Gemeente
Scherpenzeel

JAARVERSLAG 2025 FUNCTIONARIS GEGEVENSBESCHERMING

Aan: Het college van B&W en de Burgemeester
Van: Suzanne Pannemans (functionaris gegevensbescherming)
Datum: 30 januari 2026

Inhoud

Versiebeheer

Versie	Datum		Door
1.0	30-01-2026		Suzanne Pannemans

1. Inleiding

1.1 Waarom dit jaarverslag?

Een functionaris gegevensbescherming (FG)[1] is een onafhankelijk persoon die informeert, adviseert over en toezicht houdt op een zorgvuldige behandeling van persoonsgegevens door de organisatie. Deze functionaris is voor een gemeente wettelijk verplicht.

Het doel van deze functie is het bevorderen van de naleving van de kaders door middel van informeren, inspectie, waarheidsvinding, beoordeling en advisering. Vanaf april 2025 ben ik de FG van gemeente Scherpenzeel[2]. In dit jaarverslag[3] informeer ik u in uw rol als verwerkingsverantwoordelijke[4] over de stand van zaken, ontwikkelingen en aandachtspunten op het gebied van persoons- en politiegegevens.

1.2 Opbouw van dit jaarverslag

Dit verslag volgt de onderdelen in het AVG-borgingsproduct[5].

1. Beleid
2. Processen
3. Organisatorische inbedding
4. Rechten van betrokkenen
5. Samenwerking
6. Gegevensbescherming
7. Verantwoording

Het AVG-borgingsproduct is een toetsingskader. Op basis hiervan kan worden beoordeeld in hoeverre de organisatie in staat is om blijvend aan de privacywetgeving te voldoen. Als FG heb ik dit borgingsproduct ingevuld om een beeld te vormen in hoeverre de organisatie aan de privacywetgeving voldoet.

Informatiebeveiliging en privacy (IB&P) hebben raakvlakken en kunnen elkaar versterken. De organisatie pakt IB&P waar het kan in samenhang op. Daarom komt u in dit verslag vaker 'IB&P' tegen.

1.3 Kaders

Iedereen heeft 'recht op de eerbiediging van de persoonlijke levenssfeer'. Dit is een grondrecht[6]. Hieronder valt het huis, briefwisseling, communicatie, innerlijke leven, lichamelijke integriteit, niet te worden bespied of afgeluisterd en het recht op een zorgvuldige behandeling van persoonsgegevens.

Die zorgvuldige behandeling van persoonsgegevens is uitgewerkt in de Algemene Verordening Gegevensbescherming (AVG). Dit is Europese wetgeving. In Nederland staan aanvullende voorwaarden in de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

[1] Artikel 37, 39 en 39 AVG en 36 Wpg
[2] FG aanmelden bij de AP | Autoriteit Persoonsgegevens
[3] Artikel 38.3 AVG en 36.4 Wpg
[4] Artikel 4.7 AVG en 1f Wpg
[5] Borgingsproduct Informatiebeveiligingsdienst (VNG)
[6] Artikel 10 grondwet

Het college van B&W heeft buitengewoon opsporingsambtenaren (boa's) in dienst. De boa's hebben zowel toezichts- als opsporingstaken. Binnen de toezichtstaken worden persoonsgegevens verwerkt, waarop de AVG van toepassing is. Binnen de opsporingstaken worden politiegegevens verwerkt. Dit zijn persoonsgegevens die nodig zijn voor voorkoming en opsporing van strafbare feiten. Waar in dit verslag 'persoonsgegevens' staat, worden ook politiegegevens bedoeld.

Op politiegegevens is de Europese Richtlijn gegevensbescherming politie & justitie van toepassing. Deze richtlijn is in Nederland voor boa-organisaties onder meer geïmplementeerd in de volgende wetgeving:

- Wet politiegegevens (Wpg)
- Besluit politiegegevens (Bpg)
- Besluit politiegegevens buitengewoon opsporingsambtenaar (Bpgboa)
- Beleidsregel Buitengewoon opsporingsambtenaar
- Regeling periodieke audit politiegegevens

1.4 Samenvatting 2025

In 2025 is een nieuwe privacy officer (PO) gestart. Er was tijd nodig voor inwerken, kennis maken met de organisatie en onderzoek naar de huidige stand van zaken. Daarna zijn de PO en de chief information security officer (CISO) aan de slag gegaan met de voorbereidingen voor 2026 en 2027. Zo is er nu een strategisch IB&P-beleid, een IB&P-jaarplan 2026-2027 en kennis- en bewustzijnsplan.

