

JAARVERSLAG GEGEVENSBESCHERMING GEMEENTE AMELAND 2025



Functionaris

Gegevensbescherming
Maart 2026

Inhoudsopgave

INHOUDSOPGAVE	2
INLEIDING	4
LEESWIJZER	4
DEEL 1. TERUGBLIK OP 2025	6
1. BELEID	6
2. PROCESSEN	6
3. ORGANISATIE	7
4. RECHTEN VAN BETROKKENE	7
5. SAMENWERKING	7
6. BEVEILIGING	7
7. VERANTWOORDING	8
OVERIG	8
GR DE WADDEN	9
1. VERWERKINGSVERANTWOORDELIJKHEID (WIE DOET WAT?)	9
2. BELANGRIJKSTE AVG-VERPLICHTINGEN VOOR EEN GR	9
3. VERWERKERSOVEREENKOMSTEN	10
4. INFORMATIEBEVEILIGING EN BEWUSTWORDING	10
5. BEWAAR- EN VERNIETIGINGSBELEID	10
DEEL 2. VOORUITKIJKEN NAAR 2026	11
BIJLAGE 1 - STAND VAN ZAKEN AVG PER ONDERWERP	13

Samenvatting

Als onafhankelijk toezichthouder van de gemeente constateert de Functionaris Gegevensbescherming (FG) dat de gemeente Ameland in 2025 vorderingen heeft gemaakt wanneer het gaat om het voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Hieronder volgt een korte samenvatting van wat in de rest van het verslag verder wordt uitgewerkt.

Wat de gemeente in 2025 heeft bereikt:

Naar aanleiding van de geconstateerde achterstanden bij de compliance aan de AVG is er een aanpassing geweest in de contractuele afspraken met gemeente Leeuwarden. De ondersteuning vanuit Privacy is verlaagd, waardoor er financiële ruimte is ontstaan voor de inhuur van een tijdelijke privacy officer. Deze heeft naast gemeente Ameland, ook de andere Waddeneilanden ondersteund bij het oplossen van alle geconstateerde bevindingen.

- De privacy verklaring is herzien en opgesteld in B1. Naar aanleiding hiervan is ook informatie over AVG en privacy op de website van de gemeente geactualiseerd en aangevuld.
- Het privacy beleid is opgesteld en vastgesteld.
- Er zijn de nodige procedures opgesteld:
 - Procedures voor de rechten van betrokkenen
 - Procedure voor behandelen van datalekken
 - Procedure voor het opstellen van een DPIA
- Het verwerkingsregister en een procedure voor actualisatie daarvan is opgesteld.
- Cookieverklaringen zijn geactualiseerd en op de website gepubliceerd.

Inleiding

Met het jaarverslag van de Functionaris Gegevensbescherming (FG) van gemeente Ameland wordt beoogd verantwoording af te leggen van de taak van de FG zoals vastgelegd in de Algemene Verordening Gegevensbescherming (art. 39 AVG) en daarmee een beeld te scheppen over waar de gemeente staat wanneer het gaat om het verwerken van persoonsgegevens volgens de verschillende privacywetten zoals de AVG en de UAVG.

De belangrijkste taak van de FG is dat deze onafhankelijk toezicht en controle houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming door de gemeente als organisatie.

Dit jaarverslag gaat in op het algemene beeld van de compliance ten aanzien van de AVG, de bevindingen over het jaar 2025 en de aandachtspunten voor 2026. Dit verslag wordt jaarlijks opgesteld en aangeboden aan het college van Burgermeester en wethouders omdat zij eindverantwoordelijk is voor de verwerking van persoonsgegevens. Daarna kan het college via een informerende brief de gemeenteraad informeren en publiceren op de website van de gemeente. Het jaarverslag wordt ook aangeboden aan de Gemeentesecretaris en aan de Directie, aangezien zij inhoudelijk verantwoordelijk zijn voor de verwerking van persoonsgegevens binnen de gemeentelijke organisatie.

Leeswijzer

Dit verslag bestaat uit twee onderdelen. In het eerste deel wordt teruggekeken naar 2025. Wat heeft de gemeente bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn genomen om te voldoen aan de privacywetgeving?

In het tweede deel staan de aanbevelingen om gegevensbescherming vanaf 2026 naar een hoger niveau te tillen.

