FG Jaarverslag (AVG en WPG)
Gemeente Deurne 2024

1. Doel

Het doel van dit jaarverslag is om inzicht te geven in de wijze waarop de Gemeente Deurne invulling geeft aan haar wettelijke verplichtingen op het gebied van gegevensbescherming en informatiebeveiliging, conform de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (WPG).

Met dit verslag wil de gemeente:

- Verantwoording afleggen over de genomen maatregelen en de voortgang van gegevensbescherming binnen de organisatie.
- Inzicht geven in de naleving van de AVG en WPG, inclusief verbeterpunten en aandachtspunten voor de komende periode.
- Bewustwording creëren binnen de organisatie over het belang van privacy en gegevensbescherming.
- Risico's en uitdagingen identificeren die van invloed kunnen zijn op de veilige verwerking van persoonsgegevens.
- Transparantie waarborgen richting het college, de gemeenteraad en andere belanghebbenden over de uitvoering van privacybeleid en informatiebeveiliging.

Dit jaarverslag biedt een evaluatie van de ontwikkelingen en prestaties op het gebied van privacy en gegevensbescherming binnen de gemeente en dient als basis voor verdere verbetering en optimalisatie van de processen in het komende jaar.

Opbouw van het verslag

Voorheen bestonden er voor de AVG twee verschillende formats voor het jaarverslag: één gericht op het College van B&W en één voor de gemeenteraad. In de praktijk blijkt echter dat de Functionaris voor de Gegevensbescherming (FG) één verslag opstelt voor de gehele gemeente, waarin zowel de AVG als de WPG worden behandeld.

Om de verschillen in wetgeving duidelijk te maken, is ervoor gekozen om het verslag op te splitsen in drie delen:

- Deel A: Algemene Verordening Gegevensbescherming (AVG) – Behandelt de naleving van de AVG, inclusief DPIA's, het Register van Verwerkingen en incidentbeheer.
- Deel B: Wet Politiegegevens (WPG) – Beschrijft de naleving van de WPG en de getroffen maatregelen om te voldoen aan de wettelijke eisen.
- Deel C: Ontwikkelingen en toekomstperspectief – Bespreekt belangrijke externe ontwikkelingen die impact hebben op gegevensbescherming binnen de gemeente, zoals de AI Act.

De WPG vereist expliciet een jaarverslag, terwijl voor de AVG het opstellen van een jaarverslag een best practice is. Door beide onderwerpen in één verslag te combineren, wordt het ambtelijke en bestuurlijke proces efficiënter.

Vergelijking van de wetgeving:

Wetgeving	**AVG**	**WPG**
Artikel	Artikel 38 lid 3 AVG	Artikel 34 lid 3 WPG
Omschrijving	De Functionaris voor Gegevensbescherming brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker.	De privacyfunctionaris stelt jaarlijks een verslag op van zijn bevindingen (artikel 34 lid 3 WPG).

Toelichting:
De WPG benoemt expliciet de verplichting van een jaarverslag, terwijl voor de AVG het opstellen van een jaarverslag meer als een best practice wordt beschouwd. Het opstellen van een gezamenlijk verslag voor beide wetgevingen versterkt de rol van de FG binnen de organisatie en maakt het proces zowel intern als extern efficiënter.

Inhoudsopgave

Jaarverslag Gegevensbescherming

Gemeente Deurne

Datum: 19 maart 2025

Functionaris Gegevensbescherming: Natascha Westen

2. Inleiding

Het doel van dit jaarverslag is om inzicht te geven in de wijze waarop de Gemeente Deurne invulling geeft aan haar wettelijke verplichtingen op het gebied van gegevensbescherming en informatiebeveiliging, conform de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (WPG). Dit verslag dient als verantwoording en als instrument om verbeteringen te identificeren.
Door het verslag op te splitsen in AVG, WPG en Ontwikkelingen wordt een duidelijke scheiding aangebracht tussen de verschillende aandachtsgebieden en hun impact op de gemeente.

3. Managementsamenvatting

In 2024 zijn er verbeteringen gerealiseerd in het bijwerken van het Register van Verwerkingen, het uitvoeren van DPIA's en het verbeteren van bewustwording. Tegelijkertijd blijven er uitdagingen bestaan, met name op het gebied van datalekbeheer, monitoring van DPIA-maatregelen en compliance binnen samenwerkingsverbanden.

Belangrijke bevindingen:

- AVG-naleving: Structurele verbeteringen in DPIA's en verwerkingsregister, maar opvolging blijft een aandachtspunt.
- Datalekbeheer: Incidenten worden niet altijd tijdig gerapporteerd, monitoring van trends is noodzakelijk.
- Privacybewustzijn: Trainingen en workshops georganiseerd, maar deelname moet omhoog.
- WPG: Verbeteringen in logging en toegangsbeheer, maar controles moeten structureler.
- Nieuwe wetgeving: Impact van WGS en AI Act vraagt om verdere actie.

A. Deel A: AVG

Het AVG-dashboard geeft een overzicht van de voortgang van de gemeente in de naleving van de AVG. Het gebruikt een stoplichtrapportage om te laten zien waar actie vereist is, en waar de gemeente goed presteert.

2023, 2024, 2025 (verwacht)

Thema	2023	2024	2025 (verwacht)
DPIA's	Actie vereist: Twee nieuwe DPIA's, drie herzien. Geen structurele opvolging.	Verbetering: Vier extra DPIA's, monitoring verbeterd, maar opvolging blijft aandachtspunt.	Op orde: Alle noodzakelijke DPIA's uitgevoerd, met structurele monitoring en opvolging.

Register van Verwerkingen	🔴 Onvoldoende: Beoordeeld als onvoldoende betrouwbaar. Niet alle verwerkingen correct vastgelegd.	🟠 Vooruitgang: Geactualiseerd en uitgebreid met processen in i-Navigator.	🟢 Op orde: Volledig beheer binnen PIMS, continue actualisatie en structurele monitoring.
Datalekkenbeheer	🔴 Risico: Acht meldingen, één gemeld aan de AP. Geen structurele trendanalyse.	🟠 Beter: Vijf meldingen, geen meldingen aan de AP. Betere opvolging en interne beoordeling.	🟢 Op orde: Structurele trendanalyse en preventieve maatregelen geïmplementeerd.
Training en Bewustwording	🟠 Beperkt: Deelname aan AVG-trainingen, maar niet verplicht.	🔴 Afname: Deelname verminderd ondanks nieuwe initiatieven.	🟢 Op orde: Trainingen verplicht gesteld en structureel gemonitord.

De kleuren geven aan:

⇒ 🔴 (Rood) = Actie vereist/ onvoldoende prestaties
⇒ 🟠 (Oranje) = Verbetering zichtbaar, maar aandacht nodig
⇒ 🟢 (Groen) = Op orde/ goed presterend

4. Voortgang 2023 – 2025

1. DPIA's (Data Protection Impact Assessments)
    - 2023: Twee nieuwe DPIA's uitgevoerd en drie herzien. Structurele monitoring en opvolging van beheersmaatregelen ontbraken.
    - 2024: Vier extra DPIA's uitgevoerd, waaronder DPIA's op telefonie, leerplicht, camerabewaking en personeelsvolgsystemen. Monitoring van opvolging verbeterd, maar blijft een aandachtspunt.
    - 2025 (verwacht): Uitvoering van alle benodigde DPIA's en invoering van structurele monitoring en opvolging.
2. Register van Verwerkingen
    - 2023: Verwerkingen in het register waren deels geactualiseerd en werden als onvoldoende betrouwbaar beoordeeld.
    - 2024: Het register is verder geactualiseerd en uitgebreid met processen in i-Navigator, waardoor de vastlegging betrouwbaarder is geworden.
    - 2025 (verwacht): Het register wordt volledig beheerd in PIMS en structureel bijgewerkt.

3. Datalekkenbeheer
    - 2023: Acht meldingen van datalekken geregistreerd, waarvan één gemeld aan de Autoriteit Persoonsgegevens.
    - 2024: Vijf meldingen van datalekken, zonder meldingen aan de Autoriteit Persoonsgegevens. Verbeteringen doorgevoerd in opvolging en interne beoordeling.
    - 2025 (verwacht): Structurele trendanalyse en preventieve maatregelen worden geïmplementeerd om herhaling van incidenten te voorkomen.
4. Training en Bewustwording
    - 2023: Medewerkers namen deel aan AVG-trainingen, waaronder de cyberescaperoom en phishingtests. Training was niet verplicht.
    - 2024: Nieuwe bewustwordingsinitiatieven zoals de Cybersecuritybarometer en AI-awareness trainingen, maar deelname is afgenomen.
    - 2025 (verwacht): Trainingen worden verplicht gesteld en structureel gemonitord om naleving en bewustwording te verhogen.

De beleidsdoelstellingen voor 2025 zijn gebaseerd op een combinatie van:

⇒ De verplichtingen vanuit de AVG
⇒ Het Borgingsproduct VNG 3.0 als toetsingskader
⇒ De Nulmeting
⇒ Het Plan van Aanpak
⇒ Het Jaarverslag FG 2023
⇒ Interviews en documentatieanalyse

5. Terugblik op 2024

In 2024 heeft de gemeente Deurne vooruitgang geboekt op het gebied van gegevensbescherming, privacy en AVG-naleving. Belangrijke verbeteringen waren de actualisatie van het Register van Verwerkingen, de uitvoering van vier extra DPIA's en de ontwikkeling van nieuwe bewustwordingstrainingen. Daarnaast kreeg het melden en opvolgen van datalekken extra aandacht.