1.5 Conclusie over 2025

De organisatie voldoet op dit moment niet aan de privacywetgeving. Zoals u in dit jaarverslag kunt lezen, zijn er nog aandachtspunten waarop verbeteringen nodig zijn.

Veel van deze verbeteringen zijn opgenomen in het IB&P-jaarplan 2025-2027 van de organisatie. Dit maakt dat ik er vertrouwen in heb dat de gemeente Scherpenzeel de komende twee jaar de juiste stappen zet om blijvend aan de privacywetgeving te voldoen.

1.6 Contact

Als u vragen heeft naar aanleiding van mijn jaarverslag of meer informatie wilt, kunt u contact met mij opnemen. Ik maak graag een afspraak met u.

Met vriendelijke groet,

Suzanne Pannemans
Externe functionaris gegevensbescherming voor gemeente Scherpenzeel
s.pannemans@scherpenzeel.nl

2. Beleid

Een gegevensbeschermingsbeleid[7] is verplicht voor organisaties met risicovolle of grootschalige verwerkingen van persoonsgegevens. Gemeente Scherpenzeel verwerkt gevoelige en bijzondere persoonsgegevens op redelijk grote schaal en van kwetsbare doelgroepen. Een beleid is daarom verplicht.

Stand van zaken en stappen

In 2025 is het strategisch informatiebeveiligings- en privacybeleid herzien en vastgesteld door het college van B&W en de burgemeester. Vaststelling door de gemeenteraad is gepland in het eerste kwartaal van 2026.

De privacy officer, functionaris gegevensbescherming en chief information security officer hebben een IB&P-jaarplan 2026-2027 opgesteld, waarin verdere implementatie van het IB&P-beleid en verbeteringen op de aandachtspunten in dit jaarverslag, zijn gepland.

Aandachtspunten

- Interne en externe communicatie over het beleid moet nog verder plaatsvinden.
- In andere beleidsdocumenten is informatiebeveiliging en privacy nog geen onderwerp. Denk aan het inkoopbeleid. In het personeelshandboek is een verouderde privacyverklaring opgenomen.
- Er is geen bewaar- en vernietigingsbeleid.

[7] Artikel 24.2 AVG en 4a Wpg

3. Processen

3.1 Werkprocessen

Voor overzicht en inzicht is het belangrijk dat de organisatie werkprocessen waarin persoonsgegevens worden verwerkt, heeft beschreven en vastgesteld.

Stand van zaken en stappen

- In het nieuwe IB&P-beleid zijn teamleiders aangewezen als proces- en systeemeigenaren.
- Er is een werkgroep Processen gestart. De privacy officer is betrokken bij deze werkgroep.

Aandachtspunten

- Enkele processen zijn beschreven en vindbaar op intranet. Hierin is de verwerking van persoonsgegevens niet opgenomen.

3.2 Register van verwerkingen[8]

De organisatie is verplicht om een register van verwerkingen bij te houden. Per verwerking (proces) staat hierin: het doel, de categorieën van betrokkenen, de categorieën persoonsgegevens, derden ontvangers, bewaartermijn en beveiligingsmaatregelen.

Stand van zaken en stappen

Er is een register van verwerkingen.

Aandachtspunten

- Het register is verouderd en niet volledig. Verwerkingen zijn voor het laatst of in 2020 of in 2021 herzien.
- Er is geen procedure voor het opnemen van nieuwe verwerkingen, wijzigen van verwerkingen in het register en het periodiek evalueren hiervan.

3.3 DPIA's[9]

Een Data Protection Impact Assesment (DPIA) is verplicht als de verwerking van persoonsgegevens een hoog risico betekent voor de rechten en vrijheden van een persoon. Een DPIA is een uitgebreid onderzoek naar risico's en maatregelen die vooraf moet worden uitgevoerd. Het geeft antwoord op vragen als: mag het, wat is noodzakelijk, met wie deel ik, is het goed beveiligd en bewaren we niet langer dan nodig. Een pré-DPIA is een vooronderzoek om te bepalen of een DPIA nodig is.

