

Jaarverslag 2024

Gegevensbescherming

Gemeente Meierijstad



Functionaris Gegevensbescherming
Gemeente Meierijstad
Datum: juli-2025
fg@meierijstad.nl



Inhoudsopgave

1.	Inleiding	2
	Leeswijzer jaarverslag	2
2.	Deel A: AVG	3
	2.1. AVG-dashboard	3
	2.2. Deel 1. Terugblik op 2024	4
	2.3. Deel 2. Vooruitkijken naar 2025	9
3.	Deel B: WPG	13
	3.1. Inleiding	13
	3.2. Wpg-dashboard	13
	3.3. Taak van de FG	14
	3.4. Bevindingen en aanbevelingen jaar 2024	14
	3.5. Audit WPG	15
	3.6. Vooruitblik jaar 2025	15
4.	Deel C: Ontwikkelingen	16
	4.1. Dreigingsbeeld 2025-2026	16
	Bijlage 1 - Kengetallen AVG	17

1. Inleiding

Sinds de invoering van de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg), is de Functionaris Gegevensbescherming (FG) voor gemeenten de onafhankelijke toezichthouder op de naleving van de AVG/Wpg, gerelateerde wetgeving en beleidsafspraken. De FG adviseert de gemeente en brengt rechtstreeks verslag uit aan het college.

Het doel van dit jaarverslag is om als onafhankelijk toezichthouder de hoogst leidinggevende van de organisatie rechtstreeks te informeren over privacy en gegevensbescherming binnen de gemeente Meierijstad. Daarmee voldoen wij aan de wettelijke verplichtingen van de AVG (artikel 38 lid 3) en de Wpg (artikel 34 lid 3).

Door rechtstreeks verslag uit te brengen, krijgt het bestuur de kans om zijn rol goed te vervullen. Deze rol richt zich met name op het realiseren van de AVG-doelstellingen en het waarborgen van goed bestuur in het huidige digitale tijdperk. Bestuurlijke borging, regievoering, risicomanagement en verantwoordingsplicht zijn hiervan belangrijke pijlers. Dit kan alleen bereikt worden als het bestuur hierover in voldoende mate wordt geïnformeerd. Het jaarverslag draagt hieraan bij.

In dit jaarverslag over het jaar 2024 wordt aan de hand van de zeven thema's uit het AVG borgingsproduct van de Informatiebeveiligingsdienst (IBD) en de Wpg thema's op hoofdlijnen ingegaan. De stand van zaken en de status van alle verplichte privacy normen (AVG en Wpg) en de bevindingen daarover zijn in dit verslag vastgelegd. Daarnaast worden per thema de belangrijkste aandachtspunten en aanbevelingen voor het komende jaar aangegeven.

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:

1. 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;
2. Vervolgens worden per thema de bevindingen en aanbevelingen beschreven;
3. In de bijlage wordt het overzicht met kengetallen over het jaar 2024 weergegeven.

2. Deel A: AVG

2.1. AVG-dashboard

Onderstaand dashboard geeft een globaal beeld van de stand zaken rondom de borging en naleving van de AVG binnen de gemeente Meierijstad. Dit beeld is niet gebaseerd op objectieve criteria maar op subjectieve criteria en interpretaties van de FG. De beoordeling is kwalitatief door de FG uitgevoerd door directe toetsing aan de AVG. De kwalitatieve beoordeling is gebaseerd op gesprekken, documenten, periodiek overleg, adviesaanvragen, uitgevoerde risicoanalyses en zo nodig klachtonderzoek (inspectie) of ander contact.

De resultaten worden hieronder per thema kort toegelicht.

Thema:	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

2.2. Deel 1. Terugblik op 2024

In dit deel van de rapportage kijk ik vanuit mijn rol als FG terug op wat de gemeente Meierijstad in 2024 heeft bereikt en welke werkzaamheden en bevindingen ik heb gedaan als toezichthouder.

2.2.1. Beleid

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

Daarin moet de digitalisering en de opkomst van nieuwe technologieën zoals robotisering, algoritmes en kunstmatige intelligentie (generatieve AI) worden meegenomen. Vanuit de AVG en de menselijke maat bekeken moet daarbij niet alleen de vraag 'mag of kan dit wel', maar ook de vraag 'moet je dit wel willen' centraal staan.