De algehele AVG-compliance wordt gemeten aan de hand van onderstaande thema's uit het AVG borgingsproduct 3.1 van de VNG:¹ Hierbij wordt (nog) geen onderscheid gemaakt tussen de verschillende sectoren binnen de gemeente.

- Beleid
- Processen
- Organisatie
- Rechten van betrokkene
- Samenwerking
- Gegevensbescherming
- Verantwoording

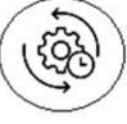
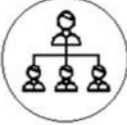
Het borgingsproduct bevat thema's, criteria en maatregelen die de AVG vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. In bijlage 1 staat per thema aangegeven in hoeverre de gemeente in algemene zin de criteria heeft geïmplementeerd.

¹ Zie het document 'Criteria borging AVG / Borgingsproduct gegevensbescherming in de gemeentelijke organisatie', [link](#).

FG Jaarverslag 2025

Totaaloverzicht van de kaders



		2024 Resultaten	2025 Resultaten
	Beleid		
	Processen Organisatie		
	Betrokkene		
	Samenwerking		
	Gegevensbescherming		
	gVerantwoording		
			

Deel 1. Terugblik op 2025

De verantwoordelijkheid voor gemeente Ameland voor het verwerken van persoonsgegevens van inwoners ligt in hoofdlijnen bij drie bestuursorganen: de burgemeester, het college van B&W en de gemeenteraad. De Functionaris Gegevensbescherming (FG) ziet erop toe dat de gemeente de Algemene Verordening Gegevensbescherming (AVG) naleeft. De FG brengt jaarlijks een verslag uit van de werkzaamheden, bevindingen en aanbevelingen.

In dit jaarverslag staat een overzicht van de huidige stand van zaken, opgemaakt in het AVG borgingsproduct van de VNG². De uitkomsten in dat borgingsproduct is ontstaan door de aanlevering van bewijsstukken vanuit de contactpersoon voor privacy in gemeente Ameland. Uit deze stand van zaken kunnen actiepunten worden opgemaakt, welke voor het komende jaar kunnen gaan gelden.

2025 stond in het teken van het verstevigen van de basis, inzetten van verbeteringen en werken aan de komende ontwikkelingen. Dit deel van het verslag geeft een terugblik op wat gemeente Ameland in 2025 heeft bereikt. Op een behoorlijk aantal onderdelen is de nodige extra inzet gepleegd, wat direct terug te zien is in de scores van het Borgingsproduct. Daar mag de organisatie dan ook met tevredenheid op terugzien!



1. Beleid

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

De gemiddelde score op Beleid in het borgingsproduct is 68%, waar dat in 2024 32% was. Er is een nieuw privacybeleid vastgesteld, een privacy verklaring opgesteld en de website is daarop ook aangepast. Het enige punt van aandacht op dit onderdeel zit nog in het punt van het opstellen van een procedure over hoe beleid vast te stellen.



2. Processen

Het verwerken van persoonsgegevens van gemeente Ameland moet voldoen aan de AVG. Dit houdt in dat de gemeente de werkprocessen, waarbinnen met persoonsgegevens wordt gewerkt, moet inrichten volgens de beginselen vanuit de AVG: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast is de gemeente bij risicovolle verwerkingen verplicht om een DPIA³ uit te voeren.

Hoewel de score op dit onderdeel gemiddeld uitkomt op 64%, zijn er geen vastgestelde werkprocessen, worden er geen onderzoeken uitgevoerd op de risico's van de verwerkingen (pre-DPIA's) en zijn er nog niet overal DPIA's uitgevoerd, waar dat nodig is. Omdat daardoor per verwerking de risico's en de daarbij ingezette mitigerende maatregelen niet inzichtelijk zijn, loopt de organisatie daar mogelijk een risico. En daarom dus nog een gematigde kleur.

² Zie het document 'Criteria borging AVG / Borgingsproduct gegevensbescherming in de gemeentelijke organisatie', [link](#).

³ DPIA staat voor een Data Protectie Impact Assessment. Dit is een onderzoek om de privacy risico's van gegevensverwerkingen in kaart te brengen. En de maatregelen om deze risico's en dilemma's weg te nemen of te verkleinen.



3. Organisatie

Voor een goede en juiste uitvoering is het van belang dat iedereen binnen de 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 bewustzijn creëren.