Stand van zaken en stappen

In het verleden zijn DPIA's uitgevoerd. Er is een procedure en format voor het uitvoeren van DPIA's.

[8] Artikel 30 AVG en 31d Wpg
[9] Artikel 35 AVG en 4c Wpg

Aandachtspunten

- De uitgevoerde DPIA's zijn verouderd. Het is onduidelijk of deze zijn voorgelegd aan de FG voor advies en of bevindingen en verbeteringen zijn opgepakt.
- De procedure en het format voor het uitvoeren van DPIA's zijn van 2022 en sindsdien niet geëvalueerd en aangepast waar nodig.

3.4 Bewaren en vernietigen

Gemeenten hebben een verplichting om gegevens te bewaren en vernietigen conform de Archiefwet. Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk[10].
De Wet politiegegevens kent specifieke bewaartermijnen[11].

Stand van zaken en stappen

Geen

Aandachtspunten

- Er is geen bewaar- en vernietigingsbeleid vastgesteld.
- Bewaar- en vernietigingstermijnen (conform de Archiefwet en VNG selectielijst) worden niet toegepast:
  - Binnen het zaaksysteem is tot op heden niet vernietigd. Er is een verbetering gestart om de achterstand over 2020-2024 te vernietigen.
  - In de applicatie die binnen het sociaal domein wordt gebruikt, was geen vernietiging mogelijk. Er is nu een module beschikbaar waarin dit wel kan en de mogelijkheden worden onderzocht.
  - Binnen andere applicaties en op de netwerkschijven vindt geen vernietiging plaats.

[10] Artikel 5 lid 1e AVG
[11] Artikel 14 Wpg

4. Organisatorische inbedding

4.1 IB&P-team

De kaders zijn complex en veranderen voortdurend en de risico's zijn hoog. Om de organisatie te adviseren en ondersteunen bij het implementeren van de kaders en het in control blijven, zijn voldoende en kundige medewerkers nodig. Ook is betrokkenheid en sturing van bestuurders en management essentieel.

Stand van zaken en stappen

- In juni 2025 is een nieuwe privacy officer gestart en in april 2025 een externe functionaris gegevensbescherming (FG). Er is een chief information security officer (CISO). Het IB&P-team is op sterkte.
- De FG is aangemeld bij de Autoriteit Persoonsgegevens en als externe voldoende onafhankelijk gepositioneerd. De contactgegevens van de FG zijn vindbaar voor inwoners op de website.
- De privacy officer, CISO en FG hebben maandelijks overleg met de teamleider Data & Control. Waar nodig informeert de teamleider Data & Control het managementteam.
- In november 2025 hebben de privacy officer en CISO een presentatie gegeven aan het managementteam over IB&P en de rollen en verantwoordelijkheden van teamleiders. Dit heeft gezorgd voor meer bewustzijn van de verantwoordelijkheid van de teamleiders en het belang van sturing.

Aandachtspunten

- De FG is niet aangewezen op basis van een officieel aanstellingsbesluit door de burgemeester, college van B&W en gemeenteraad.
- De privacy officer, CISO en FG hebben geen periodieke overleggen met de gemeentesecretaris, portefeuillehouder IB&P en teamleiders.
- Teamleiders hebben geen eigen plan om blijvend te voldoen aan de privacywetgeving.

4.2 Ondernemingsraad

De ondernemingsraad heeft instemmingsrecht ten aanzien van regelingen en voorzieningen die de privacy van medewerkers raken[12]. De Ondernemingsraad heeft adviesrecht over voorgenomen besluiten tot invoering of wijziging van een belangrijke technologische voorziening[13].

Stand van zaken en stappen

Geen

Aandachtspunten

- Er zijn geen handreikingen of procedures waarin de organisatie wordt gewezen op de rol van de Ondernemingsraad bij dergelijke regelingen en (technologische) voorzieningen.
- De Ondernemingsraad is nog niet geïnformeerd over het nieuwe IB&P-beleid.