Onder het strategisch beleid kunnen in de toekomst alle tactische beleidsuitwerkingen zoals rechten van betrokkenen, melding datalekken, privacy by design en default, etc. en operationele uitwerkingen zoals privacy procedures, instructies, handreikingen en overige producten worden gehangen. Op die manier kan er meer samenhang tussen de diverse privacy beleid- en uitvoeringsdocumenten worden gebracht.

Uitgevoerde werkzaamheden/bevindingen:

- De geldigheid van zowel het bestaande strategisch privacybeleid als het informatieveiligheidsbeleid liep in 2024 af. Beide beleidsdocumenten zijn in 2024 met een jaar verlengd met daarin de kanttekening dat deze eerder vervangen kunnen worden.
- Op strategisch niveau moet het strategisch privacybeleid en informatieveiligheidsbeleid worden geactualiseerd op basis van de nieuwe wet- en regelgeving en wereldwijde en landelijke (zowel technologische als maatschappelijke) ontwikkelingen. Dit strategisch beleid zal richting moeten geven aan de koers van de organisatie voor de komende jaren. Onderdelen van deze strategische koers zijn een missie en visie van gemeente Meierijstad en concrete doelstellingen. Dit zal uiteindelijk resulteren in concrete plannen (routekaart) voor het bereiken van deze doelen. Daarnaast zal het strategisch beleid de taken en verantwoordelijkheden op het gebied van privacy en informatieveiligheid helder af moeten bakenen.
- Het tactisch privacybeleid met betrekking tot gegevensbescherming en de procedures die daaronder vallen zoals het afhandelen van datalekken, rechten van betrokkenen en DPIA's zijn verouderd of niet formeel opgesteld en/of vastgesteld. Dit beleid en onderliggende processen moeten worden vastgelegd en waar mogelijk gestandaardiseerd zodat er een solide basis ontstaat voor herhaalbare werkzaamheden en het verkleinen van risico's en afhankelijkheden.

2.2.2. Processen

De verwerkingen van persoonsgegevens door de gemeente Meierijstad dienen te voldoen aan de AVG. Dit houdt in dat de gemeente de werkprocessen waarin persoonsgegevens worden verwerkt moet toetsen en inrichten volgens de volgende beginselen:

behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid.

Daarnaast kan het in bepaalde gevallen verplicht zijn om een (pré) data protection impact assessment (DPIA), Impact Assessment voor Mensenrechten bij de inzet van Algoritmes (IAMA) of AI Impact Assessment (AIIA) uit te voeren.

Uitgevoerde werkzaamheden/bevindingen:

- Er ontbreekt op dit moment een organisatie breed uitvoeringsplan om de werkprocessen waarin persoonsgegevens worden verwerkt goed te kunnen inrichten en toetsen. Dit uitvoeringsplan is randvoorwaardelijk om handen en voeten te geven aan de doorontwikkeling en verdere implementatie (inrichting en werking) van privacy en informatieveiligheid binnen gemeente Meierijstad. Het uitvoeringsplan moet conform de PDCA-methodiek concreet worden gemaakt aan de hand van jaarplannen die halfjaarlijks worden geactualiseerd. De verantwoordelijkheid voor het op- en vaststellen van het uitvoeringsplan ligt bij het DT en de uitvoering daarvan door middel van een jaarplan ligt bij het atelier Informatiestrategie.
- De stand van zaken m.b.t. de AVG is nog niet op basis van een normenkader met behulp van een meting (GAP-analyse/0-meting) objectief in kaart gebracht (zie ook inleiding bij 3.1 AVG Dashboard). Door dit in kaart te brengen kan het huidige volwassenheidsniveau voor privacy en informatieveiligheid op zowel organisatie- als procesniveau worden bepaald. Een Privacy Management Systeem (PMS) kan hierbij als hulpmiddel dienen. Binnen de gemeente Meierijstad zijn er al aantal plannen om hiermee aan de slag te gaan, dit is echter tot op heden nog niet van grond gekomen. Om ook op procesniveau de privacy beginselen goed te kunnen borgen moeten er op dit gebied stappen gezet worden.
- Specifieke aandacht moet besteed worden aan de opzet, bestaan en werking van privacy borging in de kritische processen waarover verantwoording moet worden afgelegd door middel van audits. Binnen de gemeente zijn dat op dit moment processen waarin gebruik wordt gemaakt van Suwinet, strafrechtelijke gegevens (Wet politiegegevens) en bijzondere/gevoelige persoonsgegevens. Met behulp van een PMS of iets soortgelijks kan de opzet, bestaan en werking van de privacy beheersmaatregelen worden vastgelegd, geborgd en inzichtelijke worden gemaakt voor interne en externe audits. Met opzet, bestaan en werking wordt het volgende bedoeld:
 - o Opzet: je hebt nagedacht - ook wel: 'ontworpen' - en dit vastgelegd in beleid.
 - o Bestaan: fysiek vastgelegde maatregelen en procedures, processen en werkwijzen.
 - o Werking: dat wat er is bedacht, werkt ook nog eens effectief in de praktijk en is aantoonbaar
- In 2024 zijn er op vier processen volledige DPIA's uitgevoerd om de risico's van de gegevensverwerking/proces in kaart te brengen. Zowel het proces als de inhoud van de uitgevoerde DPIA's moet worden verbeterd. Dit kan gedaan worden door dit meer vanuit een organisatie brede risicomanagementaanpak uit te voeren. Waarbij de rol en verantwoordelijkheid van de proceseigenaar bij het accepteren/mitigeren van risico duidelijk naar voren wordt gebracht.