De score op Organisatie is 84%. Een hele goede score, die met blijvende aandacht voor privacy kan worden vastgehouden in 2026. Door de verantwoordelijkheden daarin vast te leggen, ontstaat nog meer eigenaarschap. Hiermee wordt gegevensbescherming een vast onderdeel van het werk. Het contract voor het bewustzijnsprogramma, ARDA, is verlengd.

Punt van aandacht is dan wel, dat de deelname aan de geboden leerlijnen voldoende moet zijn. De mens is nog altijd de zwakste schakel als het gaat om het voorkomen van datalekken. De deelname aan bijvoorbeeld ARDA zal onderwerp van gesprek moeten zijn met het management. Daarnaast zal de organisatie moeten bepalen wat het gewenste resultaat moet zijn in de deelnamegraad.



4. Rechten van betrokkene

Gemeente Ameland informeert degene waarover zij de persoonsgegevens verwerkt (de betrokkene) zowel actief als passief over het verwerken, de grondslag en de maatregelen tegen onrechtmatige toegang en verwerking. Daarnaast faciliteert de gemeente de betrokkenen in het uitoefenen van hun rechten op bijvoorbeeld inzage, correctie en verwijderen van hun persoonsgegevens. De score op Rechten van betrokkene is 84%. Net als in 2024 een uitstekend resultaat.



5. Samenwerking

Gemeente Ameland werkt op meerdere beleidsterreinen, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. Vaak is er sprake van het verwerken van persoonsgegevens tussen partijen: ontvangen, verzenden, maar ook het opslaan en raadplegen van persoonsgegevens valt hieronder. De gemeente moet dan ook afspraken vastleggen hierover met deze andere partijen.

De score op Samenwerking in het toetsingsproduct is van 55% naar 75% gegaan. Dat heeft vooral te maken met het juist invullen van de vragen.

Voor het komende jaar wil de FG de samenwerkingsverbanden inzichtelijk krijgen, deze op laten nemen in het verwerkingsregister en dat deze periodiek worden geëvalueerd en waar nodig herzien.

Samenwerkingen veranderen in de loop van de tijd, gegevensuitwisselingen veranderen, soms op basis van behoefte, soms op basis van veranderende wet- en regelgeving.



6. Beveiliging

Vanuit het algemene behoorlijkeheids-, het integriteits- en het vertrouwelijkheidsbeginsel is het essentieel dat gemeente Ameland passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er een meldplicht datalekken. Dit houdt in dat de gemeente incidenten op het gebied van informatieveiligheid onder bepaalde omstandigheden moet melden aan de Autoriteit Persoonsgegevens en/of de betrokkene(n).

In 2025 is verdere invulling gegeven aan het BIO-normenkader (Baseline Informatiebeveiliging Overheid). Met name op beleidsmatig vlak is aandacht besteed aan het opstellen en actualiseren van diverse beleidsdocumenten, waaronder het cryptografiebeleid en het back-up- en restorebeleid. Momenteel scoort gemeente Ameland op alle onderdelen in de BIO een voldoende.

Daarnaast is in 2025 een TPM-verklaring (Third Party Memorandum) afgegeven voor de SSC-werkplek. Hierbij zijn de BIO-normen, welke behoren bij de SSC-werkplek, getoetst op Opzet, Bestaan maar ook de Werking. Deze TPM-verklaring wordt inmiddels door gemeente Ameland gebruikt voor de ENSIA-verantwoording binnen het BIO-normenkader. Tevens kan deze TPM-verklaring door de accountant van gemeente Ameland worden benut om de mate van volwassenheid van de informatiebeveiliging van de SSC-werkplek te toetsen.

De ICT-omgeving is in 2025 door een externe partij onderzocht, waarbij zowel de vanaf het internet bereikbare systemen als de interne systemen zijn gecontroleerd op kwetsbaarheden. Ook is aandacht besteed aan het vergroten van het informatiebeveiligingsbewustzijn. Dit is onder meer gedaan door het uitvoeren van phishingcampagnes en verlenging van het contract met ARDA (E-learning).



7. Verantwoording

De gemeente zelf is verantwoordelijk voor het aantonen dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert gemeente Ameland een belangrijke bijdrage aan de bescherming van betrokkenen op het gebied van privacy. Dit betekent dat het college van B&W, de burgemeester en de gemeenteraad moeten kunnen aantonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante andere wet- en regelgeving.

