FG Jaarverslag (AVG en WPG) Gemeente Weert 2024

GEMEENTE WEERT

1. Doel

Het doel van dit jaarverslag is om inzicht te geven in de wijze waarop de Gemeente Weert 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 NIS2-richtlijn en 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, en wordt de positie van de FG binnen de organisatie versterkt.

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.

GEMEENTE WEERT

Inhoudsopgave

1. DOEL 1
2. INLEIDING 5
3. MANAGEMENTSAMENVATTING 6
A. DEEL A: AVG 7
4. VOORTGANG 2023 - 2025 7
5. TERUGBLIK OP 2024 9
6. VOORUITBLIK OP 2025 10
7. GEGEVENSBESCHERMING EN VERANTWOORDING 11
B. DEEL B: WPG 16
8. DASHBOARD NALEVING WET POLITIEGEGEVENS (WPG) – GEMEENTE WEERT 16
9. TAAK VAN DE FG 17
10. BEVINDINGEN 2024 18
11. AUDIT WPG 19
12. BEVINDINGEN EN AANBEVELINGEN 19
C. DEEL C: ONTWIKKELINGEN 21
13. WET- EN REGELGEVING 21
14. DREIGINGSBEELD IBD 23
15. ONTWIKKELINGEN IN AI EN ALGORITMES 24

GEMEENTE WEERT

Jaarverslag Gegevensbescherming

Gemeente Weert

Datum: 28 februari 2025

Functionaris Gegevensbescherming: Natascha Westen a.i.

2. Inleiding

In 2024 heeft de Gemeente Weert aanzienlijke vooruitgangen geboekt in de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (WPG). De Functionaris Gegevensbescherming (FG) heeft toezicht gehouden op de uitvoering van noodzakelijke maatregelen, zoals de uitvoering van Data Protection Impact Assessments (DPIA's) en het bijwerken van het Register van Verwerkingen. Ook is er aandacht besteed aan de voorbereiding op nieuwe wetgeving, zoals de Wet Gegevensverwerking Samenwerkingsverbanden (WGS).

Hoewel er vooruitgang is geboekt, blijven er belangrijke verbeterpunten, zoals het verder versterken van de privacybewustwording binnen de organisatie, het afronden van DPIA's voor risicovolle verwerkingen en het volledig actualiseren van het Register van Verwerkingen.

In 2025 ligt de focus op:

- Het afronden van de uitvoering van DPIA's voor risicovolle verwerkingen.
- Het volledig actualiseren en publiceren van het Register van Verwerkingen.
- Het verbeteren van het beheer van datalekken en het implementeren van trendanalyses.
- Het versterken van de privacybewustwording door verplichte trainingen en e-learningmodules.

De Gemeente Weert heeft in 2024 ook goed toezicht gehouden op de naleving van de Wet Politiegegevens (WPG). De beveiligingsmaatregelen voor politiegegevens zijn gedefinieerd, maar moeten verder geüpdatet worden. Ook zijn de toegangscontrolemaatregelen voor politiegegevens verbeterd, maar er is ruimte voor verdere verfijning.

3. Managementsamenvatting

Het jaarverslag biedt een gedetailleerd overzicht van de voortgang die de Gemeente Weert in 2024 heeft geboekt met betrekking tot de naleving van de Algemene Verordening Gegevensbescherming (AVG). Het verslag is opgesteld door de Functionaris Gegevensbescherming (FG) en bevat belangrijke bevindingen, aanbevelingen en plannen voor 2025. Dit verslag behandelt de taken van de FG, de uitgevoerde werkzaamheden, de behaalde resultaten en de verbeterpunten op basis van de AVG.