In bijlage 1 is een overzicht opgenomen van de in 2024 uitgevoerde DPIA's.

2.2.3. 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.

Uitgevoerde werkzaamheden/bevindingen:

- In 2024 zijn er diverse personele wisselingen binnen het IV&P team geweest. Hierdoor is er afgelopen jaar niet structureel aandacht besteed aan organisatorisch inbedding van privacy in de organisatie. Er zijn diverse losse acties uitgevoerd onder andere op het gebied van bewustwording zoals het uitvoeren

van een Mystery guest-onderzoek, awareness meting en een IV&P pubquiz gedaan. Verder zijn de privacy trainingen voor nieuwe medewerkers een aantal keer uitgevoerd.

- Naar aanleiding van het programma 'organisatieontwikkeling' is het aantal leidinggevenden binnen de gemeente Meierijstad het afgelopen jaar toegenomen. Deze leidinggevenden vullen een cruciale rol in om gezamenlijk te werken aan een veilige en privacybewuste organisatie. Het activeren van het management is niet alleen essentieel in het kader van de AVG, maar ook in het kader van de NIS2 (Cyberbeveiligingswet) en BIO(2). Het management speelt een sleutelrol bij het effectief managen van (privacy)risico's die de continuïteit van gemeentelijke processen en informatiesystemen negatief kunnen beïnvloeden. Deze (privacy)risico's hebben direct en indirect impact op onze inwoners. Het kernwoord hierbij is verander- en risicomanagement. Voor gemeente Meierijstad betekent dit een verschuiving in focus: van technische oplossingen naar interne samenwerking, kennisdeling en cultuurontwikkeling, zodat iedere leidinggevende in de organisatie zijn of haar verantwoordelijkheid voor privacy en informatiebeveiliging begrijpt en oppakt.
- Risicomanagement is een belangrijke pijler van zowel informatiebeveiliging als privacy. Binnen de huidige inrichting is risicomanagement op het gebied van privacy onvoldoende geborgd in de organisatie. De belangrijkste vraag is, hoe kan gemeente Meierijstad informatieveiligheid en privacy vanuit risicomanagement perspectief goed borgen in de bestaande (besluitvormings)processen? Zodat de proceseigenaren en daarmee ook het SLIM/DT hierop beter kan sturen en het team IV&P ook meer in positie wordt gebracht om mee te kunnen denken en te adviseren. Vanuit Auditing, Processen en Kwaliteit (APK) is de concerncontroller vanuit zijn rol ook bezig om vanuit een risicomanagementaanpak aan de slag te gaan met de verschillende risico's die voorkomen in een gemeentelijke organisatie.

2.2.4. Rechten van betrokkenen

De gemeente 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 ervoor te zorgen dat de betrokkenen deze rechten ook daadwerkelijk kunnen uitvoeren.

Uitgevoerde werkzaamheden/bevindingen:

- Het afgelopen jaar zijn alle ingediende verzoeken binnen de termijn opgepakt en afgehandeld. Er is echter geen formeel beleid en procedure voor het afhandelen van rechten van betrokkenen vastgesteld. Daarnaast is het nog niet mogelijk om via DigiD digitaal een verzoek in te dienen. Identificatie kan daardoor, mits de juiste gegevens bekend zijn, telefonisch gedaan worden (dit is echter verboden door de Autoriteit Persoonsgegevens) of fysiek op locatie en dat zorgt voor onnodige drempels om een verzoek in te kunnen dienen.