De FG heeft, samen met de CISO, periodieke overleggen met de Gemeentesecretaris. Deze overleggen zijn ingepland per kwartaal en worden tevens spontaan belegd waar nodig. Er zijn ook nieuwe of geactualiseerde initiatieven. Denk aan het gebruik van het Borgingsproduct 3.1 van de VNG. Dit is een toetsingskader waarmee de organisatie kan toetsen in hoeverre zij in staat is om de naleving van de AVG te waarborgen. Dit jaarverslag en het toezicht plan van de FG zijn input voor de organisatie om te toetsen in hoeverre zij aan de AVG voldoet en waar nog actiepunten liggen om in het komende jaar op te pakken. Evenals dit jaar zullen deze documenten ook komend jaar in de jaarlijkse cyclus worden gebruikt.

De score op Verantwoording in het toetsingsproduct is 57%; een lichte stijging ten opzichte van de score van 50% in 2024. Nu de basis redelijk op orde is, is het tijd voor de FG om een toezicht plan in te zetten. Als dit gecombineerd kan worden met de periodieke controle die onder aansturing van het management moet worden gedaan, voldoet gemeente Ameland aan de verantwoordingsplicht.

Overig

De FG heeft dit jaar deelgenomen aan periodieke overleggen met de privacy officers, de CISO, record manager, de regionale experttafel en het regionale FG-overleg. Verder heeft afstemming plaatsgevonden met externe partijen zoals FG's/PO's van andere gemeenten of van samenwerkingspartners.

De FG heeft daarnaast deelgenomen aan diverse (digitale) bijeenkomsten van VNG/IBD zoals bijeenkomsten rondom de Wams (Wet aanpak meervoudige problematiek sociaal domein) en kennissessies over de Wpg en de Wgs (wet gegevensdeling samenwerkingsverbanden).

Ten aanzien van Kennisbevordering heeft de FG deelgenomen aan diverse (bij-)scholingsactiviteiten en cursussen.

GR de Wadden

De Gemeenschappelijke Regeling (GR) de Waddeneilanden is een samenwerking tussen de Waddeneilanden Texel, Vlieland, Terschelling, Ameland en Schiermonnikoog. Een Gemeenschappelijke Regeling (GR) tussen overheidsinstanties (zoals gemeenten) wordt onder de Algemene Verordening Gegevensbescherming (AVG) gezien als een zelfstandige entiteit. Dit betekent dat de GR verwerkingsverantwoordelijke is voor de persoonsgegevens die zij verwerkt, en dus zelfstandig aan alle AVG-verplichtingen moet voldoen en een eigen FG heeft om daar toezicht op te houden.

De FG van de GR is ook de FG van 4 van de 5 deelnemende Waddeneilanden. Daarom kiest de FG ervoor om het verslag van de GR onderdeel te maken van de jaarverslagen van de 4 eilanden. Deze paragraaf wordt ook ter informatie gedeeld met de FG van gemeente Texel. Hieronder volgt een overzicht van de verplichtingen vanuit de AVG rondom de GR en in hoeverre de GR daaraan voldoet. Anders dan bij de Waddeneilanden, wordt hiervoor gebruik gemaakt van een deel van de vragen vanuit het borgingsproduct van de VNG. Niet alle vragen zijn namelijk relevant.

1. Verwerkingsverantwoordelijkheid (Wie doet wat?)

- **GR als Verantwoordelijke:** De GR bepaalt zelf het doel en de middelen voor de verwerking van persoonsgegevens. Zij is daarmee de 'verwerkingsverantwoordelijke' in de zin van de AVG.
- **Bestuurlijke verantwoordelijkheid:** Het Algemeen Bestuur (AB) of Dagelijks Bestuur (DB) van de GR is juridisch aansprakelijk voor de naleving van de privacywetgeving.
- **Afspraken met deelnemers:** De deelnemende gemeenten en de GR moeten in de regeling duidelijk vastleggen welke bevoegdheden en verantwoordelijkheden de GR heeft ten aanzien van gegevensverwerking.