De implementatie van PIMS en i-Navigator heeft de documentatie van verwerkingsactiviteiten verbeterd, maar verdere optimalisatie en structurele monitoring blijven noodzakelijk.

De uitvoering van DPIA's is verbeterd, maar de opvolging van beheersmaatregelen is nog niet volledig geborgd. Daarnaast is het onduidelijk of voor alle processen waarin persoonsgegevens met een hoog risico worden verwerkt, een DPIA is uitgevoerd. Er wordt gewerkt aan een periodieke review van bestaande DPIA's, maar een volledig overzicht van alle processen die een hoog risico vormen en of hier een DPIA voor aanwezig is, ontbreekt. Dit benadrukt de noodzaak van een structureel

controlemechanisme om te waarborgen dat alle vereiste DPIA's tijdig worden uitgevoerd en bijgewerkt.

Het aantal geregistreerde datalekken daalde van acht in 2023 naar vijf in 2024, maar een structurele trendanalyse ontbreekt nog, waardoor onduidelijk is of de daling komt door betere preventie of onderrapportage. Daarnaast is het huidige datalekregister niet volledig AVG-proof. Voor 2025 wordt dit aangepast om te voldoen aan de AVG-eisen, waarbij een datalekregister moet bestaan uit datum en tijdstip van het lek, aard van het incident, betrokken persoonsgegevens, getroffen personen, genomen maatregelen en de meldstatus bij de Autoriteit Persoonsgegevens.

In 2024 was de deelname aan privacybewustzijnstrainingen lager dan in 2023, ondanks nieuwe initiatieven zoals de Cybersecuritybarometer en AI-awareness trainingen. Uit de monitoring van het awarenessplan en de evaluatie van het Leerpad I-bewustzijn blijkt dat de betrokkenheid bij deze trainingen achterblijft, ondanks aanvullende activiteiten zoals phishingcompetities en gerichte bewustwordingscampagnes. Dit benadrukt de noodzaak om deelname aan privacybewustzijnstrainingen in 2025 verplicht te stellen en structureel te monitoren. Hiermee wordt niet alleen de naleving verbeterd, maar ook de effectiviteit van de trainingen gewaarborgd en de algehele bewustwording binnen de organisatie versterkt.

6. Vooruitblik op 2025

Om de naleving van de AVG verder te professionaliseren, richt de gemeente zich in 2025 op de volgende verbeteringen:

1. DPIA-monitoring en volledigheid
   De gemeente zal controleren of alle risicovolle processen correct zijn beoordeeld door het DPIA-overzicht te vergelijken met het procesoverzicht. Oude verwerkingen die een DPIA vereisen, maar nog niet beoordeeld zijn, moeten alsnog worden meegenomen. Daarnaast wordt een structureel monitoringssysteem opgezet voor de opvolging van beheersmaatregelen.
2. Volledige implementatie van het Register van Verwerkingen
   In 2025 wordt het register volledig beheerd in PIMS. Dit betekent dat alle verwerkingen actueel blijven en structureel worden gecontroleerd. De integratie met i-Navigator wordt verder verbeterd, zodat processen helder en consistent worden vastgelegd.
3. Systematische analyse en preventie van datalekken
   Er wordt een structurele trendanalyse geïntroduceerd om patronen in datalekken te signaleren en preventieve maatregelen te nemen. Dit zorgt ervoor dat incidenten niet alleen worden gemeld en opgevolgd, maar ook beter worden geanalyseerd om toekomstige risico's te minimaliseren.

4. Verplichte training en monitoring
   Vanaf 2025 wordt deelname aan AVG-trainingen verplicht gesteld. Dit betekent dat medewerkers actief worden getraind in gegevensbescherming en informatiebeveiliging, met als doel een bredere bewustwording binnen de organisatie. Daarnaast wordt structureel gerapporteerd over deelname en het effect van de trainingen.

Met deze maatregelen wordt in 2025 een volwassen en duurzaam privacybeleid binnen de gemeente gerealiseerd.

7. Gegevensbescherming en verantwoording beleid

Een belangrijke leidraad voor de gemeente is het Borgingsproduct VNG 3.0, dat wordt gebruikt om de mate van AVG-naleving inzichtelijk te maken en structureel te verbeteren. Dit borgingsmodel helpt bij het toetsen van processen, het in kaart brengen van risico's en het opstellen van verbetervoorstellen. Door periodiek de status van verwerkingen, DPIA's en bewustwordingsactiviteiten te evalueren, wordt gestuurd op continue verbetering en aantoonbaarheid van compliance.

Op basis van de huidige borgingsscore per thema is beoordeeld in hoeverre de gemeente Deurne voldoet aan de AVG en waar verdere verbeteringen nodig zijn.

8. Overzicht per thema en verbeterpunten 2025

1. Processen (Score: 71%)

In 2024 zijn de verwerkingsprocessen van persoonsgegevens verder verbeterd, maar blijven er tekortkomingen in de naleving van AVG-beginselen zoals doelbinding, dataminimalisatie en opslagbeperking.

- Werkprocessen scoren slechts 54%, wat betekent dat er nog onvoldoende AVG-compliance is.
- Het Verwerkingsregister is 75% geactualiseerd, maar vereist in 2025 volledige afronding en continue actualisatie.
- DPIA's scoren hoog (90%), maar de opvolging van maatregelen is nog niet structureel geborgd.
- Het bewaar- en vernietigingsbeleid scoort slechts 59%, wat betekent dat er nog onvoldoende aandacht is voor tijdige verwijdering van persoonsgegevens.

Actiepunten voor 2025:

- Werkprocessen verder structureren en verbeteren om een hoger nalevingsniveau te bereiken.
- Het Verwerkingsregister volledig actualiseren en integreren in PIMS.
- DPIA-maatregelen actiever monitoren en opvolgen.

- Het bewaar- en vernietigingsbeleid verbeteren en duidelijke richtlijnen implementeren.

2. Organisatorische Inbedding (Score: 88%)

De organisatorische structuur voor gegevensbescherming is grotendeels op orde, maar kent nog enkele verbeterpunten:

- Het privacyteam functioneert goed (88%), maar moet beter samenwerken met proceseigenaren.
- De positie en taken van de Functionaris Gegevensbescherming (FG) zijn goed verankerd (93%), maar de opvolging van privacybeleid kan beter.
- Bewustwording onder medewerkers blijft een aandachtspunt (75%), omdat trainingen niet verplicht waren.

Actiepunten voor 2025:

- Samenwerking verbeteren tussen de FG, Privacy Officer (PO) en proceseigenaren.
- Bewustwordingstrainingen verplicht stellen om naleving van de AVG te versterken.

3. Rechten van Betrokkenen (Score: 79%)

De naleving van de rechten van betrokkenen is grotendeels op orde, maar kan worden verbeterd op de volgende punten:

- Recht op informatie scoort 80%, wat betekent dat er nog een lichte tekortkoming is in de volledigheid van de informatievoorziening.
- Toestemming en geautomatiseerde besluitvorming scoren respectievelijk 81% en 75%, wat aangeeft dat strengere controle nodig is.

Actiepunten voor 2025:

- Verbeteren van de informatievoorziening richting betrokkenen.
- Striktere controle op geautomatiseerde besluitvorming, met extra aandacht voor menselijke tussenkomst.

4. Samenwerking (Score: 71%)

De samenwerking tussen gemeentelijke afdelingen en externe partijen kent nog tekortkomingen:

- AVG-rollen en verantwoordelijkheden zijn niet altijd duidelijk (71%).
- Gegevensverstrekking binnen samenwerkingsverbanden wordt onvoldoende gemonitord (70%).

Actiepunten voor 2025:

- Duidelijke afbakening van verantwoordelijkheden binnen samenwerkingsverbanden.
- Striktere monitoring van gegevensuitwisseling en verwerkersovereenkomsten.

5. Gegevensbeveiliging (Score: 86%)

De gemeente voldoet grotendeels aan de beveiligingseisen, maar enkele punten blijven een aandachtspunt:

- Privacyincidenten en datalekken scoren goed (94%), wat wijst op een effectieve afhandeling van incidenten.
- Informatiebeveiliging scoort 75%, wat betekent dat technische en organisatorische maatregelen nog verbeterd moeten worden.
- Privacy by default scoort slechts 50%, wat aangeeft dat dit onvoldoende wordt toegepast.

Actiepunten voor 2025:

- Informatiebeveiliging verder verbeteren om risico's te minimaliseren.
- Privacy by design en privacy by default strikter toepassen.
- Doorlopende controle op privacyincidenten en risicoanalyses versterken.

Conclusie en aanbevelingen

De naleving van de AVG binnen de gemeente Deurne is in 2024 verbeterd, maar er blijven aandachtspunten bestaan. De focus voor 2025 ligt op:

1. Het verder verbeteren van werkprocessen en de volledige implementatie van het Verwerkingsregister in PIMS.
2. Versterken van de samenwerking tussen FG, PO en proceseigenaren.
3. Verbetering van de informatievoorziening en striktere controle op geautomatiseerde besluitvorming.
4. Duidelijkere rolverdeling binnen samenwerkingsverbanden en betere controle op gegevensuitwisseling.
5. Extra aandacht voor privacy by default en het structureel verbeteren van informatiebeveiliging.