In bijlage 1 is bij de kengetallen onder andere een overzicht opgenomen van het aantal verzoeken van betrokkenen voor het jaar 2024.

2.2.5. Samenwerking

De gemeente Meierijstad 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 Meierijstad maakt hierover afspraken met deze andere partijen.

Uitgevoerde werkzaamheden/bevindingen:

- De samenwerkingen met leveranciers en andere organisatie zijn via de IT-architectuur in kaart gebracht. Vanuit IT-architectuur is het echter niet mogelijk om samenwerkingen met (mede) overheden, hulpverlenings- en vrijwilligersorganisaties en andere externe organisaties in kaart te brengen die buiten onze IT-architectuur om met ons samenwerken. Binnen het Sociaal Domein en Openbare Orde & Veiligheid vinden veel van dit soort formele en informele samenwerkingen plaats, waarbij in bijna alle gevallen persoonsgegevens worden uitgewisseld. In veel gevallen worden met deze partijen (verwerkers)overeenkomsten afgesloten, maar wij hebben niet altijd zicht op de gevallen waarin wij gezamenlijk verwerkingsverantwoordelijk zijn of gegevens worden overgedragen aan een derde partij. Vanuit de organisatie ontbreekt er een concreet zicht op en dit wordt nergens centraal beheerd in bijvoorbeeld een verwerkingsregister.
- Vanuit de gemeente zijn er ook plannen om vanuit het sociaal domein meer integraal te gaan werken met hulpverleningsorganisaties. Dit wordt onder andere concreet gemaakt door op bepaalde locaties fysiek te gaan samenwerken met deze organisaties. Dit heeft als gevolg dat de samenwerking met deze organisatie gaat veranderen en dat hiervoor nieuwe afspraken, overeenkomsten/convenanten, werkinstructies en communicatie opgesteld zullen moeten worden om de risico's voor de cliënten op privacy gebied zo klein mogelijk te houden. Op dit moment ontbreekt er ook nog een wettelijke grondslag om volledig integraal te werken binnen het sociaal domein. De Wet aanpak meervoudige problematiek in het sociaal domein (Wams) zou dit probleem moeten oplossen. Dit wetsvoorstel is echter in 2023 controversieel verklaard en sindsdien nog niet in behandeling genomen door het (ondertussen ook al demissionair verklaard) kabinet.

2.2.6. Beveiliging

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

Uitgevoerde werkzaamheden/bevindingen:

- Doordat er vanuit informatieveiligheid en privacy gezamenlijk wordt gewerkt, zijn er korte lijntjes met betrekking tot het beoordelen en afhandelen van beveiligingsincidenten en datalekken. Dit zorgt ervoor dat incidenten en datalekken snel opgepakt worden en indien nodig direct geschakeld kan worden met derden om passende technische en organisatorische maatregelen te nemen.
- De gemelde incidenten en datalekken zijn in het afgelopen jaar allemaal opgepakt en afgehandeld. Dit is op basis van niet vastgelegde afspraken gedaan. Voor het afhandelen van incidenten en datalekken is er geen concreet beleid, procedure en processen opgesteld en vastgesteld. De registratie van datalekken heeft ook niet volledig gecentraliseerd plaatsgevonden. Dit moet worden verbeterd zodat er een basis ontstaat waarin werkzaamheden herhaalbaar en de risico's en afhankelijkheden minder groot worden. In bijlage 1 is een overzicht opgenomen van het aantal privacy incidenten in 2024.

2.2.7. Verantwoording

De verantwoordelijkheid om aan te tonen of en in welke mate wordt voldaan aan de privacyregels ligt bij de gemeente. 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.

Uitgevoerde werkzaamheden/bevindingen:

- Begin 2024 heeft er een beeldvormende avond met de gemeenteraad over informatieveiligheid, privacy en ethiek plaatsgevonden. Het doel van deze avond was om de gemeenteraad te informeren over waar de organisatie mee bezig is met betrekking tot deze onderwerpen en een beeld te schetsen welke onderwerpen op dit moment actueel zijn. Daarover konden aanvullende vragen gesteld worden en werd er inhoudelijk gediscussieerd.
- De gemeente Meierijstad heeft zich afgelopen jaar ook aangemeld bij het algoritmeregister. In het Algoritmeregister van de overheid publiceren Nederlandse overheidsorganisaties informatie over algoritmes die zij gebruiken in hun werk. Het register focust op impactvolle algoritmes (waaronder hoog risico AI-systemen) en geeft de bezoeker inzicht in hoe deze algoritmes werken. Vanuit Meierijstad zijn de eerste twee AI-systemen (algoritmes) met een beperkt risico gepubliceerd in het register. Zie website van algoritmeregister voor meer informatie: <https://algoritmes.overheid.nl/nl/organisatie/gemeente-meierijstad>
- In 2024 is er ook door middel van interviews met diverse intern verantwoordelijken een privacy 0-meting uitgevoerd. De resultaten hiervan zijn eind vorig jaar besproken met directeur Bedrijfsvoering en leidinggevende van het IV&P team. De belangrijkste aandachtspunten uit deze 0-meting zijn daarnaast verwerkt in dit jaarverslag en worden door de strategisch adviseur IV&P indien nodig in de plannen van aanpak voor de komende jaren opgenomen.
- Het versterken van het interne toezicht op besluitvorming en opvolging van privacyadviezen en DPIA's krijgen nu onvoldoende aandacht. Door tijdige en gestructureerde controles kunnen privacyrisico's beter worden geïdentificeerd en beheerst, waardoor onbewuste en bewuste risico's worden beperkt. Proactieve controles kan negatieve beoordelingen van adviezen voorkomen en reduceert de noodzaak van ingrijpende aanpassingen achteraf.
- Vanwege beperkte beschikbare capaciteit kan de Functionaris Gegevensbescherming niet alle wettelijke verplichtingen volledig invullen, waardoor het toezicht voornamelijk op afstand en reactief plaatsvindt.

2.2.8. Conclusie

Het jaar 2024 kan gezien worden als een tussenjaar als het gaat over de implementatie van privacy/gegevensbescherming binnen de gemeente Meierijstad. De lopende werkzaamheden zijn opgepakt. Dat er geen stappen vooruit zijn gezet heeft te maken met diverse personele wisselingen binnen het IV&P team en de beperkte capaciteit om naast de lopende werkzaamheden ook vanuit een gestructureerde aanpak privacy verder te borgen in de organisatie. Het beeld is over het algemeen een krappe voldoende, maar de basis is voldoende om goede stappen vooruit te zetten. De komende jaren zullen er serieuze stappen gezet moeten worden om doorontwikkeling en verdere implementatie van privacy in alle lagen van de organisatie voor elkaar te krijgen. Door gezamenlijk vanuit alle lagen in de organisatie aan de slag te gaan met gegevensbescherming kan de interne en externe dienstverlening worden verbeterd, het vertrouwen van de burger in de gemeente worden vergroot en kan de organisatie risicobewust aan de slag met alle nieuwe (digitale) mogelijkheden en ontwikkelingen.

2.3. Deel 2. Vooruitkijken naar 2025

In dit deel van de rapportage worden per thema de belangrijkste aanbevelingen voor de komende jaren gegeven.

2.3.1. Beleid

Aanbeveling	Prioritering	Planning (advies)
1. Actualiseer het bestaande strategisch beleid informatieveiligheid en privacy.	Hoog	2025
2. Actualiseer het bestaande tactisch privacybeleid	Midden	2025

2.3.2. Processen

Aanbeveling	Prioritering	Planning (advies)
3. Actualiseer de procedures m.b.t. het afhandelen van datalekken en incidenten, rechten van betrokkenen en DPIA's. En leg de daaronder liggende privacy processen vast en zorg voor zoveel mogelijk standaardisatie zodat er een basis ontstaat waarin werkzaamheden herhaalbaar en de risico's en afhankelijkheden minder groot worden.	Midden	2025
4. Bepaal aan de hand van 0-meting/GAP analyse het volwassenheidsniveau voor privacy.	Hoog	2025
5. Ga met behulp van een PDCA-cyclus aan de slag met het inrichten, implementeren, onderhouden en continu verbeteren van gegevensbescherming in de organisatie.	Midden	2026

6. Breng de privacy risicovolle processen in kaart en controleer of er DPIA's daarop zijn uitgevoerd. Stel op basis daarvan een risico gebaseerde routekaart op om de achterstanden op dit gebied weg te werken.	Laag	2026
--	------	------