Bevinding	In de Gemeenschappelijke Regeling is niets opgenomen rondom de verwerking van persoonsgegevens en daarmee de verwerkingsverantwoordelijkheid.
Advies	Ga na of de GR daarvoor aangepast kan worden, zodat de verantwoordelijkheden op het gebied van de privacywetgeving duidelijk zijn vastgelegd

2. Belangrijkste AVG-verplichtingen voor een GR

- **Grondslag:** Voor elke verwerking van persoonsgegevens moet een grondslag aanwezig zijn (bijv. uitvoering van een wettelijke taak of het algemeen belang).
- **Verwerkingsregister:** Een GR is verplicht een register van verwerkingsactiviteiten (art. 30 AVG) bij te houden. Hierin staat welke gegevens, waarom en hoe lang worden bewaard.
- **Functionaris Gegevensbescherming (FG):** Vanwege het publieke karakter en vaak grootschalige verwerking van gevoelige gegevens, is een GR meestal verplicht een FG aan te stellen.
- **DPIA (Data Protection Impact Assessment):** Als de GR werkt met privacygevoelige gegevens (bijv. in het sociaal domein) of grootschalig monitort, moet er vooraf een DPIA worden uitgevoerd om risico's in kaart te brengen.

Bevinding	• Er is een actueel verwerkingsregister; • De FG is in 2025 benoemd; • Voor alle verwerkingen is een grondslag opgenomen; • Er zijn processen beschreven om de actualiteit periodiek te controleren; • Er is vastgesteld dat er alleen voor de processen binnen HRM een DPIA noodzakelijk is. Deze is in de afrondende fase.
------------------	--

3. Verwerkersovereenkomsten

Als de GR gegevens deelt met de deelnemende gemeenten, of als de GR diensten inkoopt bij derden (bijv. IT-leveranciers), moeten er **verwerkersovereenkomsten** worden gesloten. Hierin wordt afgesproken dat de verwerker de gegevens veilig en conform de AVG behandelt.

Bevinding	• Er is voor alle samenwerkingen, waarbij er sprake is van de inzet van een verwerker voor de GR, inzichtelijk of een verwerkersovereenkomst nodig is. • Er is nog een verwerkersovereenkomst nodig voor de ondersteuning op ICT-gebied door gemeente Leeuwarden.
Advies	• Maak een overzicht van alle verwerkers die worden ingezet door de GR en zorg voor een actuele verwerkersovereenkomst. • Zorg voor een proces, om de actualiteit van de verwerkersovereenkomst periodiek te controleren.

4. Informatiebeveiliging en bewustwording

Voor informatiebeveiliging wordt vooral gebruik gemaakt van de diensten van gemeente Leeuwarden, als SSC-partner. Daarnaast is er sprake van samenwerking met de verschillende Waddeneilanden.

Bevinding	• Informatiebeveiliging is onderdeel van het contract met gemeente Leeuwarden. • Er is sprake van samenwerking met een van de gemeenten op het gebied van applicaties; • Er is inzicht in de deelname aan e-learning ARDA; • De deelname aan ARDA wordt in werkoverleggen besproken; • Afwijkingen in de deelname wordt met medewerkers besproken.
------------------	--

5. Bewaar- en vernietigingsbeleid

In de GR staat informatie opgenomen over de locatie van het archief voor de stukken van de GR. In het verwerkingsregister staan de bewaartermijnen opgenomen van de verschillende verwerkingen. Dat betekent dat documenten, die niet langer bewaard mogen worden, vernietigd moeten worden. Dit moet door de Archivaris worden goedgekeurd.

Bevinding	• In de GR staat informatie over locatie van het Archief; • In het verwerkingsregister staat informatie over bewaartermijnen; • De FG heeft geen inzage in vernietigingsbesluiten; • Er zijn nog geen werkprocessen opgesteld voor het vernietigen van documenten.
Advies	• Beschrijf processen voor het vernietigen van documenten na het aflopen van de bewaartermijn; • Zorg voor overleg met de Archivaris in verband met de vernietiging van documenten; • Stel de FG in staat om hier toezicht op uit te kunnen oefenen.

Deel 2. Vooruitkijken naar 2026

Op basis van de bevindingen over 2025 doet de FG de hieronder beschreven aanbevelingen. De aanbevelingen zijn 'risico gebaseerd'. Deze worden aangevuld met ontwikkelingen op het gebied van digitalisering en wetgeving, waar dit jaar aandacht aan gegeven moet worden.

Aanbevelingen

- **Aandacht hebben voor de uitvoering van de DPIA's**

Ten aanzien van het uitvoeren van DPIA's is er afgelopen jaar een start gemaakt, mede door de extra inzet van de externe privacy officer. Maar dit is nog steeds slechts het begin. Er moet eerst een pre-DPIA worden uitgevoerd en daarna de nodige DPIA's uitvoeren.

