeente neemt om onrechtmatige toegang en verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens. De gemeente heeft de plicht om de betrokkenen te wijzen op deze rechten en om er voor te zorgen dat de betrokkenen deze rechten ook daadwerkelijk kunnen uitvoeren.

Ook in 2024 maakte de gemeente Scherpenzeel gebruik van een extern bureau om te ondersteunen op het gebied van privacy. De inzet is vooral geleverd op verzoek in de tweede helft van 2024. Het externe bureau maakte een opzet voor een herzien cookiebeleid en voor de privacy verklaringen.

4.2.5. Samenwerking

De gemeente Scherpenzeel werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: het ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt hieronder. Deze verwerkingen dienen dan ook te voldoen aan de AVG. De gemeente Scherpenzeel maakt hierover afspraken met deze andere partijen. Dit gebeurt middels verwerkersovereenkomsten en het uitvoeren van een pré-DPIA of DPIA op deze voorgenomen verwerking.

4.2.6. Gegevensbescherming

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente Scherpenzeel passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er onder de AVG een meldplicht voor inbreuken met persoonsgegevens (privacyincidenten). Dit houdt in dat incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).

4.2.7. Verantwoording

De verantwoordelijkheid om aan te tonen of en in welke mate wordt voldaan aan de privacyregels ligt bij de gemeente zelf. Dit is in de AVG zo geregeld. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

4.2.8. Conclusie

In 2024 zijn er mooie stappen gezet. Een nieuw samengesteld privacyteam werkte aan bewustwording binnen de gemeente Scherpenzeel, aan het uitvoeren van pré-DPIA's en DPIA's, verwerkersovereenkomsten en waar nodig het oplossen van datalekken en phishing mails. Naar aanleiding van het borgingsproduct is een jaarplan voor 2025 opgesteld. Er is gestart met het herzien van het privacybeleid en na het gereedkomen worden de procedures geactualiseerd.

4.3. Deel 2. Vooruitkijken naar 2025

Dit deel van de rapportage bevat aanbevelingen voor 2025. Deze aanbevelingen komen voort uit het opgestelde jaarplan.

4.3.1. Beleid

Aanbevelingen:

- * herzien van het privacybeleid;
- * herzien van het cookiebeleid;
- * opstellen van een bewaar- en vernietigingsbeleid.

4.3.2. Processen

Aanbevelingen:

- * herzien van de privacyverklaringen;
- * herzien van de procedure datalekken;
- * opstellen van de procedure verwerkingen;
- * opstellen van de procedure pré-DPIA en DPIA;
- * opstellen van de rechten van betrokkenen;
- * werkprocessen nalopen.

4.3.3. Organisatorische inbedding

Aanbevelingen:

- * contact zoeken met OR;
- * introductie in het MT overleg;
- * driemaandelijks rapporten aan het MT;
- * monitoren gebruik Sir Askalot (Recourse);
- * jaarlijks langs bij de teams.

4.3.4. Rechten van betrokkenen

Aanbevelingen:

- * opstellen proces recht van betrokkenen.

4.3.5. Samenwerking

Aanbevelingen:

- * continueren van IB&P overleg één keer in de drie weken;
- * continueren van strategisch overleg één keer in de zes weken.

4.3.6. Beveiliging

Aanbevelingen: acties in overleg met CISO.

4.3.7. Verantwoording

Aanbevelingen:

- * opmaken jaarverslag over 2025.

5. Deel B: Wpg

5.1. Inleiding

De FG ziet toe op de naleving van de Wet politiegegevens (Wpg). Het college dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van politiegegevens. De FG rapporteert jaarlijks de bevindingen aan de hand van een jaarverslag.

5.2. Wpg-dashboard

Onderstaand dashboard moet het gemeentebestuur in één opslag een beeld geven van de stand van zaken rondom de naleving van de Wpg binnen de gemeente Scherpenzeel.

Het nieuwe privacyteam richtte zich in 2024 op de AVG. De Wpg kreeg vanwege tijdgebrek onvoldoende aandacht en zou in 2025 worden opgepakt. Het dashboard is daarom niet gevuld.