Door deze maatregelen wordt de AVG-naleving binnen de gemeente verder geprofessionaliseerd en worden privacyrisico's beter beheerst.

Verantwoording werkwijze FG

Eind 2024 ben ik aangesteld als Functionaris Gegevensbescherming (FG) binnen de gemeente Deurne. Om de stand van zaken rondom privacy en gegevensbescherming vast te stellen, heb ik een nulmeting uitgevoerd. Deze is gebaseerd op de verplichtingen vanuit de AVG en Wpg en het Borgingsproduct VNG 3.0. Dit bood een gestructureerde methode om de naleving van privacywetgeving te beoordelen.

Bij de nulmeting is specifiek gekeken naar de inrichting en werking van processen, zoals vastgelegd in het privacybeleid en het Register van Verwerkingen. Dit sluit aan bij hoofdstuk 7 van het Borgingsproduct, waarin wordt aanbevolen om periodiek een gapanalyse uit te voeren om structurele tekortkomingen te identificeren en verbetermaatregelen te implementeren.

Dit verslag is gebaseerd op mijn waarnemingen, het Jaarverslag FG 2023, de acties van de Privacy Officer (PO) en het externe auditrapport over de Wet politiegegevens (Wpg).

Conclusie en acties voor 2025:

- Interne audits herintroduceren om de naleving van de AVG en Wpg structureel te toetsen.
- DPIA-opvolging beter borgen door middel van continue monitoring en rapportage.
- Privacyprocessen verder verbeteren op basis van de resultaten van de uitgevoerde gap-analyse en bevindingen uit de Wpg-audit.
- Extra controles en aanpassingen doorvoeren naar aanleiding van de uitbreiding van Wpg-verwerkingen per 1 januari 2025 (Domeinen I, II en V).

B. Deel B: WPG

9. Inleiding

Dit verslag geeft een actueel beeld van de naleving van de Wet politiegegevens (Wpg) binnen de gemeente Deurne in 2024 en beschrijft de noodzakelijke verbetermaatregelen voor 2025. De nadruk ligt op het structureel borgen van de Wpg binnen de gemeentelijke organisatie, de implementatie en actualisatie van beleid, en het vergroten van de bewustwording onder medewerkers. Specifieke aandachtspunten zijn het autorisatiebeheer, logging & toezicht, het consequent toepassen van bewaartermijnen en het correct verstrekken van politiegegevens.

Uit eerdere analyses en toetsingen blijkt dat de gemeente Deurne reeds stappen heeft gezet om de Wpg-naleving te verbeteren, maar dat er nog belangrijke tekortkomingen zijn geconstateerd:

- Ontbreken van structurele monitoring van autorisaties en logging → Implementatie van periodieke controles en risicoanalyses.
- Ontbreken van een interne Wpg-audit → Invoering van een structurele auditcyclus en verantwoordingsmechanismen.
- Onvoldoende naleving van bewaartermijnen → Realiseren van een geautomatiseerd verwijderproces met regelmatige controles.
- Inconsistenties bij de verstrekking van politiegegevens → Aanbrengen van striktere nalevingscontroles en aanvullende richtlijnen voor medewerkers.

Het doel van dit verslag is om deze bevindingen duidelijk inzichtelijk te maken en concrete verbetermaatregelen voor 2025 te formuleren. Door een gestructureerde aanpak met periodieke controles, audits en training kan de gemeente Deurne de naleving van de Wpg aanzienlijk versterken, en zorgen voor een veilige, transparante en rechtmatige verwerking van politiegegevens binnen haar organisatie.

10. Dashboard naleving Wet politiegegevens (Wpg) – Gemeente Deurne

Thema	Status/ Bevindingen	Actiepunten/ Verbetermaatregelen	Stoplicht
Borging Wpg	Er is een basisstructuur aanwezig, maar structureel toezicht en interne controle ontbreken.	Implementeren van een structureel toezichtmodel met jaarlijkse interne Wpg-controles.	🔴
Beleid	Het beleid voor politiegegevens is	Voer een jaarlijkse evaluatie van het Wpg-beleid uit en	🟠

	vastgesteld, maar wordt niet jaarlijks geëvalueerd.	actualiseer dit op basis van wijzigingen in wet- en regelgeving.	
Bewustwording	Medewerkers die met politiegegevens werken zijn bekend met de Wpg, maar structurele training en toetsing ontbreken.	Invoeren van verplichte jaarlijkse Wpg-trainingen en e-learnings. Periodieke assessments voor kennis en naleving.	🔴
Autorisatieproces	Toegangsrechten zijn te ruim verleend en periodieke controles ontbreken.	Halfjaarlijkse controles uitvoeren op autorisaties en strikt toepassen van het 'least privilege'-principe.	🔴
Bewaartermijnen	Bewaartermijnen zijn vastgesteld, maar worden niet altijd nageleefd; er is geen geautomatiseerd verwijderproces.	Implementeer een geautomatiseerd verwijderproces en wijs verantwoordelijken aan voor periodieke controles.	🟠
Verstrekken van politiegegevens	Politiegegevens worden gedeeld via gemeentelijke systemen, maar procedures worden niet altijd correct gevolgd.	Voer nalevingscontroles uit op gegevensverstrekking en zorg voor strikte documentatie en afweging van de noodzaak.	🟠
DPIA (Data Protection Impact Assessment)	Niet alle risicovolle verwerkingen zijn beoordeeld via een DPIA, en opvolging ontbreekt.	Zorg voor systematische beoordeling van alle risicovolle verwerkingen via DPIA's en actieve monitoring van maatregelen.	🔴
Register van Verwerkingen	Het register is aanwezig, maar wordt niet structureel bijgewerkt of gecontroleerd.	Jaarlijkse actualisatie van het register en aanwijzing van verantwoordelijke voor monitoring en beheer.	🟠

Logging & toezicht	Logging is aanwezig, maar structurele monitoring en analyse ontbreken.	Periodieke controles uitvoeren op logbestanden, inclusief rapportage en analyse van afwijkingen; benoem een verantwoordelijke hiervoor.	🔴
Auditverplichting	Er is geen interne Wpg-audit uitgevoerd in 2023 en 2024; toetsingsmechanismen ontbreken.	Opzetten van een jaarlijkse verplichte Wpg-audit en integreren in het gemeentelijk toezichtskader; FG verantwoordelijk voor rapportage.	🔴
Samenwerking externe partijen	Er ontbreekt structureel toezicht op de naleving van verwerkersovereenkomsten bij samenwerking met externe partijen.	Jaarlijkse evaluaties van samenwerkingen uitvoeren en naleving van afspraken controleren.	🟠

Betekenis van de kleuren:

- 🔴 **(Rood)** = Urgente actie nodig; grote tekortkomingen.
- 🟠 **(Oranje)** = Verbetering nodig; basis is aanwezig maar niet voldoende geborgd.
- 🟢 **(Groen)** = Op orde; geen directe actie vereist.

Analyse van de tabel:

- **Veel rode thema's** wijzen op urgente verbeteringen, zoals autorisatiebeheer, DPIA-opvolging en het ontbreken van interne audits.
- **Oranje thema's** zoals beleid en bewaartermijnen laten zien dat er een basis is, maar structurele borging ontbreekt.
- **Geen groen**, wat betekent dat er nog geen enkel aspect volledig voldoet aan de Wpg-eisen zonder verbetermaatregelen.

Taak van de FG

De Functionaris Gegevensbescherming (FG) heeft een essentiële rol in het toezicht op de naleving van de Wet politiegegevens (Wpg). Artikel 36 van de Wpg schrijft voor dat de FG periodieke controles uitvoert op de naleving van de wettelijke verplichtingen. Dit houdt in

dat de FG niet alleen toetst of de gemeente voldoet aan de eisen van de Wpg, maar ook adviseert over verbetermaatregelen en bewustwording binnen de organisatie stimuleert.

De belangrijkste taken van de FG met betrekking tot de Wpg kunnen als volgt worden samengevat:

1. Toezicht houden op de naleving van het gemeentelijk beleid met betrekking tot de Wpg.
2. Controleren of medewerkers voldoende bewust zijn van hun verantwoordelijkheden onder de Wpg.
3. Toetsen van het autorisatieproces voor het verwerken van politiegegevens en de juiste toekenning van toegangsrechten.
4. Bewaken van de kwaliteit en nauwkeurigheid van de vastgelegde politiegegevens.
5. Toezien op de juiste verwerking van politiegegevens conform de wettelijke eisen.
6. Controleren of de bewaartermijnen voor politiegegevens correct worden gehanteerd.
7. Beoordelen van het proces rondom het verstrekken en delen van politiegegevens.
8. Toezien op de informatiebeveiliging en de uitvoering van risicoanalyses met betrekking tot politiegegevens.
9. Controleren van het verplichte register van verwerkingen van politiegegevens.
10. Toezicht houden op de uitvoering van audits en het naleven van de auditverplichtingen onder de Wpg.