In 2024 heeft de Gemeente Weert belangrijke stappen gezet om te voldoen aan de vereisten van de AVG. Er is gewerkt aan het uitvoeren van Data Protection Impact Assessments (DPIA's), het bijwerken van het Register van Verwerkingen en het verbeteren van het incidentbeheer bij datalekken. Er is echter nog werk aan de winkel, vooral met betrekking tot:

- Het inhalen van de achterstand in DPIA's, met een realistisch doel van 75% uitvoering in 2025 en volledige afronding in 2026.
- Het versterken van privacybewustwording binnen de organisatie, waarbij privacy-ambassadeurs een actievere rol zullen krijgen.
- Het volledig actualiseren van het Register van Verwerkingen, met een centraal AVG-coördinator om de updates te bewaken.
- Het verbeteren van het incidentbeheer bij datalekken, met nadruk op de implementatie van trendanalyses om risicovolle patronen te identificeren.

In 2025 zullen de belangrijkste focuspunten zijn:

- Het afronden van de uitvoering van DPIA's voor risicovolle verwerkingen, waarbij clustering van verwerkingen wordt onderzocht om het proces efficiënter te maken.
- Het volledig actualiseren en publiceren van het Register van Verwerkingen, met duidelijke samenwerking tussen afdelingen.
- Het versterken van het incidentbeheer bij datalekken, met nadruk op trendanalyses en impactmonitoring.
- Het verder verbeteren van de privacybewustwording en trainingen voor medewerkers, inclusief verplichte afronding en een monitoringssysteem voor naleving.

Het verslag is onderverdeeld in drie secties:

1. Deel A: AVG – Bevat gedetailleerde informatie over de naleving van de AVG, met focus op de uitvoering van DPIA's, het bijwerken van het Register van Verwerkingen, en incidentbeheer.
2. Deel B: WPG – Behandelt de naleving van de Wet Politiegegevens (WPG), en de maatregelen die zijn genomen om deze wet te waarborgen (dit deel komt later aan bod).

3. Deel C: Ontwikkelingen – Bespreekt belangrijke externe ontwikkelingen zoals de impact de Wet Gegevensverwerking Samenwerkingsverbanden (WSG) en de AI Act.

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	28% uitgevoerd	36% uitgevoerd	75% uitgevoerd
Register van Verwerkingen	48% geactualiseerd	60% geactualiseerd	Volledig geactualiseerd
Datalekkenbeheer	Baseline bereikt	Verbeterd	Trendanalyse geïmplementeerd
Training en Bewustwording	50% deelname	47% deelname	75% deelname

4. Voortgang 2023 - 2025

DPIA's (Data Protection Impact Assessments)

- 2023: Slechts 28% van de DPIA's zijn uitgevoerd. Dit betekent dat een aanzienlijk deel van de risicovolle verwerkingen nog niet volledig beoordeeld is. Er is een duidelijke achterstand.
- 2024: Gedurende het jaar zijn acht DPIA's opgepakt, waarvan acht opnieuw zijn opgestart en twee volledig zijn afgerond. Hiermee is het percentage uitgevoerde DPIA's gestegen naar 36%. Ondanks deze vooruitgang blijft een aanzienlijk deel van de DPIA's nog openstaan, waardoor een versnelde inhaalslag in 2025 noodzakelijk is om volledige naleving van de AVG te waarborgen.
- 2025 (verwacht): Het streven is om 75% van de DPIA's uit te voeren. Dit vereist een structurele verankering van DPIA's in de gemeentelijke processen.
- Gezien de achterstand van 96 openstaande DPIA's zal het streven naar 100% uitvoering in 2025 een aanzienlijke inspanning vereisen. Daarom wordt onderzocht welke DPIA's gebundeld kunnen worden op basis van vergelijkbare risico's en verwerkingsdoelen, zodat een realistischer doel van 75% uitvoering in 2025 wordt nagestreefd, met een volledige afronding in 2026.

Register van Verwerkingen

- 2023: Het Register van Verwerkingen was 48% geactualiseerd. Veel verwerkingen ontbraken of waren niet volledig gedocumenteerd.
- 2024: Er is een toename naar 60% (schatting) in 2024. Er zijn verbeteringen in de volledigheid en juistheid van de gegevens, maar er blijven lacunes.
- 2025 (verwacht): Het doel is een volledig geactualiseerd register, inclusief beveiligingsmaatregelen en bewaartermijnen.