Dit gaat nog wel de nodige tijd kosten en dus is het aan te raden om hiervoor een plan van aanpak op te zetten. Aangezien veel processen en gebruikte systemen bij gegevens verwerkingen in veel gemeenten identiek zijn, kan hiervoor de samenwerking gezocht worden met andere gemeenten of gebruik te maken van de DPIA-bibliotheek van de IBD/VNG.

- **Aandacht blijven houden voor privacy onder medewerkers**

De mens is de belangrijkste schakel in het vertrouwelijk houden van persoonsgegevens en voorkomen van datalekken. Het creëren van meer bewustwording zal sterk bijdragen aan een informatieveilig werken. Een van de manieren waarop dit vormgegeven wordt is via de e-learning ARDA. Maar daarvoor is wel een hogere deelname-graad nodig. Aandacht daarvoor vanuit leidinggevenden is cruciaal hierin.

Maar er is meer nodig. Medewerkers hebben, afhankelijk van hun functie, ook kennis nodig over specifieke onderwerpen zoals:

- Wanneer een verwerkersovereenkomst moet worden afgesloten en wat daarbij van belang is;
- Welke informatie nodig is voor het opstellen van het verwerkingsregister;
- Wanneer informatie wel of niet mag worden gedeeld en welk afwegingskader daarbij kan worden gebruikt;
- Hoe een DPIA uit te voeren en wanneer dit verplicht is.

Bovenstaande zal niet alleen helpen bij de uitvoering van DPIA's, het actueel houden van het verwerkingsregister en het (tijdig) melden van datalekken, maar vooral ook bij het zo veel mogelijk veilig en privacy bewust werken.

Daarnaast maakt de gemeente ook meer en meer gebruik van Algoritmen en AI. Ook hierbij spelen AVG en privacy een rol, met name wanneer bij de inzet daarvan persoonsgegevens worden gebruikt en vooral wanneer de uitkomsten van deze AI-tools gevolgen voor individuele betrokkenen kunnen hebben. Medewerkers hebben hierbij ook meer kennis nodig om op basis daarvan ook meer risicobewustzijn te ontwikkelen en te weten wanneer bij het gebruik van Algoritmes extra onderzoek nodig is naar risico's.

Hierbij is naast de DPIA vaak ook een aanvullend onderzoek nodig: de IAMA ofwel 'Impact Assessment Mensenrechten en Algoritmes'. De FG beveelt aan om na te gaan hoe het proces van de IAMA gecombineerd kan worden met die van de DPIA.

- **Aandacht hebben voor het Algoritmeregister**

Hoewel het register nog niet verplicht is, zal dat niet zo lang meer duren. Gemeente Ameland is aangesloten op het landelijk format van het algoritmeregister, maar het register is niet volledig gevuld en daarmee niet actueel. Het probleem ligt hierbij in het eigenaarschap; mij is niet bekend wie verantwoordelijk is voor het invullen van het register. Het is zaak dit duidelijk te maken en actie hierop in te zetten. Zeker nu er diverse ontwikkelingen zijn op het gebied van digitalisering en AI.

Ontwikkelingen op het gebied van digitalisering en wetgeving

Voor het komende jaar zijn er ontwikkelingen die gegevensbescherming raken en daarmee de nodige aandacht vragen. Het algoritmeregister, de AI Act en de daarmee samenhangende digitale weerbaarheid en tenslotte de Wet gegevensdeling door samenwerkingsverbanden zijn daar voorbeelden van. Ook de AP noemt een aantal van deze zaken in haar jaarplan. Het is goed om een aantal van deze punten mee te nemen in het eigen jaarplan.

Jaarplan AP:

De AP heeft haar [jaarplan](#) voor 2026 gepubliceerd, waarin drie thema's centraal: massasurveillance, AI en digitale weerbaarheid.

1. Massasurveillance: inclusief tracking

De AP kijkt bij massasurveillance niet alleen naar cameratoezicht of opsporingspraktijken, maar ook naar de manier waarop mensen online gevolgd worden. Tracking en cookies worden daarbij ook geplaatst onder het bredere begrip surveillance.