Thema:	2022/2023	2024	2025
Borging Wpg	Jaarverslag	Resultaat	Verwacht
Beleid			
Bewustwording			
Autorisatieproces			
Bewaartermijnen			
Verstrekken van persoonsgegevens			
DPIA			
Register van verwerkingen			
Auditverplichting			

Legenda:

	AANDACHT VEREIST VAN MANAGEMENT
	IN TE HALEN ACHTERSTAND
	OP SCHEMA

De taken van de FG voor de Wpg (artikel 36 van de Wet politiegegevens) zijn als volgt samengevat:

De FG voert periodiek controles uit op het naleven van de wettelijke verplichtingen die voortkomen uit de Wpg, waaronder de controle op:

1. het hebben van een beleid aangaande de uitvoering van de Wpg;
2. de bewustwordingsverplichting;
3. het autorisatieproces met betrekking tot het vastleggen van politiegegevens;
4. de kwaliteit en waarborging van de juistheid van de nauwkeurigheid van politiegegevens;
5. het verwerken van politiegegevens;
6. de bewaartermijnen;
7. het ter beschikking stellen en verstrekken van politiegegevens;
8. de controle op de informatiebeveiliging en de controle op het uitvoeren van een risicoanalyse;
9. het register voor verwerkingen;
10. de verplichtingen ten aanzien van de audit;

5.3. Bevindingen en aanbevelingen jaar 2025

De thema's van de Wpg (genoemd op pagina 11) verdienen in 2025 veel aandacht.

Er is een document samengesteld met openstaande acties met betrekking tot de Wpg implementatie. Team privacy gebruikt deze aanbevelingen bij het voldoen aan de eisen vanuit de Wpg.

5.4. Audit Wpg

Jaarlijks dient er een interne audit plaats te vinden met betrekking tot de Wpg. De interne audit moet voldoen aan de vereisten van de Wpg.

Eén keer in de vier jaar moet er een externe audit plaatsvinden. De externe audit staat voor 2025 op de planning.

5.5. Vooruitblik jaar 2025

Een procesbeschrijving handhaving is in concept voorbereid. Het document met openstaande acties met betrekking tot de Wpg implementatie kan dienen als leidraad. In 2025 vindt een externe audit plaats. Een interne audit vindt jaarlijks plaats. Een externe audit één keer in vier jaar. Voor de interne audit dient er een auditplan, auditplanning en auditrapportage opgesteld te worden. De FG dient toezichtacties te houden.

6. Deel C: Ontwikkelingen

Een aantal belangrijke ontwikkelingen zijn van invloed op de verwerking van persoonsgegevens. Hierbij valt te denken aan de steeds belangrijkere rol van automatische besluitvorming (AI en algoritmes). De gemeente Scherpenzeel moet intern bespreken hoe zij omgaat met automatische besluitvorming. Op de website van VNG en IBD wordt met regelmaat iets geplaatst over de ontwikkeling van AI en algoritmes. Ook verschijnt er met regelmaat een nieuwsbericht via de e-mail. Het is belangrijk om de VNG en IBD te volgen en om tips te bespreken en eventueel op te volgen.

Een andere belangrijke ontwikkeling is de verplichting om steeds vaker een pré-DPIA of DPIA uit te voeren. Het bijwerken van het verwerkingsregister is ook een belangrijke taak. Dit moet zorgvuldig plaatsvinden.

Het privacyteam volgt ontwikkelingen omtrent cookies. De AP (Autoriteit Persoonsgegevens) is niet gediend van het ongeoorloofd online volgen van personen. Het AP is in 2024 daarom een campagne gestart om het onrechtmatig verzamelen van gegevens via tracking cookies tegen te gaan. Bij een geconstateerde overtreding kan het AP een boete uitdelen. Het privacyteam is in 2024 gestart met herzien van de privacyverklaring voor cookies.

In 2025 vindt het aanscherpen van de eisen voor informatiebeveiliging plaats. De oorzaak hiervan is onder andere de invoering van de NIS2-richtlijn. Het evalueren van de huidige beveiligingsmaatregelen is daarom aan te raden. Ook is het daarom belangrijk om met ICT Veenendaal te overleggen over het waarborgen van de informatiebeveiliging.