Door middel van deze taken draagt de FG bij aan de borging van de privacy en veiligheid van politiegegevens binnen de gemeente Deurne. Dit vraagt om structureel toezicht, regelmatige evaluaties en nauwe samenwerking met betrokken afdelingen. In het komende verslagjaar zal de FG hier extra aandacht aan besteden en waar nodig aanvullende maatregelen voorstellen.

In 2024 heeft er een wisseling van de FG plaatsgevonden, waardoor er gedurende een deel van het jaar geen actief toezicht is geweest op de naleving van de Wpg. Dit vraagt om een inhaalslag in 2025, waarbij extra aandacht wordt besteed aan structurele controles en rapportages.

11. Bevindingen 2024

In 2024 zijn belangrijke ontwikkelingen en knelpunten geïdentificeerd op het gebied van gegevensbescherming, Wpg-naleving en privacybewustzijn binnen de gemeente Deurne. Hieronder volgen de belangrijkste bevindingen per thema:

Borging Wpg

- Er is een basisstructuur voor de naleving van de Wpg, maar structureel toezicht en interne controle ontbreken.
- De FG voert toezicht uit op de Wpg-naleving, maar er is nog geen structureel model voor interne controles en verantwoording.

- Vanaf 1 januari 2025 zal de gemeente Deurne politiegegevens verwerken in de
- domeinen I (Openbare Ruimte), II (Milieu, welzijn en infrastructuur) en V (Werk, inkomen en zorg). Dit betekent dat de Wpg-verantwoordelijkheden zich uitbreiden naar extra beleidsdomeinen, waardoor aanvullende beheersmaatregelen, training en auditcontroles noodzakelijk worden. Dit vraagt om een versterkt toezichtmechanisme en een bredere toepassing van Wpg-naleving binnen de organisatie.

Beleid

- Het beleid voor politiegegevens is vastgesteld, maar er vindt geen jaarlijkse evaluatie plaats.
- Wijzigingen in wet- en regelgeving worden niet structureel verwerkt in het beleid.
- Bewustwording
- Medewerkers die met politiegegevens werken zijn op de hoogte van de Wpg, maar structurele training en toetsing ontbreken.
- Er is geen verplicht trainingsprogramma of periodieke toetsing op kennis en naleving.

Autorisatieproces

- Toegangsrechten zijn te ruim verleend, waardoor gebruikers toegang hebben tot gegevens die niet noodzakelijk zijn voor hun functie.
- Er vinden geen periodieke controles plaats op autorisaties, en het 'least privilege'-principe wordt niet strikt nageleefd.
- Uit de audit blijkt dat een leerplichtambtenaar politiegegevens heeft verwerkt zonder wettelijke grondslag. Dit vormt een overtreding van de Wpg en vereist directe actie. In 2025 moet worden vastgesteld of deze verwerking nog plaatsvindt en welke maatregelen nodig zijn om dit structureel te voorkomen.

Bewaartermijnen

- Bewaartermijnen zijn vastgesteld, maar worden niet consequent nageleefd.
- Er is geen geautomatiseerd verwijderproces, waardoor sommige gegevens langer bewaard blijven dan toegestaan.

Verstrekken van politiegegevens

- Politiegegevens worden gedeeld via gemeentelijke systemen, maar procedures voor verstrekking worden niet altijd correct gevolgd.
- Er is geen sluitend controlesysteem om de noodzaak en rechtmatigheid van gegevensdeling te beoordelen.

DPIA (Data Protection Impact Assessment)

- Niet alle risicovolle verwerkingen zijn beoordeeld via een DPIA, ondanks de wettelijke verplichting.
- Opvolging van DPIA-beheersmaatregelen is onvoldoende geborgd, waardoor risico's blijven bestaan.

Register van Verwerkingen

- Het register is aanwezig, maar wordt niet structureel bijgewerkt of gecontroleerd.
- Nieuwe of gewijzigde verwerkingen worden niet altijd tijdig toegevoegd, wat leidt tot onvolledigheid.
- Uit de audit blijkt dat de gemeente Deurne nog geen gestructureerde werkwijze heeft voor het voldoen aan de documentatieplicht voor politiegegevens. Dit betekent dat er geen duidelijke procedure is voor het vastleggen en bijhouden van de verwerking van politiegegevens conform de wettelijke vereisten. Dit vormt een risico voor de verantwoording en naleving van de Wpg. In 2025 moet een proces worden ingericht om de documentatieplicht systematisch te borgen en toe te passen.

Logging & toezicht

- Logging van toegang en verwerking van politiegegevens is aanwezig, maar er ontbreekt een structureel monitorings- en analysetraject.
- Er wordt geen periodieke controle uitgevoerd op logbestanden en afwijkingen worden niet systematisch gerapporteerd.

Auditverplichting

- In 2023 en 2024 is geen interne Wpg-audit uitgevoerd, waardoor toetsingsmechanismen ontbreken.
- Zonder audits is er geen onafhankelijke beoordeling van de naleving en effectiviteit van beheersmaatregelen.
- Samenwerking externe partijen
- Structureel toezicht op naleving van verwerkersovereenkomsten ontbreekt.
- Er zijn geen jaarlijkse evaluaties van samenwerking met externe partijen om te controleren of afspraken worden nageleefd.

Samenvatting

- Positieve ontwikkelingen: Er is een basis voor Wpg-naleving, een register van verwerkingen en logging van gegevensverwerking.
- Belangrijkste knelpunten: Gebrek aan structurele controlemechanismen, onvoldoende training en toetsing van medewerkers, en beperkte opvolging van DPIA's en audits.
- Noodzakelijke verbeteringen: In 2025 moet de focus liggen op het formaliseren van toezicht, het versterken van interne controles en het borgen van structurele monitoring en naleving.

12. Audit WPG

De Wet politiegegevens (Wpg) vereist dat gemeenten periodiek toetsen of de verwerking van politiegegevens voldoet aan de wettelijke eisen. Dit gebeurt onder andere via interne en externe audits. In 2024 heeft de gemeente Deurne geen interne audit uitgevoerd, waardoor een structurele beoordeling van beleid, procedures en controlemechanismen

ontbreekt. Hierdoor is onvoldoende inzicht in mogelijke risico's binnen de verwerking van politiegegevens.

Wel wordt er een externe audit uitgevoerd door Duijnborgh Audit B.V. Deze audit richt zich specifiek op het domein Leerplicht (Domein 1). Voor de scope van het Wpg-jaarverslag 2024 betekent dit dat alleen het domein Leerplicht wordt gedekt, aangezien Domein 1 vóór 1 januari 2024 ondergebracht was bij gemeente Eindhoven.

Het ontbrekende interne controlemechanisme vormt een verbeterpunt voor 2025, waarbij het essentieel is om interne controles structureel te integreren in het gemeentelijke toezichtskader.

Daarnaast beveelt de externe audit aan om in 2025 extra interne audits in te plannen voor de nieuw toegevoegde domeinen waarin politiegegevens worden verwerkt (I, II en V). Door de uitbreiding van de Wpg-verwerkingen moet de gemeente niet alleen periodieke controles uitvoeren, maar ook een structureel monitoringsmechanisme inrichten voor de volledige scope van politiegegevens.

Actiepunten en verbetermaatregelen voor 2025

Om in 2025 volledig aan de Wpg-verplichtingen te voldoen, is het noodzakelijk om een structureel auditproces en controlemechanismen op te zetten. Dit omvat:

1. Jaarlijkse interne auditcyclus

- Opstellen van een auditplan waarin alle kernaspecten van de Wpg worden geëvalueerd, zoals logging, toegangsbeheer en bewaartermijnen.

2. Structurele controlemechanismen

- Periodieke evaluatie van autorisaties volgens het 'least privilege'-principe.
- Implementeren van een geautomatiseerd proces voor het tijdig verwijderen van politiegegevens met periodieke nalevingscontroles.
- Toetsing van logging en toezichtmaatregelen, inclusief regelmatige analyse van logbestanden.

3. Betere borging auditverplichtingen

- Inbedden van de Wpg-audit in de bredere gemeentelijke controlemechanismen voor gegevensbescherming.

Conclusie en aanbevelingen

De gemeente Deurne heeft in 2024 stappen gezet om de naleving van de Wet politiegegevens (Wpg) te verbeteren, maar er blijven significante tekortkomingen

bestaan. Met name het ontbreken van structurele interne audits, gebrekkige controle op autorisaties en logging, en onvoldoende naleving van bewaartermijnen vormen belangrijke risico's. Hoewel er momenteel een externe audit specifiek gericht op het domein Leerplicht loopt via Duijnborgh Audit b.v., is deze nog niet afgerond. Het is essentieel dat in 2025 een gestructureerd audit- en controlemechanisme wordt geïmplementeerd, ondersteund door regelmatige trainingen en bewustwordingsactiviteiten, om zo een veilige, transparante en rechtmatige verwerking van politiegegevens duurzaam te borgen binnen de gemeentelijke organisatie.

C. Deel C: Ontwikkelingen

In 2024 en de komende jaren worden verschillende nieuwe wet- en regelgevingen van kracht die invloed hebben op de gegevensbescherming en informatieveiligheid binnen de Gemeente Deurne. Hieronder volgt een overzicht van de belangrijkste ontwikkelingen en de impact op de gemeentelijke processen.

13. Wet- en Regelgeving

De volgende nieuwe en aangepaste wetgevingen hebben gevolgen voor de verwerking en beveiliging van persoonsgegevens.