2. AI: regels moeten vooraf duidelijk zijn

De AP ziet dat AI zich razendsnel ontwikkelt en steeds vaker invloed heeft op beslissingen die mensen direct raken. Denk aan selectie, beoordeling, risicoprofilering of geautomatiseerde dienstverlening. Dat brengt reële risico's mee, zoals discriminatie, desinformatie en verlies van menselijke autonomie. Ingrijpen achteraf bij AI-systemen is vaak moeilijk of zelfs onmogelijk. Zodra systemen eenmaal draaien en persoonsgegevens zijn verwerkt, zijn fouten en ongewenste effecten niet eenvoudig terug te draaien.

Duidelijke kaders vooraf zijn effectiever dan correcties achteraf. Transparantie, uitlegbaarheid en het voorkomen van structurele bias worden daarbij steeds belangrijker. Deze preventieve insteek sluit aan bij de Europese AI-wetgeving, waarin risicogericht toezicht en waarborgen aan de voorkant centraal staan. AI-governance is dan ook geen toekomstvraag meer. Wanneer AI wordt ingezet in processen waar persoonsgegevens een rol spelen, moet vooraf nagedacht worden over controle, verantwoording en waarborgen, voordat toezicht, klachten of maatschappelijke discussie volgen.

3. Digitale weerbaarheid: grip op digitale afhankelijkheden

Burgers en organisaties worden steeds afhankelijker van digitale diensten en infrastructuren, juist ook bij essentiële publieke processen. Die afhankelijkheid vergroot de impact van verstoringen, datalekken of misbruik van persoonsgegevens. Digitale weerbaarheid gaat verder dan technische beveiliging alleen. Het raakt aan de vraag hoe je omgaat met leveranciers, ketens en data en hoe zij zorgen dat digitale dienstverlening betrouwbaar blijft. Vertrouwen in digitale systemen wordt een structurele randvoorwaarde.

Dit is dan ook hét moment om privacy en AI-governance vooraf in te bouwen. Door nu al na te denken over transparantie, verantwoord datagebruik en digitale weerbaarheid, voorkom je reputatierisico's en ingrijpend toezicht achteraf.

Bijlage 1 - Stand van zaken AVG per onderwerp

Dit is het dashboard dat voortkomt uit het invullen van het Borgingsproduct van de VNG. Het Borgingsproduct beschrijft precies wat geregeld moet zijn om als organisatie aan de AVG te voldoen.

Per onderdeel leidt het antwoord op de vragen tot een percentage. Dat percentage geeft vervolgens aan in hoeverre de organisatie voldoet aan dat specifieke onderdeel. Op dit moment wordt de vragenlijst gemeentebreed ingevuld door de contactpersoon van gemeente Ameland en de CISO voor informatiebeveiliging. Om tot een score te komen die inzage geeft in een sector of zelfs een team, zouden de hoofdstukken 2, 4, 5 en 6 door de verschillende managers ingevuld moeten worden.

Paragraaf	Titel	Percentage
1.	Beleid	68%
1.1	Beleid vaststellen	0%
1.2	Privacybeleid	69%
1.3	Verantwoordelijkheden	88%
2.	Processen	64%
2.1	Werkprocessen	46%
2.2	Verwerkingsregister	85%
2.3	Pre-DPIA's	0%
2.4	DPIA's	60%
2.5	Bewaar- en vernietigingsbeleid	81%
3.	Organisatorische inbedding	84%
3.1	Privacyteam	75%
3.2	Aanstelling, positie en taken FG	93%
3.3	Informereren OR	75%
3.4	Bewustwording	70%
4.	Rechten van betrokkenen	84%
4.1	Recht op informatie	90%
4.2	Processen rechten van betrokkenen	100%
4.3	Toestemming	81%
4.4	Geautomatiseerde individuele besluitvorming	30%
4.5	Websites en applicaties	100%
4.6	Technische ondersteuning	100%
5.	Samenwerking	75%
5.1	AVG rollen	63%
5.2	Gegevensverstrekking	89%
6.	Gegevensbescherming	81%
6.1	Risico's	100%
6.2	Gegevensbescherming door ontwerp	88%
6.3	Gegevensbescherming door standaardinstellingen	75%
6.4	Informatiebeveiliging	64%
6.5	Privacyincidenten en datalekken	92%
7.	Verantwoording	57%
7.1	Evaluatie naleving AVG	25%
7.2	Evaluatie informatiebeveiliging	100%
7.3	Rapportage	100%