2.3.3. Organisatorische inbedding

Aanbeveling	Prioritering	Planning (advies)
7. Stel vanuit het IV&P team een bewustwordingsplan op waarin bepaalde doelen (bewust bekwaam) worden gesteld en voer deze uit.	Midden	2026
8. Zorg ervoor dat alle leidinggevendenden voldoende gefaciliteerd worden om hun rol als proceseigenaar op het gebied van Informatieveiligheid en privacy in te kunnen vullen.	Midden	2026/2027
9. Zorg ervoor dat de verantwoordelijken (proceseigenaren, SLIM, DT, college etc) kunnen sturen op privacy en informatiebeveiligingsrisico's en het IV&P team in positie wordt gebracht om hierover te adviseren. Neem het onderwerp gegevensbescherming bijvoorbeeld mee in de intaketafels die worden georganiseerd om eventuele risico's van nieuwe projecten vooraf te beoordelen.	Midden	2026
10. Ga aan de slag met gegevensbescherming vanuit een risicomanagement aanpak. Sluit daarbij aan op de risicomanagement aanpak die door de concerncontroller vanuit APK wordt ontwikkeld.	Midden	2025/2026

2.3.4. Rechten van betrokkenen

Aanbeveling	Prioritering	Planning (advies)
11. Stel een procedure Rechten van betrokkenen op en zorg voor digitaal aanvraagformulier inclusief mogelijkheid tot digitale identificatie via DigiD. Zie ook aanbeveling 3.	Midden	2025

2.3.5. Samenwerking

Aanbeveling	Prioritering	Planning (advies)
12. Breng risico gebaseerd alle samenwerkingen waarin persoonsgegevens worden uitgewisseld buiten de IT-architectuur om in kaart en leg dit vast in het verwerkingsregister. Focus in eerste instantie met name op hoog risico domeinen zoals het Sociaal Domein en Openbare Orde & Veiligheid.	Midden	2026
13. Voer een risicoanalyse (DPIA) uit op de plannen om vanuit het Sociaal Domein integraal te gaan werken. Gebruik de uitkomsten uit deze risicoanalyse om de risico's voor de cliënten zo klein mogelijk te houden en indien nodig de restrisico's door de proceseigenaar en/of eindverantwoordelijke te accepteren.	Midden	2025

2.3.6. Beveiliging

Aanbeveling	Prioritering	Planning (advies)
14. Actualiseer de bestaande procedures en procesbeschrijvingen met betrekking tot het afhandelen van datalekken en incidenten. Zie ook aanbeveling 3.	Midden	2025

2.3.7. Verantwoording

Aanbeveling	Prioritering	Planning (advies)
15. Zorg voor goede interne controleprocessen op besluitvorming en/of opvolging van privacy adviezen/DPIA's. Hiervoor gelden de volgende uitgangspunten: - o Voer risicoanalyses (DPIA's) vooraf uit voordat een proces, project of ontwikkeling wordt geïmplementeerd. - o Leg adviezen, risico's en besluitvorming zwart op wit vast in het besluitvormingsproces en indien nodig in een risicoregister. - o De proceseigenaar is verantwoordelijk voor de uitvoering van de resultaten uit risicoanalyses. Aanpakken risico's (mitigeren, delegeren, accepteren, etc.). - o Er vindt toetsing plaats op de opvolging van de privacy-adviezen/DPIA's en privacy is vanuit risicomanagementperspectief een vast onderdeel van ambtelijke en bestuurlijke besluitvorming.	Midden	2025/2026
16. Evalueer de huidige positie en tijdsinzet van de huidige FG.	Hoog	2025

2.3.8. Conclusies

Er is op het gebied van privacy/gegevensbescherming genoeg te doen binnen de gemeente Meierijstad. Om proactief aan de slag te gaan met de doorontwikkeling en verdere implementatie van privacy in de organisatie moet minimaal het volgende worden opgepakt:

1. Bepaal de koers voor de komende jaren waarnaartoe de organisatie wil gaan groeien.
2. Maak deze koers concreet aan de hand van doelstellingen, concrete acties en een meerjarenplanning (routekaart).
3. Zorg voor een duidelijke afbakening van de taken en verantwoordelijkheden op het gebied van privacy en wijs verantwoordelijken aan voor de uitvoering van de acties.
4. Evalueer en stel jaarlijks een nieuw jaarplan op waarmee je uitvoering geeft aan de koers en de meerjarenplanning.

3. Deel B: WPG

3.1. Inleiding

De FG houdt toezicht 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. In dit jaarverslag staat beschreven welke acties en maatregelen in 2024 zijn genomen om de doelstellingen en beginselen uit de Wet politiegegevens (Wpg) te behalen en te waarborgen.