1.1 NIS2-richtlijn (Netwerk- en Informatiebeveiliging)

Ingangsdatum: 17 oktober 2024, nationale wetgeving uiterlijk eind 2025 van kracht via de Cyberbeveiligingswet en vernieuwde Baseline Informatiebeveiliging Overheid (BIO 2.0).

Toelichting:
Gemeenten moeten voldoen aan strengere eisen voor cyberbeveiliging. Dit betekent dat:

- Bestuurders en management moeten worden opgeleid om effectief te sturen op cyberrisico's.
- Kritieke processen moeten worden geïdentificeerd en beoordeeld via risicoanalyses.
- De meldplicht voor datalekken wordt uitgebreid naar beveiligingsincidenten in kritieke processen.
- Het toezicht en de verantwoordingsplicht worden verzwaard en verwerkt in de ENSIA-systematiek.

Aanbeveling:

- Identificeer kritieke systemen en stel een incidentbeheerplan op.
- Leid bestuurders en management op en zorg voor risicogebaseerd beveiligingsbeleid.
- Beoordeel of de gemeente Deurne onder de essentiële of belangrijke entiteiten van NIS2 valt en pas de maatregelen hierop aan.

Gemeentelijke acties:

- De gemeente Deurne werkt samen met de Informatiebeveiligingsdienst (IBD) en andere gemeenten om cyberweerbaarheid te versterken.

- De CISO van Deurne coördineert de implementatie van NIS2, de Cyberbeveiligingswet en BIO 2.0 via een opdracht op de concernplanning.

1.2 AI Act (Europese Wetgeving Kunstmatige Intelligentie)

Verwachte goedkeuring: 2024, gefaseerde invoering met volledige impact per 2 augustus 2027.

Toelichting:
De AI Act stelt strikte regels voor het gebruik van kunstmatige intelligentie, vooral bij risicovolle toepassingen zoals geautomatiseerde besluitvorming in jeugdzorg of fraudedetectie. Gemeenten moeten voldoen aan transparantie-eisen en extra waarborgen instellen voor hoog-risicosystemen.

Aanbeveling:

- Inventariseer alle AI-toepassingen binnen de gemeente.
- Voer DPIA's (Data Protection Impact Assessments) uit voor risicovolle AI-systemen.
- Zorg voor een formele bestuurlijke vaststelling van AI-beleidsrichtlijnen (bijv. door het CMT).
- Stel een intern toezichtmechanisme in voor AI-systemen en informeer burgers transparant over hoe AI wordt gebruikt.

Gemeentelijke acties:

- De gemeente Deurne heeft AI-toepassingen geïnventariseerd en geregistreerd in het landelijke algoritmeregister.
- Er zijn richtlijnen opgesteld voor ethisch AI-gebruik, maar deze moeten nog formeel worden vastgesteld door het CMT.
- Transparantie wordt verbeterd via privacyverklaringen en DPIA's voor hoog-risicosystemen.
- De gemeente heeft verwerkersovereenkomsten met AI-leveranciers aangescherpt en werkt aan een structurele verantwoordingscyclus.
- Bestaande IT-leveranciers die AI-functionaliteit integreren, vallen ook onder de AI Act en moeten worden beoordeeld op naleving.
- AI-trainingen worden structureel geborgd in het opleidingsprogramma van de gemeente.

1.3 Wet Gegevensverwerking door Samenwerkingsverbanden (WGS)

Ingangsdatum: 1 maart 2025

Toelichting:
De WGS stelt strengere eisen aan de uitwisseling van persoonsgegevens binnen samenwerkingsverbanden zoals jeugdzorg, veiligheid en sociale diensten.

Aanbeveling:

- Controleer of de gegevensuitwisseling binnen samenwerkingsverbanden voldoet aan de WGS-eisen.
- Implementeer extra waarborgen voor de bescherming van persoonsgegevens.

Gemeentelijke acties:

- Proceseigenaren binnen de gemeente zijn geïnformeerd over de WGS en hun eindverantwoordelijkheid.
- Naleving wordt halfjaarlijks gemonitord, inclusief aandachtspunten van de Autoriteit Persoonsgegevens.
- De gemeente volgt de ontwikkelingen binnen Eindhoven en het RIEC over de rol van de Coördinerend Functionaris Gegevensbescherming (CFG).

1.4 Wet gegevensverwerking persoonsgerichte aanpak radicalisering en terroristische activiteiten

Ingangsdatum: 1 januari 2025

Toelichting:
Deze wet biedt een juridisch kader voor de persoonsgerichte aanpak van radicalisering en terrorismebestrijding.

Aanbeveling:

- Stem af met betrokken partners en zorg voor privacyvriendelijke gegevensdeling.

Gemeentelijke acties:

- De gemeente neemt deel aan het Zorg- en Veiligheidshuis om radicalisering vroegtijdig te signaleren.
- Er wordt een proces ingericht om gegevens te delen binnen de privacykaders van de wet.

1.5 Wet Digitale Overheid (Wdo)

Gefaseerde invoering: vanaf 1 juli 2023, met volledige acceptatieplicht in 2025.

Toelichting:
De wet verplicht gemeenten om veilige en toegankelijke digitale dienstverlening te bieden, inclusief DigiD en eHerkenning.

Gemeentelijke acties:

- De gemeente heeft de uitgifte van eHerkenning uitbesteed aan een derde partij.
- Een DigiD-audit heeft aangetoond dat de beveiliging voldoet aan de wettelijke eisen.

14. Dreigingsbeeld IBD (Informatiebeveiligingsdienst)

De IBD publiceert jaarlijks een dreigingsbeeld voor gemeenten. De belangrijkste trends zijn:

- Toename van ransomware-aanvallen.
- Kritieke kwetsbaarheden in software, zoals Log4j.
- Toenemende afhankelijkheid van externe leveranciers en ketenrisico's.
- Datadiefstal en reputatieschade door datalekken.

Gemeentelijke acties:

- Cybersecurity versterken via GAP-analyse en BIO 2.0-implementatie.
- Logging en monitoring verbeteren.
- Bewustwordingscampagnes en extra cybersecuritytrainingen uitvoeren.
- Samenwerking met de IBD en gemeenten intensiveren.
- Betere contractuele afspraken met leveranciers over cybersecurity.

15. Conclusie en aanbevelingen

De gemeente Deurne heeft vooruitgang geboekt, maar er zijn nog aandachtspunten:

1. AI-richtlijnen moeten formeel worden vastgesteld op bestuurlijk niveau (CMT).
2. Leveranciers met AI-functionaliteit moeten periodiek worden beoordeeld op naleving van de AI Act.
3. AI-kennis en vaardigheden moeten structureel worden geborgd binnen de organisatie.
4. NIS2 en BIO 2.0 vereisen verdere implementatie, inclusief risicogebaseerde beveiligingsmaatregelen.
5. Meer focus op cybersecurity in de keten, inclusief monitoring en incidentrespons.

16. Ontwikkelingen in AI en Algoritmes

De AI Act, aangenomen in maart 2024, stelt strenge eisen aan het gebruik van AI, vooral bij toepassingen die een aanzienlijke impact hebben op burgers, zoals fraudeopsporing en sociale zekerheidsregelingen. De wet verplicht organisaties, waaronder gemeenten, tot transparantie, ethisch gebruik, verantwoording en verantwoordelijkheid voor het gebruik van AI door leveranciers.

De AI Act wordt gefaseerd ingevoerd. Sinds 2 februari 2025 zijn bepaalde AI-systemen verboden en moeten organisaties hun medewerkers AI-geletterd maken. Vanaf 2 augustus 2026 gelden extra vereisten voor specifieke AI-systemen en per 2 augustus 2027 treedt de wet volledig in werking.

AI-systemen die persoonsgegevens verwerken, moeten transparant en juridisch onderbouwd zijn. Gemeenten dienen duidelijk te communiceren over de werking van hun AI-systemen, vooral bij geautomatiseerde besluitvorming. AI-toepassingen worden ingedeeld op risiconiveau. Hoog-risicosystemen, zoals die in de jeugdzorg of fraudecontrole, vereisen strengere privacy- en beveiligingsmaatregelen om discriminatie en onterechte uitsluiting te voorkomen.

Gemeenten moeten toezicht houden op AI-systemen om te garanderen dat deze voldoen aan wettelijke en ethische normen. In plaats van audits als enige controlemechanisme, wordt aanbevolen om gebruik te maken van een bredere vorm van toezicht en verantwoording. Dit kan bestaan uit periodieke leveranciersbeoordelingen, rapportages over AI-gebruik en toetsing van nalevingseisen. Dit geldt niet alleen voor AI-leveranciers, maar ook voor leveranciers die AI-componenten in hun software integreren. Leveranciers moeten voldoen aan de privacy- en beveiligingseisen van de AI Act, wat vraagt om duidelijke afspraken en periodieke evaluaties.

Gemeentelijke acties met betrekking tot de AI Act

De gemeente Deurne heeft stappen gezet om te voldoen aan de AI Act, maar er zijn nog verbeterpunten.