Datalekkenbeheer

- 2023: In 2023 werd een basis gelegd voor het datalekkenbeheer. De gemeente had een proces voor het melden en afhandelen van datalekken, maar er werd nog geen trendanalyse uitgevoerd.
- 2024: Het incidentbeheer en datalekkenbeheer zijn verder verbeterd, met snellere opvolging en evaluatie van meldingen.
- 2025 (verwacht): Er wordt een trend-analyse geïmplementeerd om risicovolle trends te monitoren en maatregelen te nemen om terugkerende problemen te voorkomen.

Training en bewustwording

- 2023: De deelname aan privacytrainingen was 50%. Dit betekende dat een groot deel van de medewerkers de verplichte training nog niet had gevolgd.
- 2024: De werkelijke trainingsdeelname is 47%, wat lager is dan verwacht. Dit suggereert dat er onvoldoende opvolging is om medewerkers te stimuleren de training tijdig te voltooien.
- 2025 (verwacht): Het doel is 75% deelname, wat betekent dat er extra aandacht nodig is voor bewustwording en actieve deelname.

Samenvattende conclusie

De voortgang in gegevensbescherming binnen de gemeente Weert is zichtbaar, maar er blijven verbeterpunten:

- DPIA’s moeten versneld worden uitgevoerd om de achterstand in te halen. In 2024 heeft er bij alle proceseigenaren contact plaatsgevonden om de hoog-risico beoordelingen (DPIA's) uit te voeren. Deze exercitie heeft aanzienlijke tijd en inspanning gekost, maar heeft er ook toe geleid dat er nog steeds 96 DPIA's openstaan die achterstallig zijn. Ondanks dat er in 2024 acht DPIA’s zijn opgepakt, blijft het aantal achterstallige beoordelingen hoog, en is het duidelijk dat de huidige voortgang onvoldoende is om in lijn te blijven met de vereisten van de AVG. Gezien de initiële achterstand van 96 openstaande DPIA's, zal er verdere

versnelling nodig zijn om de achterstand in te halen en te voldoen aan de AVG-eisen.
- Het Register van Verwerkingen moet volledig actueel zijn in 2025.
- Datalekkenbeheer moet proactief worden verbeterd, met een focus op trendanalyses.
- Privacytrainingen moeten een structurele verplichting zijn om te garanderen dat alle medewerkers voldoende kennis hebben.

5. Terugblik op 2024

In 2024 heeft de Gemeente Weert aanzienlijke vooruitgangen geboekt met de naleving van de AVG. De belangrijkste ontwikkelingspunten zijn:

1. DPIA's (Data Protection Impact Assessments):
    - De gemeente heeft DPIA's uitgevoerd voor verschillende risicovolle verwerkingen, zoals het jeugdzorgsysteem en het wagenparkregistratiesysteem.
    - Er zijn echter achterstanden in de uitvoering van DPIA's voor bepaalde verwerkingen, met name in de jeugdzorg en WMO-processen.
    - In 2024 is een uitgebreid onderzoek uitgevoerd naar hoog-risicoverwerkingen binnen de gemeente. Uit dit onderzoek is gebleken dat er 96 DPIA's nog uitgevoerd moeten worden. Deze achterstand vormt een uitdaging voor de naleving van de AVG en vereist een gestructureerde aanpak in 2025.
    - Om dit efficiënter aan te pakken, wordt in 2025 onderzocht of bepaalde DPIA's samengevoegd kunnen worden. Een groot deel van de openstaande DPIA's betreft bijvoorbeeld WMO-verwerkingen, waarbij meerdere processen mogelijk een vergelijkbaar doel en risicoanalyse hebben. Door clustering van vergelijkbare verwerkingen kan de DPIA-afhandeling efficiënter verlopen, zonder dat dit ten koste gaat van de inhoudelijke kwaliteit en risicobeoordeling.
    - De verwachting is dat deze aanpak zal leiden tot een aanzienlijke vermindering van het aantal benodigde DPIA's, waardoor de werkdruk afneemt en de gemeente in kortere tijd compliant kan worden met de AVG. De FG dient in 2025 actief te adviseren en toezicht houden te op dit proces om te waarborgen dat risico's correct worden geïdentificeerd en gedocumenteerd.
2. Register van Verwerkingen:
    - Het Register van verwerkingen is gedeeltelijk geactualiseerd, maar mist nog cruciale informatie over de Wpg, beveiligingsmaatregelen en internationale overdracht. Het is belangrijk dat dit register volledig wordt geactualiseerd en opnieuw op de gemeentelijke website wordt gepubliceerd voor transparantie.