3.2. Wpg-dashboard

Onderstaand Wpg-dashboard geeft een globaal beeld van de stand zaken rondom de borging en naleving van de Wpg binnen de gemeente Meierijstad. Dit beeld is gebaseerd op de resultaten uit de interne en externe audits die de afgelopen jaren zijn uitgevoerd.

Thema:	2024	2025
Borging WPG	Resultaat	Verwacht
Beleid		
Bewustwording		
Autorisatieproces		
Bewaartermijnen		
Verstrekken van persoonsgegevens		
DPIA		
Register van verwerkingen		
Auditverplichting		
FG-toezicht		

Legenda:

	AANDACHT VEREIST VAN MANAGEMENT
	IN TE HALEN ACHTERSTAND
	OP SCHEMA

3.3. Taak van de FG

De taken van de FG (artikel 36 Wpg) met betrekking tot de Wpg kunnen als volgt worden 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;

3.4. Bevindingen en aanbevelingen jaar 2024

Onderwerp	Bevindingen	Aanbeveling
Beleid	Er is nog geen intern Wpg beleid	Opstellen van een tactisch Wpg beleid en de Wpg kaders verwerken in het nog op te stellen strategisch IV&P beleid.
Bewustwording	Er wordt intern weinig aan bewustwording over de Wpg en de geheimhoudingsplicht voor de aangestelde BOA's gedaan.	Stel een bewustwordingsprogramma op over de Wpg voor de aangestelde BOA's en neem dit op in de aanstellingsprocedure en zorg voor jaarlijkse training van de nieuwe en huidige BOA's.
Autorisatieproces	Er is geen autorisatieprocedure en autorisatiematrix.	Stel een autorisatieprocedure en autorisatiematrix op en maak deze aantoonbaar (opzet, bestaan en werking).
Bewaartermijnen	Door middel van de TPM heeft CityControl aangetoond dat zij conform de wettelijke eisen van de Wpg politiegegevens bewaren.	-
Verstrekken van politiegegevens	In het handboek Wpg wordt onvoldoende aandacht besteed aan de wettelijke kaders met betrekking tot het verstrekken van politiegegevens.	Actualiseer het handboek Wpg op dit punt en zorg ervoor dat de verstrekkingen getoetst worden aan de wettelijke kaders en dat deze worden geregistreerd.
DPIA	Er is nog geen DPIA op de applicatie CityControl en het proces uitgevoerd.	Voer een DPIA op de applicatie en het proces uit.
Register van verwerkingen	Het verwerkingsregister is niet actueel. Huidige Wpg processen zijn daarin niet opgenomen.	Actualiseer het verwerkingsregister en maak deze volledig.

Onderwerp	Bevindingen	Aanbeveling
Auditverplichting	Over het jaar 2024 is er een interne audit uitgevoerd. De aanbevelingen hieruit zijn opgenomen in het verbeterplan. De resultaten van de interne audit zijn via de rapportage VIC gedeeld met directie.	Voer in het jaar 2025 over het jaar 2025 een interne audit uit en geef de opdracht aan een externe auditor om de externe audit over de jaren 2020 t/m 2024 uit te voeren.
FG-toezicht	De FG heeft in 2024 niet volledig kunnen toezien op de naleving van de Wpg. Hiervoor is een controleplan opgesteld en op basis van de uitgevoerde interne controles kan de FG toezicht houden.	Voer de interne controles op basis van het controleplan uit en informeer de FG over de uitkomsten hieruit.

3.5. Audit WPG

In 2024 is er met ondersteuning van een externe auditor een interne audit over het jaar 2023 uitgevoerd. Deze uitgevoerde interne audit over het jaar 2023 is als basis gebruikt voor de interne audit over het jaar 2024. Deze is zelfstandig door de interne auditor van gemeente Meierijstad uitgevoerd. De rapportages van beide interne audits zijn opvraagbaar bij interne auditor.

3.6. Vooruitblik jaar 2025

Naar aanleiding van eerdere audits is er in 2024 een verbeterplan 2024 opgesteld. Vanuit het team VTH is in samenwerking met de privacy officers en FG hard gewerkt aan het oppakken van alle verbetermaatregelen. Vorig jaar zijn er op dat gebied goede stappen vooruit gezet. Niet alle verbeteracties zijn vorig jaar afgerond. De openstaande acties zijn daarom doorgezet naar het verbeterplan 2025 en daar wordt in 2025 verdere uitvoering aangegeven. De focus ligt daarbij op de hierboven genoemde aanbevelingen en het verder borgen van de opzet, bestaan en werking van alle beheersmaatregelen. De verwachting is ook dat we dit jaar goede stappen vooruit kunnen blijven zetten. Dit moet uiteindelijk resulteren in hogere score op de interne audit over 2025. Let op, in de externe audit van 2025 zullen deze resultaten nog niet zichtbaar zijn. De externe audit wordt namelijk maar één keer in de vier jaar uitgevoerd en zal nu over de periode 2020 tot en met 2024 gaan. De resultaten van 2025 worden daarin niet meegenomen.