[12] Artikel 27 lid 1 k en l Wet op de ondernemingsraden
[13] Artikel 25 lid 1 k Wet op de ondernemingsraden

4.3 Bewustwording

Medewerkers zijn een belangrijke schakel bij informatiebeveiliging en privacy. Het is belangrijk dat ze bewust zijn en kennis hebben om risico's te verkleinen en incidenten (tijdig) herkennen.

Stand van zaken en stappen

- De organisatie maakt gebruik van de microlearnings van 'Sir Askalot'. Wekelijks krijgen medewerkers een stelling in de mailbox over informatiebeveiliging en privacy.
- Alle nieuwe medewerkers volgen een IB&P-workshop die gegeven wordt door de privacy officer en CISO.
- In het 4e kwartaal 2025 is een kennis en bewustzijnsplan voor 2026 vastgesteld door het managementteam.

Aandachtspunten

- In het personeelshandboek (onderdeel van de arbeidsovereenkomst) is onvoldoende opgenomen wat er van medewerkers wordt verwacht bij de omgang met persoonsgegevens. Dit geldt ook voor externen.
- Er is geen procedure waarin is vastgelegd dat medewerkers bij indiensttreding en externen bij de start van de opdracht, bewust worden gemaakt van hun verantwoordelijkheden met betrekking tot het beschermen en geheimhouden van persoonsgegevens.

5. Rechten van betrokkenen

Personen hebben rechten om controle te houden op wat er gebeurt met hun persoonsgegevens[14].

5.1 Recht op informatie

De organisatie heeft een actieve plicht om personen vooraf in duidelijke en eenvoudige taal te informeren over de verwerking van persoonsgegevens.

Er moet in ieder geval informatie zijn over:

- waarom persoonsgegevens worden verwerkt en binnen welke grondslag.
- welke persoonsgegevens worden verwerkt.
- hoe lang persoonsgegevens worden bewaard.
- welke organisaties de persoonsgegevens ontvangen.
- van wie de persoonsgegevens zijn ontvangen (als dit niet van de persoon zelf is).
- de rechten die personen hebben en hoe ze hier gebruik van kunnen maken.
- als er sprake is van geautomatiseerde besluitvorming (waaronder profilering): uitleg over de logica, belang en verwachte gevolgen voor de personen.
- uitleg als er sprake is van een voornemen tot verdere verwerking voor een ander (gerelateerd) doel.
- wie de verwerkingsverantwoordelijke en de functionaris gegevensbescherming is en hoe ze deze kunnen bereiken.

Stand van zaken en stappen

De gemeente Scherpenzeel heeft de volgende privacyverklaringen op de website:

- Algemene privacyverklaring
- Privacyverklaring Wet politiegegevens (Wpg)
- Privacyverklaring Werving en Selectie
- Rechten
- Cookieverklaring

Aandachtspunten

- Betrokkenen worden nog onvoldoende geïnformeerd over de verwerkingen van persoonsgegevens door de organisatie. De privacyverklaringen zijn nog te algemeen.
- De privacyverklaring op de website bevat niet alle verplichte onderdelen.

5.2 Rechten van betrokkenen

Betrokkenen hebben het recht op inzage, aanpassing, verwijdering, overdraagbaarheid, beperking en bezwaar. Om gebruik te maken van deze rechten moeten personen een verzoek kunnen indienen en systemen moeten hierin kunnen voorzien. Het is belangrijk dat medewerkers kennis hebben van de rechten van betrokkenen, zodat ze verzoeken herkennen en weten hoe te handelen.

Stand van zaken en stappen

- Betrokkenen worden op de website geïnformeerd over hun rechten en hoe ze hier gebruik van kunnen maken.
- Er is een procedure voor het behandelen van de rechten van betrokkenen opgesteld in maart 2025.

[14] Artikel 5, 12 t/m 22 en 38.4 AVG en 24a tm 28 Wpg en Telecommunicatiewet

- In het zaaksysteem is in 2025 één verzoek tot verwijdering van persoonsgegevens geregistreerd en afgehandeld. Er zijn geen andere verzoeken geregistreerd.