    - Er zijn verbeteringen nodig in de samenwerking met verschillende afdelingen om het register continu bij te werken.
3. Datalekkenbeheer:
    - Er is voortgang geboekt in het incidentbeheer bij datalekken, maar er is onvoldoende trendanalyse uitgevoerd op gedocumenteerde datalekken.
    - In 2025 moet er een systematische aanpak voor het analyseren van datalekken komen, om trends te identificeren en preventieve maatregelen te nemen.
4. Training en Bewustwording:
    - Trainingen en e-learningmodules werden opgestart, maar de deelnamegraad bleef lager dan verwacht (47% van de medewerkers voltooide de trainingen). Dit moet in 2025 worden opgevoerd om de privacybewustwording binnen de organisatie te versterken.
    - Er is onvoldoende monitoring van nieuwe medewerkers die in dienst komen.

6. Vooruitblik op 2025

De prioriteiten voor 2025 zijn:

- Het afronden van de DPIA's voor risicovolle verwerkingen en het opstellen van een plan voor het uitvoeren van ontbrekende DPIA's.
    - Gezien de achterstand van 96 openstaande DPIA's zal het streven naar 100% uitvoering in 2025 een aanzienlijke inspanning vereisen. Daarom wordt onderzocht welke DPIA's gebundeld kunnen worden op basis van vergelijkbare risico's en verwerkingsdoelen, zodat een realistischer doel van 75% uitvoering in 2025 wordt nagestreefd, met een volledige afronding in 2026.
- Het volledig actualiseren en publiceren van het Register van Verwerkingen.
    - Hoewel het streven is om het register volledig geactualiseerd te hebben in 2025, blijft samenwerking tussen afdelingen een uitdaging. Daarom wordt een centraal AVG-coördinator aangewezen die verantwoordelijk is voor het bewaken van updates en het oplossen van knelpunten tussen afdelingen.
- Het verbeteren van het beheer van datalekken en het implementeren van trendanalyses.
    - Hoewel er vooruitgang is geboekt in het incidentbeheer, is de implementatie van een trendanalyse uitgesteld. Dit belemmert een preventieve aanpak van datalekken en moet in 2025 een prioriteit worden.
    - De gemeente zal in 2025 een systematische trendanalyse van datalekken implementeren, waarbij patronen in datalekken worden geanalyseerd en risicogebieden worden geïdentificeerd. Dit zal jaarlijks worden geëvalueerd en gedeeld met de FG en het management.

- Het versterken van de privacybewustwording door verplichte trainingen voor medewerkers, en het opzetten van een structureel monitoringssysteem voor training en compliance.
    - De daling van de deelname aan privacytrainingen in 2024 (47%) laat zien dat de huidige aanpak onvoldoende effectief is. Om de stijging naar 75% in 2025 te realiseren, wordt een verplichte afronding van trainingen ingevoerd.
- Het ontwikkelen van beleidsdocumenten voor gegevensbescherming die zorgen voor volledige compliance en transparantie richting betrokkenen.

7. Gegevensbescherming en verantwoording beleid

In 2023 heeft de gemeente Weert haar privacybeleid verder geactualiseerd om te voldoen aan de AVG. Er zijn maatregelen genomen om persoonsgegevens rechtmatig, eerlijk en transparant te verwerken. De algemene nalevingsscore voor beleid is 75%, waarbij verantwoordelijkheden goed zijn belegd (83%), maar verdere versterking nodig is.