4. Deel C: Ontwikkelingen

4.1. Dreigingsbeeld 2025-2026

Ieder jaar wordt door de Informatiebeveiligingsdienst (IBD) van de VNG een algemeen Dreigingsbeeld informatiebeveiliging 2025-2026 gepubliceerd. Dit Dreigingsbeeld Informatiebeveiliging 2025-2026 is speciaal voor (gemeente)bestuurders en de (gemeente)secretaris geschreven. De belangrijkste ontwikkelingen/risico's uit dit dreigingsbeeld zullen hieronder kort worden toegelicht.

Gemeente Meierijstad staat in de komende jaren voor een onverminderd complex digitaal dreigingslandschap. Ransomware, datalekken en uitval van processen door incidenten vormen de grootste bedreigingen. Dit vraagt om een proactieve aanpak om digitale veiligheid te waarborgen en vertrouwen van inwoners en ondernemers te behouden. Dit alles in het licht van algemene organisatieontwikkelingen, bezuinigingen en personele krapte.

4.1.1. Huidige situatie en uitdagingen

- **Ransomware** blijft de grootste dreiging. Criminelen gebruiken kwetsbare systemen om gevoelige data te stelen en organisaties af te persen, met aanzienlijke gevolgen zoals privacyschendingen, imagoschade en financiële verliezen.
- **Incidenten bij leveranciers** leiden tot verstoringen in onze gemeentelijke processen. Als gemeente zijn wij afhankelijk van externe partijen, wat de noodzaak benadrukt van duidelijke afspraken over beveiliging.
- **Beperkte capaciteit, kennis en middelen** bemoeilijken investeringen in digitale veiligheid.

4.1.2. Weerbaarheid

Gemeente Meierijstad kan haar digitale weerbaarheid versterken door:

1. **Basismaatregelen** zoals toegangsbeheer met multifactorauthenticatie, netwerkscheiding, back-ups en monitoring in combinatie met bewustwording op orde te hebben.
2. **Leveranciersmanagement** te verbeteren met expliciete eisen aan informatiebeveiliging en controle hierop.
3. **Samenwerking en standaardisatie** tussen gemeenten te intensiveren om kosten te verlagen en kennis te bundelen

4.1.3. Lange termijn

De opkomst van AI biedt zowel kansen als risico's. AI kan beveiligingsprocessen efficiënter maken, maar wordt ook gebruikt door criminelen voor verfijnde aanvallen zoals deepfake-fraude. Gemeente Meierijstad zal alert moeten blijven op technologische ontwikkelingen.

4.1.4. Conclusie

Digitale veiligheid is geen luxe maar een noodzakelijke voorwaarde voor continuïteit en vertrouwen in onze gemeentelijke dienstverlening. Gemeente Meierijstad moet blijven investeren in bewustwording, technologie en samenwerking om huidige én toekomstige dreigingen effectief het hoofd te kunnen bieden.

Bijlage 1 - Kengetallen AVG

Overzicht (pré)DPIA's

Onderwerp pré DPIA / DPIA light	Datum	Conclusie:
P&O ATS systeem	8-1-2024	DPIA noodzakelijk
Plinkr WGS	17-1-2024	DPIA light noodzakelijk / Afgerond

Onderwerp DPIA	Datum	Status
DPIA ATS systeem	8-1-2024	Afgerond
Regionale DPIA Zorg- en Veiligheidshuis Noordoost Brabant	Januari 2024	Afgerond / Regionaal FG advies
DPIA Divtag	April 2024	Afgerond
DPIA Signalen	Augustus 2024	Afgerond
DPIA Wet Open Overheid	December 2024	In afronding

Overzicht rechten van betrokkenen

Aantal verzoeken	2023	2024
	1	5

Overzicht privacyincidenten

Privacyincidenten	2023		2024	
	Totaal	AP	Totaal	AP
Aantal:	27	1	22	3