Aandachtspunten
- De procedure is niet intern gecommuniceerd en mogelijk te technisch voor de meeste medewerkers om goed te kunnen volgen.
- Op de website staat dat betrokkenen een AVG-verzoek online kunnen indienen via DigiD of fysiek afgeven op het gemeentehuis. Ook via de andere kanalen moeten betrokkenen een verzoek kunnen indienen.
- Op de website is onderscheid gemaakt tussen de rechten van betrokkenen in de Wpg en de AVG. Dit is niet duidelijk genoeg uitgelegd en niet eenduidig. Betrokkenen kunnen Wpg-verzoeken bijvoorbeeld niet via DigiD indienen.
- Voor het verzoek dat in 2025 is ontvangen, is geen ontvangstbevestiging verstuurd. Het verzoek is niet binnen de wettelijke termijn afgehandeld.

5.3 Toestemming

Als personen toestemming hebben gegeven voor het verwerken van persoonsgegevens, dan hebben ze het recht om deze toestemming in te trekken. Toestemming intrekken moet net zo eenvoudig zijn als toestemming geven.

Eén van de eisen aan toestemming is dat deze in vrijheid is gegeven. Daardoor is toestemming als grondslag bij de gemeente meestal niet mogelijk, omdat er vaak een afhankelijkheid van de gemeente is. De verwachting is dan ook dat het aantal verwerkingen dat op toestemming is gebaseerd laag is. Verwerkingen zoals de nieuwsbrief van Scherpenzeel en foto's en filmpjes, zijn op toestemming gebaseerd.

Stand van zaken en stappen
Geen.

Aandachtspunten
Er is geen inzicht in de verwerkingen van persoonsgegevens die op de grondslag 'toestemming' zijn gebaseerd. Daardoor is het ook niet duidelijk of toestemming geven en intrekken aan de regels voldoet.

5.4 Geautomatiseerde besluitvorming

Bij geautomatiseerde besluitvorming wordt er automatisch (door een computer) een beslissing over iemand genomen. Dit gebeurt op basis van gegevens over die persoon, zonder dat een mens dit nog beoordeelt. Personen die een geautomatiseerd besluit hebben ontvangen, hebben het recht om de organisatie te verzoeken om een nieuw besluit te nemen waarbij een mens hun gegevens beoordeelt.

Stand van zaken en stappen
Geen.

Aandachtspunten
- Er is geen overzicht van processen waarbinnen geautomatiseerde besluitvorming plaatsvindt. Daardoor is het niet duidelijk of aan de regels is voldaan. De verwachting is dat geautomatiseerde besluitvorming niet veel voorkomt binnen de gemeente Scherpenzeel.

5.5 Websites en applicaties

Een cookie is een klein bestand, dat bij een bezoek aan een website wordt opgeslagen op het apparaat van de bezoeker. Er zijn drie soorten cookies:

- Functionele cookies. Deze cookies zijn nodig om een website goed te laten werken. Deze kan een websitebezoeker niet uitschakelen.
- Beperkt analytische cookies. Deze helpen om te begrijpen hoe bezoekers een website gebruiken en kan een website worden verbeterd. Deze cookies verzamelen anoniem gegevens en rapporteren hierover.
- Overige cookies. Deze cookies kunnen het surfgedrag van de websitebezoeker over verschillende websites volgen. Ze worden ook wel tracking- of volgcookies genoemd.

Organisaties zijn verplicht om websitebezoekers te informeren over alle cookies die worden geplaatst. Overige cookies mogen alleen worden geplaatst als de websitebezoeker hier toestemming voor heeft gegeven.

Stand van zaken en stappen

In november 2025 heb ik als FG een onderzoek gedaan naar de cookieverklaring en cookies op de website www.scherpenzeel.nl. Verbetermaatregelen zijn opgenomen in het jaarplan IB&P 2026-2027.

Aandachtspunten

- De organisatie heeft niet vastgelegd aan welke eisen websites en applicaties die toegankelijk zijn voor burgers (zoals iBabs), moeten voldoen om privacywetgeving en de Telecommunicatiewet na te leven.
- De cookieverklaring op de website www.scherpenzeel.nl is niet juist en volledig. Websitebezoekers worden niet geïnformeerd over de cookies die worden geplaatst. Het lijkt er op dat er enkele overige cookies worden geplaatst waar geen toestemming voor wordt gevraagd.
- Er is geen overzicht van websites en applicaties die onder de verantwoordelijkheid vallen van de gemeente Scherpenzeel. Daardoor is het niet duidelijk of alle websites en applicaties aan de regels voldoen.