Bevindingen

- AI-toepassingen die binnen de gemeente worden gebruikt, zijn geregistreerd in het landelijke algoritmeregister.
- Er zijn richtlijnen opgesteld voor het ethisch gebruik van AI binnen de gemeentelijke organisatie. Deze richtlijnen moeten echter nog formeel worden vastgesteld door het CMT.
- Er wordt gewerkt aan het verbeteren van transparantie door middel van privacyverklaringen en het vastleggen van rechtsgrondslagen voor AI-systemen.
- DPIA's (Data Protection Impact Assessments) voor hoog-risicosystemen worden nog niet structureel uitgevoerd.

- Er ontbreekt een structureel toezichtmechanisme voor AI-leveranciers, waaronder een periodieke beoordeling van verwerkersovereenkomsten en naleving van de AI Act. Dit geldt zowel voor leveranciers die AI ontwikkelen als leveranciers die AI-functionaliteit integreren in hun producten.

Aanbevelingen en aandachtspunten voor 2025

Om de naleving van de AI Act verder te versterken en risico's rondom AI-gebruik te minimaliseren, worden de volgende acties aanbevolen:

1. Uitvoeren van DPIA's voor alle risicovolle AI-systemen en het structureel borgen van de opvolging ervan.
2. Versterken van transparantie richting burgers over AI-gebruik, vooral bij geautomatiseerde besluitvorming. Dit kan door duidelijke communicatie en het toegankelijk maken van informatie over AI-systemen.
3. Inrichten van een toezicht- en verantwoordingsmechanisme voor AI-systemen. Dit betekent dat controle niet uitsluitend via audits plaatsvindt, maar ook door middel van periodieke verantwoording, leveranciersrapportages en evaluaties op verzoek.
4. Verbeteren van toezicht op AI-leveranciers, inclusief de beoordeling van verwerkersovereenkomsten en periodieke evaluaties. Dit kan worden geïntegreerd in de jaarlijkse leveranciersgesprekken. Ook bestaande leveranciers die AI-functionaliteit in hun software hebben geïntegreerd, moeten hierin worden meegenomen.
5. Borgen van kennis en vaardigheden binnen de organisatie door AI-trainingen verder uit te breiden en structureel te verankeren in opleidingsprogramma's. Dit omvat niet alleen eenmalige workshops, maar ook continue kennisontwikkeling voor medewerkers die AI-systemen gebruiken of hier toezicht op houden.
6. Formaliseren van AI-beleidsregels op bestuurlijk niveau, zodat de richtlijnen breed binnen de organisatie worden gedragen en geborgd.
7. Beoordelen en aanpassen van contracten met leveranciers, zodat AI-specifieke eisen worden opgenomen in nieuwe aanbestedingen en bestaande overeenkomsten, inclusief afspraken over transparantie en verantwoording.

Conclusie

De gemeente Deurne heeft stappen gezet om te voldoen aan de AI Act, maar er zijn nog structurele verbeteringen nodig. Met name op het gebied van DPIA's, toezicht op leveranciers en het borgen van AI-kennis en vaardigheden binnen de organisatie moeten verdere maatregelen worden genomen. In 2025 moet extra aandacht worden besteed aan het inrichten van een effectief toezichtmechanisme en aan het vergroten van de transparantie richting burgers over AI-gebruik.

Bijlagen (3)

Bijlage 1 – Overzicht uitgevoerde DPIA's 2024
Bijlage 2 – Overzicht Datalekken 2024
Bijlage 3 – Overzicht inzage verzoeken
Bijlage 3 – Nulmeting n.a.v. verplichtingen AVG

Bijlage 1 - DPIA Overzicht 2024 – Gemeente Deurne

Afdeling	Onderwerp	Datum Advies FG	Datum DPIA Gereed	Planning
Bedrijfsvoering	Teams, Onedrive & Sharepoint	-	01-02-2022	Afgerond
Samenleving	Wvggz	Aug 2023	31-08-2023	Afgerond
Samenleving	WGS/ Vroegsignalering / Grip op Schuld	Aug 2023	31-08-2023	Afgerond
GR Peelgemeenten	Toezicht en rechtmatigheid	-	Okt 2023	Afgerond
Samenleving	Bibob-onderzoek	12-03-2024	12-03-2024	Afgerond
Bedrijfsvoering	Telefonie mbv Teams	04-04-2024	04-04-2024	Afgerond
Samenleving	Zorg in Deurne Jeugd	-	31-12-2023	In bewerking (2022?)
Samenleving	Leerplicht (focus op WPG-verwerkingen)	25-04-2024	25-04-2024	Afgerond
Ruimte	Camerabewaking gemeentehuis en tijdelijke huisvesting	29-04-2024	29-04-2024	Afgerond
Bedrijfsvoering	DPIA Datamask (anonimiseringstool)	29-05-2024	04-06-2024	Afgerond
Bedrijfsvoering	DPIA Personeelsvolgsystemen (4ME/I-burgerszaken/Powerbrowser/Djuma/Zorgned/MDM/Toegangsysteem/TIM)	23-10-2024	Instemming OR	Gereed voor instemming OR
Bedrijfsvoering	Enable U	05-11-2024	07-11-2024	In bewerking (30/12 Eric B?)
Ruimte	Landelijk Honderbijt- en Overlast Dossier	-	-	DPIA n.v.t.
Bedrijfsvoering	4ME Service Management applicatie	-	-	DPIA n.v.t.

Afdeling	Onderwerp	Datum Advies FG	Datum DPIA Gereed	Planning
Ruimte	PowerBrowser (Omgevingswet / VTH)	-	-	DPIA n.v.t.
Bedrijfsvoering	Djuma Zaaksysteem	-	-	DPIA n.v.t.
Bedrijfsvoering	Kassasysteem JCC-Betalen	-	-	DPIA n.v.t.
Samenleving	Recherche op Internet (digitale opsporing)	-	-	DPIA n.v.t.
Bedrijfsvoering	Personeel & Organisatie	n.v.t.	DPIA n.v.t.	
Ruimte	Peelland Interventie Team (PIT)	-	Ontvangen en analyse uitgevoerd iom Hans	Actie ligt bij Esther
Bedrijfsvoering	Identiteitsvaststelling Publiekszaken & Dienstverlening	-	-	
Samenleving	WMO door GR Peelgemeenten (DPIA i.v.m. mandatering)	-	-	
GR Peelgemeenten	Beschermd Wonen/Beschermd Thuis	2022	-	-

Bijlage 2 - Overzicht Datalekken 2024

Onderwerp	Datum aangemaakt
Beveiligingsincident + Datalek: BOA is telefoon verloren	02-02-2024
Datalek: BIBOB stukken naar omgevingsdienst gedeeld	09-04-2024
Datalek: mail naar ex-partner	26-08-2024
Datalek: mail naar andere ouder	12-06-2024
GR Peelgemeenten: Datalek Wmo - brief aan verkeerde persoon	04-07-2024
Datalek bij besluit inzake Woo-verzoek	22-01-2024
Datalek: bijlage met persoonsgegevens in Trefpunt bericht	20-06-2024
Datalek: document in verkeerde personeelsdossier	23-12-2024
Datalek: documenten Djuma onbevoegd in te zien via DataMask	30-08-2024
Datalek: e-mail adressen netwerkpartners gedeeld	21-02-2024
Datalek: e-mail bouwbesluit naar verkeerde persoon	14-02-2024
Datalek: overeenkomst gedeeld met verkeerde partij	30-05-2024
Datalek: link naar bestand KBO leden in Trefpuntbericht	20-06-2024
Datalek: persoonsgegevens op tekening	30-01-2024
Beveiligingsincident of datalek	11-12-2024
Datalek Notaris van Kaam veroorzaakt phishing mails	24-09-2024
Beveiligingsincident phish mail "gemeentesecretaris.nl" - Start Datalek	01-10-2024
Beveiligingsincident + Datalek JCC Software - Start Datalek	05-11-2024
Datalek: NAW en BSN busongeval via WhatApp	27-08-2024
Datalek (mogelijk): berichtgeving over datalek bij Fortinet	16-09-2024
melding van Kessel onveilig mailaccount	29-04-2024

Bijlage 3 - Overzicht verzoeken rechten van betrokkene

Overzicht verzoeken rechten van betrokkene				
2024				
Bron: AVG-Privacy/8.Rechten van betrokkene/inzage verzoeken/2024/dossiers				
Datum verzoek	*Verzoeker*	*datum afhandeling*	*Binnen 1 maand*	*Opmerking*
17-jul	Calis	09-aug	ja	5/9 schrijven verzonden i.v.m. afhandeling en geen reactie op ontvangen
01-sep	Baram	05-nov	nee	inwoner van Amersfoort en geen reactie op beslissing ontvangen
16-okt	Vos	05-nov	ja	geen reactie op schrijven ontvangen

Bijlage Nulmeting n.a.v. verplichtingen AVG

Onderdeel	Vragen	Toelichting	Status
1. Beleid en procedures	- Is er een formeel en actueel gegevensbeschermingsbeleid?	Dit beleid benadrukt het belang van transparantie, risicomanagement en governance binnen de gemeente. Het governance-model is gebaseerd op het "Three Lines Model", waarbij proceseigenaren verantwoordelijk zijn voor de bescherming van persoonsgegevens in hun processen.	Ja, beschikbaar op de website van de gemeente. Het privacybeleid is in december 2023 geactualiseerd en is op 27 februari 2024 officieel worden vastgesteld. CISO: De procedures zijn toegankelijk voor medewerkers via de gemeentelijke leeromgeving BROS-academie en Trefpunt (Intranet), zodat zij eenvoudig toegang hebben tot de benodigde richtlijnen
	- Zijn er procedures voor datalekken, DPIA's, en verzoeken van betrokkenen?	Procedures helpen bij een snelle en conforme afhandeling van privacy-incidenten.	Ja, procedures zijn aanwezig en worden regelmatig bijgewerkt.
	- Zijn de procedures bekend en toegankelijk voor medewerkers?	Medewerkers moeten eenvoudig toegang hebben tot deze richtlijnen.	Ja, de procedures zijn toegankelijk voor medewerkers via de gemeentelijke leeromgeving BROS-academie en, na gesprekken met de FG, ook zichtbaar voor teamleiders.