6. Samenwerking

Als organisaties persoonsgegevens uitwisselen is het belangrijk om na te gaan of dit is toegestaan en onder welke voorwaarden en verwerkingsverantwoordelijkheid. Het is verplicht om schriftelijke afspraken te maken over de voorwaarden en beveiliging. Bijvoorbeeld in een:

- convenant of samenwerkingsovereenkomst als partijen (gezamenlijk) verwerkingsverantwoordelijke[15] zijn binnen een samenwerking.
- verwerkersovereenkomst als een organisatie die ontvangt of toegang heeft, een 'verwerker'[16] is. Een verwerker verwerkt persoonsgegevens namens, in opdracht en volgens instructie van de verwerkingsverantwoordelijke.
- gegevensleveringsovereenkomst als organisaties de persoonsgegevens verder verwerken als verwerkingsverantwoordelijke. Hierin staan afspraken over een veilige manier van overdragen van de persoonsgegevens en moment van overgaan van de verwerkingsverantwoordelijkheid.

Stand van zaken en stappen

In het inkoopformulier worden medewerkers gewezen op het afstemmen met de CISO en Privacy Officer over informatiebeveiliging en privacy.

De organisatie gebruikt de standaard verwerkersovereenkomst van de Informatiebeveiligingsdienst (IBD, onderdeel VNG). Gemeenten hebben met elkaar afgesproken deze als standaard te gebruiken en hier niet vanaf te wijken.

Aandachtspunten

- Er is geen procedure ingericht die ervoor zorgt dat persoonsgegevens alleen worden uitgewisseld als dit is toegestaan en dat de juiste contractuele afspraken worden gemaakt, centraal gearchiveerd en nageleefd.
- Het register van verwerkingen is verouderd en niet volledig. Hierdoor is er geen actueel overzicht van organisaties en landen buiten de Europese Unie, waarmee persoonsgegevens worden uitgewisseld.
- Er wordt niet gemonitord of uitwisseling volgens de regels plaatsvindt en contractuele afspraken worden nageleefd.
- In de praktijk worden de CISO en privacy officer achteraf betrokken als externe partijen al benaderd zijn. Om tijdig te kunnen bijsturen is het van belang dat vooraf afstemming wordt gezocht.

[15] Artikel 4.7, 24, 26 AVG en 20 Wpg
[16] Artikel 28 AVG en 6c Wpg

7. Gegevensbescherming

7.1 Risico's

Het onzorgvuldig omgaan met gegevens kan enorme gevolgen hebben voor betrokkenen. Denk aan een inbreuk op het grondrecht privacy of slachtoffer worden van digitale criminaliteit. Dit kan reputatieschade, financiële schade, emotionele schade, het gevoel continu gevolgd te worden, uitsluiting, discriminatie en onjuiste besluitvorming tot gevolg hebben.

Risico's voor de organisatie kunnen ook groot zijn, bijvoorbeeld:

- Uitval van de dienstverlening en bedrijfsvoering.
- Incidenten zoals digitale criminaliteit en datalekken.
- Personen hebben recht op schadevergoeding[17] als er schade is omdat de organisatie verwijtbaar in strijd met de wet heeft gehandeld.
- Onder verscherpt toezicht worden gesteld door de Autoriteit Persoonsgegevens en sancties opgelegd krijgen. De belangrijkste sancties zijn de boete[18], de last onder dwangsom, het verwerkingsverbod, de berisping en de waarschuwing.

De gevolgen kunnen hoge (herstel)kosten, impact op de capaciteit, reputatieschade en verlies van vertrouwen in de organisatie zijn. Het niet beschikbaar zijn van systemen, dienstverlening en/of bedrijfsvoering heeft impact op klanten en medewerkers omdat ze hun werk niet of minder goed kunnen doen.

Stand van zaken en stappen

Zie mail 24-11. Jan 1-12 gevraagd huidige situatie. Er is een beoordeling BMC model.

Aandachtspunten

- Er is geen risicomanagementproces en Plan-Do-Check-Act cyclus waar IB&P onderdeel van zijn.