Onderdeel	Vragen	Toelichting	Status
2. Gegevensverwerking en verwerkingsregister	- Is er een volledig en actueel verwerkingsregister?	Een compleet verwerkingsregister is essentieel voor AVG-naleving.	Nee, het verwerkingsregister heeft nog aanvullend onderhoud nodig om volledig en actueel te zijn. Tijdens de recente studiedag over I-Navigator, BIO, en AVG werd besproken dat I-Navigator als "single point of truth" moet dienen voor processen en verwerkingen. Hoewel de Privacy Officer (PO) het register beheert, is het bij de beheerders nog onvoldoende bekend.
	- Welke soorten persoonsgegevens worden verwerkt, en wat is het doel ervan?	Alle verwerkingen moeten gerechtvaardigd en doelgericht zijn.	De gemeente verwerkt persoonsgegevens voor wettelijke taken in het sociaal en openbare domein.
	- Is er een wettelijke basis voor alle verwerkingen?	Iedere verwerking moet gebaseerd zijn op een geldige wettelijke grondslag.	Ja, verwerkingen zijn gebaseerd op geldige wettelijke grondslagen zoals vastgelegd in het privacybeleid.
	- Hoe wordt de verwerking van gevoelige gegevens gemanaged?	Speciale maatregelen moeten genomen worden voor gevoelige gegevens zoals medische gegevens.	Hoewel DPIA's beschikbaar zijn, ontbreekt de controle op de naleving van de voorgestelde maatregelen. De Privacy Officer (PO) werkt aan een inhaalslag door processen in kaart te brengen en verwerkersovereenkomsten te herzien.

Onderdeel	Vragen	Toelichting	Status
3. Toestemming en rechten van betrokkenen	- Wordt er op de juiste wijze toestemming gevraagd voor gegevensverwerkingen?	Toestemming moet expliciet en duidelijk gevraagd worden wanneer nodig.	Ja, verzoeken worden ingeboekt in het zaaksysteem door de Privacy Officer (PO).
	- Hoe worden betrokkenen geïnformeerd over hun rechten (privacyverklaring)?	Privacyverklaring moet toegankelijk en duidelijk zijn voor alle betrokkenen.	Privacyverklaring is beschikbaar op de gemeentelijke website.
	- Hoe worden verzoeken van betrokkenen (inzage, correctie, verwijdering) afgehandeld?	Er moeten efficiënte procedures zijn voor het afhandelen van verzoeken van betrokkenen.	Ja, deze procedures zijn aanwezig en verzoeken worden afgehandeld via het zaaksysteem door de PO.
4. Datalekken en incidentmanagement	- Is er een formeel protocol voor het melden en afhandelen van datalekken?	Er moet een duidelijk en gedocumenteerd proces zijn voor het melden van datalekken.	Datalekken worden geregistreerd in Xurrent, maar er is behoefte aan een groter signalerend vermogen bij medewerkers.
	- Worden medewerkers getraind om datalekken te herkennen en te melden?	Medewerkers moeten bewust zijn van hoe ze datalekken kunnen identificeren en melden.	Ja, via e-learnings en bewustwordingsacti viteiten zoals phishingtests en cyberescaperooms.
	- Worden datalekken binnen 72 uur gemeld aan de Autoriteit Persoonsgegevens?	Het is wettelijk vereist dat datalekken binnen 72 uur worden gemeld.	Ja, datalekken worden binnen 72 uur gemeld.
5. Data Protection Impact Assessments (DPIA's)	- Worden DPIA’s uitgevoerd voor projecten of verwerkingen met een hoog risico?	DPIA's zijn vereist voor verwerkingen met een hoog risico voor de rechten van betrokkenen.	DPIA's worden uitgevoerd voor risicovolle verwerkingen, maar er blijft de vraag of daadwerkelijk alle noodzakelijke DPIA's zijn uitgevoerd.
	- Bestaat er een procedure voor het uitvoeren en beoordelen van DPIA’s?	DPIA-processen moeten gedocumenteerd en consequent worden toegepast.	Ja, er is een procedure voor het uitvoeren en beoordelen van DPIA's.

Onderdeel	Vragen	Toelichting	Status
	- Hoe worden de resultaten van DPIA's opgevolgd?	Acties op basis van DPIA-resultaten moeten worden gemonitord en nagevolgd.	Volgens het Q2-rapport van de PO is de monitoring momenteel onvoldoende. Verdere controle en opvolging van de DPIA-maatregelen zijn nodig om consistentie en effectiviteit te waarborgen.

6. Toegang en autorisatiebeheer	- Wordt er gewerkt met rolgebaseerde toegang tot persoonsgegevens?	Alleen noodzakelijke medewerkers moeten toegang hebben tot persoonsgegevens (need-to-know-principe).	De toegang tot systemen binnen de gemeente Deurne is gedeeltelijk ingericht volgens het need-to-know-principe. Voor de meeste applicaties is een autorisatiematrix beschikbaar, die is geïntegreerd in de helpdeskprocessen en centraal wordt beheerd in Teams. Functioneel beheerders zijn verantwoordelijk voor het beheren van autorisaties en rapporteren hierover aan de systeemeigenaar. Ondanks deze maatregelen zijn er verbeterpunten. Toegang wordt momenteel vaak breed verleend aan hele teams of gebaseerd op de functie van de medewerker, in plaats van op individuele behoeften. Dit vraagt om een strengere toepassing van het autorisatiebeleid en betere controlemechanismen. Nieuwe medewerkers worden geregistreerd in Youforce, en er is een format beschikbaar voor periodieke controles die worden

Onderdeel	Vragen	Toelichting	Status
			meegenomen in de wpg-audits.
	- Hoe wordt toegang geregeld, en worden deze rechten periodiek geëvalueerd?	Toegangsrechten moeten regelmatig worden geëvalueerd en aangepast.	Het is onzeker of deze evaluaties volledig en consistent worden uitgevoerd.
	- Zijn er procedures voor het intrekken van toegang bij functiewijzigingen of uitdiensttreding?	Toegang moet onmiddellijk worden ingetrokken wanneer niet langer vereist.	Ja, toegang wordt direct ingetrokken bij functiewijzigingen of uitdiensttreding.

7. Beveiliging van persoonsgegevens	- Worden persoonsgegevens versleuteld, zowel in rust als tijdens overdracht?	Gegevensversleutelin g is essentieel voor zowel opslag als overdracht.	Er zijn vraagtekens bij de effectiviteit van de gebruikte tools, zoals Secumailer. De Privacy Officer (PO) adviseert om extra controles uit te voeren om zeker te stellen dat alle gevoelige gegevens correct worden verwerkt. CISO: Alle uitgaande e-mails worden via Secumailer beveiligd verzonden. Secumailer dwingt af dat dit altijd compliant gebeurt met de geldende normen (NTW 7516 Verklaring). Wanneer gezondheidsinforma tie wordt verstuurd, wordt dit gedaan via extra beveiligde e-mail. De netwerklaag is beveiligd via Secumailer. Wanneer "vertrouwelijk" wordt toegevoegd in een e-mail, controleert Secumailer of er een geldige verklaring aanwezig is. Als dat niet het geval is, wordt om een 06-nummer gevraagd. Status van controles Er heeft eerder een controle plaatsgevonden op de correcte registratie van 06-

Onderdeel	Vragen	Toelichting	Status
			nummers binnen het Sociaal Domein. De CISO is momenteel niet op de hoogte van de actuele status hiervan. Het lijkt er niet op dat versleutelde opslag van gegevens noodzakelijk is binnen de systemen. Reden: We werken uitsluitend met SaaS-applicaties die volledig in de cloud draaien. Zorgdossiers, zoals WMO en Jeugd, worden beheerd door de GR Peelgemeenten. De medewerkers werken in Zorgnet, en de GR Peelgemeenten vallen volledig onder hun verantwoordelijkheid.

	- Worden back-ups veilig beheerd en opgeslagen?	Back-ups moeten veilig opgeslagen en beheerd worden om gegevensverlies te voorkomen.	Back-ups worden veilig beheerd en opgeslagen. Voor de gemeente Deurne worden back-ups voornamelijk gebruikt voor netwerkschijven en de gegevensmakelaar van PinkRoccade, die nog lokaal draait. Er zijn twee Dell-back-upunits in gebruik: één op locatie en één op een externe locatie voor geografische redundantie. Eisen bij SaaS-applicaties: De CISO hanteert de richtlijnen van GiBIT 29.4 (2023) voor back-ups: Back-ups op minimaal twee geografische locaties. Bescherming tegen ransomware met versleuteling en monitoring. Veilig e-mailverkeer via protocollen zoals DKIM, DMARC, SPF, SNS Sec en DANE. Het informatiebeveiligingsbeleid dateert van 23 maart 2021 en is inmiddels drie jaar oud. Het beleid staat gepland voor een update in 2024 om te voldoen aan nieuwe wetgeving, zoals de NIS2-richtlijn.