7.2 Gegevensbescherming door ontwerp en standaard instellingen19

Bij veranderingen en vernieuwingen is het verplicht om vanaf de inrichting rekening te houden met een zorgvuldige behandeling van persoonsgegevens. Denk hierbij aan minimaal gebruik van persoonsgegevens en een passende bescherming. Standaardinstellingen zijn zo gekozen dat dit maximaal wordt geborgd.

Stand van zaken en stappen

In het inkoopformulier worden medewerkers gewezen op het afstemmen met de Privacy Officer en CISO over informatiebeveiliging en privacy.

Aandachtspunten

- Er is geen procedure ingericht voor het toepassen van privacy by design en default.
- In het inkoopformulier is de verantwoordelijkheid neergelegd bij de Privacy Officer en CISO en niet bij de proceseigenaar.
- Privacy by design en privacy by default wordt in de praktijk nauwelijks of achteraf toegepast in de ontwerpfase van vernieuwingen, veranderingen en inkoop.

[17] Artikel 82 AVG en 31c Wpg.
[18] Boetebeleidsregels Autoriteit Persoonsgegevens 2023
[19] Artikel 25 AVG en 4a en b Wpg, ook wel privacy by design en privacy by default.

7.3 Informatiebeveiliging

In de privacywetgeving is verplicht gesteld dat organisaties zorgen voor passende technische en organisatorische informatiebeveiligingsmaatregelen[20].

Binnen de overheid is afgesproken om aan de Baseline Informatiebeveiliging Overheid(BIO)[21] te voldoen. In 2026 treed de Cyberbeveiligingswet in werking. De BIO is herzien naar BIO 2.0. Hierin is de Cyberbeveiligingswet verwerkt.

Door te voldoen aan de BIO (2.0) voldoen organisaties voor een deel aan de verplichting tot het treffen van passende technische en organisatorische informatiebeveiligingsmaatregelen voldaan.

Stand van zaken en stappen

Zie paragraaf 3.1 over het IB&P-beleid en 8.1 over risico's.
De tool Zivver is in gebruik genomen waarmee e-mails en grote bestanden versleuteld kunnen worden verstuurd.

Aandachtspunten

- De organisatie voldoet niet aantoonbaar aan de BIO.
- De gemeente Veenendaal levert, beheert en beveiligt de ICT-omgeving van de gemeente Scherpenzeel. Er zijn geen contractuele met de gemeente Veenendaal over informatiebeveiliging en het aantoonbaar maken hiervan. Ook is er geen verwerkersovereenkomst gesloten. Er wordt gewerkt aan een nieuwe dienstverleningsovereenkomst waarin deze afspraken wel worden opgenomen.
- Het is onduidelijk in hoeverre de gemeente Veenendaal en onze ICT-omgeving voldoet aan de BIO en zich voorbereid op de Cyberbeveiligingswet en BIO 2.0.

7.4 Datalekken[22]

Bij een datalek zijn persoonsgegevens onterecht vernietigd of verloren gegaan, veranderd, gedeeld of toegankelijk geweest voor anderen. Het is verplicht om datalekken te registreren in een intern datalekkenregister, ernstige datalekken binnen 72 uur te melden bij de Autoriteit Persoonsgegevens en betrokkenen te informeren.

Stand van zaken en stappen

In 2025 zijn er twee datalekken intern gemeld. De impact van deze datalekken was laag en daarom zijn ze niet gemeld bij de Autoriteit Persoonsgegevens en betrokkenen.

In 2025 is een procedure vastgesteld voor de behandeling van datalekken. Op intranet is informatie over datalekken te vinden voor medewerkers. In het introductieprogramma nieuwe medewerkers en in de 'Sir Askalot' microlearnings is datalekken een onderwerp.

Aandachtspunten

- Gezien het lage aantal gemelde datalekken, zijn medewerkers mogelijk nog niet genoeg bewust om datalekken te herkennen en te melden.

[20] Artikel 32 AVG en 4a Wpg
[21] Baseline Informatiebeveiliging Overheid
[22] Artikel 33 en 34 AVG en 33a Wpg

8. Verantwoording

8.1 Audit en controle

Periodieke IB&P-audits en controles zijn belangrijk om aantoonbaar te monitoren in hoeverre de organisatie in control is, betrokkenen grip hebben op hun persoonsgegevens en waar nodig verbeteringen te kunnen treffen.

De Wet politiegegevens kent auditverplichtingen[23]:

- Jaarlijks moet er een interne audit worden uitgevoerd. De resultaten van deze audit moeten in een rapportage worden vastgelegd en aangeboden aan de verwerkingsverantwoordelijke. De auditor moet onafhankelijk zijn, een auditorenopleiding hebben gevolgd en voldoende kennis en ervaring hebben.
- Om de vier jaar moet er een audit worden uitgevoerd door een externe auditor. Het is verplicht om de rapportage naar de Autoriteit Persoonsgegevens en de verwerkingsverantwoordelijke (college van B&W) te sturen.

Stand van zaken en stappen

- Als functionaris gegevensbescherming heb ik eind 2025 het borgingsproduct ingevuld om een beeld te vormen in hoeverre de organisatie aan de privacywetgeving voldoet (zie ook paragraaf 1.3). De bevindingen zijn verwoord in dit jaarverslag.
- In 2022 heeft de gemeente Scherpenzeel een externe audit op de Wet politiegegevens in domein 1 uit laten voeren. Domein 1 zijn de boa's in de openbare ruimte. De uitkomst was een afkeurende verklaring omdat de gemeente niet voldeed aan de Wet politiegegevens. Dit rapport is naar de Autoriteit Persoonsgegevens verstuurd.
- Eind 2025 is een extern bureau ingeschakeld om de organisatie te ondersteunen bij de implementatie van de Wet politiegegevens. Ook is er een externe auditor gecontracteerd voor het uitvoeren van de externe audits over de verantwoordingsjaren 2021 tot en met 2024.

Aandachtspunten

- Er is naar aanleiding van de afkeurende verklaring op domein 1, geen verbeterplan opgesteld en geïmplementeerd en er is geen externe heraudit uitgevoerd. Dit is wettelijk verplicht.
- Er zijn eerder geen interne en externe audits uitgevoerd op domein 3. Domein 3 zijn de boa's die de leerplichtwet uitvoeren (leerplichtambtenaren). De leerplichtwet wordt voor de gemeente Scherpenzeel uitgevoerd door de gemeente Veenendaal. De gemeente Scherpenzeel was in de veronderstelling dat de audit bij de gemeente Veenendaal ook volstond voor de gemeente Scherpenzeel.
- Er worden geen periodieke controles uitgevoerd op basis van een auditplan. Denk aan controles op rollen, rechten en logging in risicovolle systemen en bewaar- en vernietigingstermijnen.

8.2 Evalueren en rapporteren naleving IB&P

Als verwerkingsverantwoordelijke is het belangrijk dat u geïnformeerd bent over in hoeverre de organisatie in control is en hierop kunt sturen. Om te zorgen dat alle managementlagen invulling geven aan hun verantwoordelijkheid, is het van belang dat

[23] *Artikel 33 Wpg en Regeling periodieke audit politiegegevens*

ze verantwoording afleggen over de stand van zaken binnen hun eigen organisatieonderdeel.

Stand van zaken en stappen

De privacy officer en de CISO hebben een IB&P jaarplan 2025-2027 opgesteld. Hierin staat wat de privacy officer en CISO doen om de organisatie te ondersteunen en adviseren op het gebied van IB&P.

Als functionaris gegevensbescherming heb ik een toezichts- en adviesplan 2025 en 2026 voorgelegd aan de teamleider Data & Control. Hierin staat hoe ik toezicht hou op de naleving van de privacywetgeving door de organisatie.

Aandachtspunten

- Informatiebeveiliging en privacy is geen onderwerp in de planning- en controldocumenten.
- Er vinden geen periodieke aantoonbare evaluaties en controles plaats op naleving van IB&P.
- Teamleiders leggen geen verantwoording af over de stand van zaken en voortgang aan de directie en verantwoordelijke bestuursorganen.
- Het college van B&W is niet geïnformeerd over het jaarverslag 2023 en 2024 van de vorige functionaris gegevensbescherming. Voor de gemeenteraad is geen jaarverslag door de Functionaris gegevensbescherming opgesteld.