Onderdeel	Vragen	Toelichting	Status
			In 2024 wordt een vernieuwd beleid opgesteld, waarbij de focus ligt op: Het implementeren van de nieuwste BIO-normen (BIO 2.0). Versterkte maatregelen op het gebied van cyberbeveiliging.
	- Is er een informatiebeveiligingsbeleid dat regelmatig wordt geëvalueerd?	Het informatiebeveiligingsbeleid benadrukt governance, risicomanagement en naleving van wetgeving zoals de AVG. Het wordt periodiek geëvalueerd.	Informatiebeveiligingsbeleid dateert van 23 maart 2021 en is inmiddels drie jaar oud. Er is een geplande herziening in 2024 om het beleid te actualiseren en af te stemmen op nieuwe wetgeving, zoals ook de NIS2-richtlijn. Het vernieuwde beleid gericht zijn op de versterking van cyberbeveiliging en het voldoen aan de normen van BIO 2.0, die vanaf 2024 van kracht worden.

Onderdeel	Vragen	Toelichting	Status
8. Verwerkersovereen-komsten en derde partijen	- Zijn er verwerkersovereenkomsten met alle derde partijen die persoonsgegevens verwerken?	Verwerkersovereenkomsten zijn verplicht om de verantwoordelijkheden vast te leggen.	In december 2023 heeft de Privacy Officer (PO) een interne controle uitgevoerd op de verwerkersovereenkomsten. Uit deze controle bleek dat 33% van de overeenkomsten voldeed aan de wettelijke eisen. Actie: De PO heeft samen met de contracteigenaren (eindverantwoordelijken voor de contracten) en de contractbeheerders (uitvoerend verantwoordelijk) een overzicht opgesteld van de betreffende overeenkomsten. De opdracht is belegd bij de contractbeheerders om de tekortkomingen in de verwerkersovereenkomsten te herstellen en te zorgen voor naleving van de AVG.

Onderdeel	Vragen	Toelichting	Status
	- Worden verwerkers periodiek gecontroleerd op naleving van de afspraken?	Het is belangrijk om verwerkers regelmatig te controleren op naleving van afspraken.	Nee, verwerkers worden momenteel niet regelmatig gecontroleerd op naleving van afspraken, omdat er geen leveranciersmanagement of leveranciersbeoordeling is ingeregeld. De Privacy Officer (PO) heeft een kick-off gepland voor een workshop om leveranciersmanagement op te zetten en te implementeren.
	- Hoe worden verwerkers gemonitord (bijvoorbeeld via audits)?	Er moeten mechanismen zijn voor de monitoring en beoordeling van verwerkers.	Nee, er zijn momenteel onvoldoende mechanismen voor de monitoring en beoordeling van verwerkers. Uit de interne controle door de Privacy Officer (PO) in december 2023 bleek dat 70% van de verwerkersovereenkomsten niet op orde was.
9. Bewaartermijnen en geautomatiseerde verwijdering	- Zijn er bewaartermijnen vastgesteld voor de verschillende soorten persoonsgegevens?	Er moeten duidelijke bewaartermijnen zijn voor alle soorten gegevens.	Ja, bewaartermijnen zijn vastgesteld volgens wettelijke richtlijnen.
	- Worden gegevens verwijderd na het verstrijken van de bewaartermijn?	Gegevens moeten tijdig worden verwijderd om te voldoen aan AVG-vereisten.	Nee, gegevens worden niet altijd tijdig verwijderd na het verstrijken van de bewaartermijn. Uit de interne controle uit Q3 2024 blijkt dat de naleving hiervan niet voldoet aan de AVG-vereisten.

Onderdeel	Vragen	Toelichting	Status
	- Is dit proces geautomatiseerd?	Geautomatiseerde processen helpen menselijke fouten te voorkomen.	Het regionale rapport van de RHCe bevestigt een bestaande achterstand in het verwijderen en archiveren van persoonsgegevens.
10. Training en bewustwording	- Worden medewerkers regelmatig getraind over gegevensbescherming en de AVG?	De gemeente Deurne werkt actief aan bewustwording over privacy en informatiebeveiliging onder medewerkers, met trainingen en testjes om bewustwording te vergroten.	Ja, er worden regelmatig trainingen en bewustwordingsacti viteiten georganiseerd, zoals phishingtests en een Cyber Escaperoom.
	- Is er een bewustwordingsprogra mma om medewerkers te informeren over hun verantwoordelijkheden?	Bewustwordingsprogr amma's moeten medewerkers ondersteunen bij hun taken.	Ja, er is een bewustwordingsprog ramma via de BROS-academie en dit wordt up-to-date gehouden in samenwerking met Brooklyn Partners.
	- Worden medewerkers intern gecontroleerd op naleving van gegevensbeschermingsv ereisten?	Interne audits zorgen voor naleving van beleid en procedures.	Nee, interne audits zijn aanwezig, maar er ontbreekt rapportage en opvolging specifiek gericht op de naleving van trainingen, wat de consistentie in naleving van beleid en procedures beperkt.
11. Informatievoorziening aan burgers	- Zijn er duidelijke en toegankelijke privacyverklaringen beschikbaar voor burgers?	Privacyverklaringen moeten gemakkelijk beschikbaar en begrijpelijk zijn.	Ja, deze is beschikbaar op de website van de gemeente.
	- Worden burgers geïnformeerd over hoe ze hun rechten kunnen uitoefenen (inzage, verwijdering)?	Burgers moeten goed geïnformeerd zijn over hoe zij hun rechten kunnen uitoefenen.	Ja, dit wordt beschreven in de privacyverklaring.

Onderdeel	Vragen	Toelichting	Status
12. Privacy by Design en Privacy by Default	- Wordt privacy by design toegepast bij nieuwe processen en systemen?	Privacybescherming moet ingebouwd zijn in de systemen.	Inkoopformulier als hulpmiddel: Er is een document genaamd Inkoopformulier beschikbaar dat als hulpmiddel dient bij het opnemen van privacy als vast onderwerp in het inkoopproces. Ontbreken van een inkoopadviseur: Er is momenteel geen inkoopadviseur beschikbaar om het inkoopproces te begeleiden of privacyrisico's structureel te beoordelen. Het signaleren van privacyrisico's wordt nu opgepakt door de CISO tijdens het CAB-overleg. Programma van eisen: Privacy by design wordt als eis opgenomen in het programma van eisen en gesteld aan de leverancier/opdrachtnemer door de eis onderdeel te maken van de overeenkomst wordt gesloten.
	- Wordt privacy by default toegepast, met de strengste privacy-instellingen standaard?	Standaard instellingen moeten privacy-vriendelijk zijn.	Ja, privacy by default wordt toegepast, en de Privacy Officer (PO) wordt proactief benaderd om te adviseren bij privacy-instellingen.

Onderdeel	Vragen	Toelichting	Status
13. Verwerkingsverantwoordelijke en Verwerker	- Is het onderscheid tussen verwerkingsverantwoordelijke en verwerker duidelijk?	Duidelijke rollen helpen bij het naleven van de verantwoordelijkheden.	Ja, dit onderscheid is duidelijk vastgelegd in de verwerkersovereenkomsten.
	- Zijn de verplichtingen van verwerkers goed vastgelegd en bekend?	Verwerkers moeten hun verplichtingen begrijpen en naleven.	Nee, de controle op naleving van verplichtingen door verwerkers is momenteel onvoldoende, zoals blijkt uit de interne controle in het Excel-bestand van PO.
14. Transparantie en Documentatieplicht	- Worden alle verwerkingen, DPIA's en incidenten gedocumenteerd?	Documentatie is verplicht om verantwoording te kunnen afleggen.	Ja, alle verwerkingen en DPIA's worden gedocumenteerd, en incidenten worden geregistreerd in het datalekregister. De Privacy Officer (PO) speelt een belangrijke rol in het proces; wanneer incidenten via 4me worden gemeld, zorgt de PO ervoor dat deze correct worden afgehandeld.
	- Worden betrokkenen goed geïnformeerd over gegevensverwerkingen?	Transparantie is belangrijk voor de AVG-compliance.	Ja, dit wordt gewaarborgd via de privacyverklaring en door actieve communicatie met betrokkenen.
15. Internationale Gegevensoverdracht	- Worden persoonsgegevens overgedragen buiten de EU?	Internationale overdracht moet voldoen aan strikte eisen onder de AVG.	Deze overdrachten zijn beperkt en vinden voornamelijk plaats binnen de EER.

Onderdeel	Vragen	Toelichting	Status
	- Zijn er waarborgen zoals standaardcontractbepalingen of bindende bedrijfsvoorschriften (BCR's)?	Deze waarborgen zijn nodig voor veilige internationale gegevensoverdracht.	Bij de actualisatie van het verwerkingsregister is gebleken dat er enkele sub verwerkers buiten de EER actief zijn, hoewel het hoofdbedrijf in Nederland gevestigd is en deze verwerking onder contractuele waarborgen valt. CISO geeft aan zich niet bewust te zijn dat er overdracht plaatsvindt buiten de EER.