Verbeterpunten voor 2025:

- Beleid vaststellen en formaliseren (huidige score: 50%) door duidelijke richtlijnen en implementatieplannen.
- Privacybeleid verder doorontwikkelen (75%) en beter integreren in gemeentelijke processen.
- Verantwoordelijkheden verduidelijken binnen de organisatie en afdelingen meer betrekken bij naleving.

In 2025 ligt de focus op het verder versterken van beleidsmaatregelen, met speciale aandacht voor de rechten van betrokkenen en de praktische toepassing van het privacybeleid binnen de organisatie.

1. Processen

In 2024 zijn de verwerkingsprocessen van persoonsgegevens verbeterd in lijn met de AVG-beginselen, zoals doelbinding, dataminimalisatie en opslagbeperking. De algemene nalevingsscore voor processen is echter 45%, wat aangeeft dat verdere optimalisatie noodzakelijk is.

Verbeterpunten voor 2025:

- Achterstanden in DPIA's wegwerken (huidige score: 28%) door een versnelde uitvoering en betere monitoring.
- Het Verwerkingsregister volledig actualiseren (48%) om inzicht te behouden in verwerkingen en risico's.
- Pre-DPIA's structureler uitvoeren (33%) en beter integreren in de besluitvorming.

- Bewaar- en vernietigingsbeleid verder versterken (80%) door handhaving en naleving te verbeteren.

In 2025 ligt de focus op het effectiever inrichten van processen en het inhalen van achterstanden, met name bij DPIA's en het Verwerkingsregister, om de naleving van de AVG te versterken.

2. Organisatorische inbedding

In 2024 is gewerkt aan de verdere integratie van gegevensbescherming binnen de gemeente Weert. De nalevingsscore voor organisatorische inbedding is 86%, met een goed functionerend privacyteam (100%) en een duidelijke positionering van de Functionaris Gegevensbescherming (FG) (95%).

Hoewel de organisatorische inbedding sterk is (86%), blijkt uit de lage bewustwordingsscore (65%) dat er een kloof is tussen beleid en praktijk. Privacy-ambassadeurs zullen een actievere rol krijgen in het trainen van afdelingen en het vertalen van beleid naar de dagelijkse praktijk

Verbeterpunten voor 2025:

- Bewustwording vergroten (huidige score: 65%) door gerichte trainingen en een actievere rol van privacy-ambassadeurs.
- OR (Ondernemingsraad) beter informeren (75%) over privacyontwikkelingen en relevante beleidswijzigingen.
- Privacy-ambassadeurs actiever inzetten om compliance per afdeling te ondersteunen en de privacycultuur verder te versterken.

In 2025 zal de focus liggen op training en cultuurverandering, waarbij privacy-ambassadeurs een centrale rol spelen in de bewustwording en naleving van de AVG binnen de organisatie.

3. Rechten van Betrokkenen

In 2024 is gewerkt aan het verbeteren van de procedures voor het verwerken van verzoeken van betrokkenen, zoals inzage-, correctie- en verwijderingsverzoeken. De nalevingsscore voor de uitvoering van deze processen is 77%, met een sterke score van 97% op de afhandeling van verzoeken, maar verbeterpunten op andere onderdelen.

In 2025 wordt geautomatiseerde besluitvorming voor het eerst systematisch geëvalueerd. Er wordt een proces ingericht om betrokkenen inzicht te geven in geautomatiseerde beslissingen, met een mogelijkheid tot bezwaar en menselijke tussenkomst indien nodig

Verbeterpunten voor 2025:

- Recht op informatie versterken (huidige score: 40%) door duidelijkere en toegankelijke communicatie richting betrokkenen.
- Toestemmingsprocedures verbeteren (63%) en consistent integreren in verwerkingsprocessen.
- Geautomatiseerde besluitvorming beoordelen (0%), zodat betrokkenen hierop invloed kunnen uitoefenen.
- Verbetering van technische ondersteuning (81%) om verzoeken efficiënter en tijdig te verwerken.

Door deze maatregelen wordt de naleving van de AVG versterkt en kunnen betrokkenen beter gebruik maken van hun privacyrechten.

4. Samenwerking

De gemeente Weert werkt samen met diverse externe partijen, waaronder overheden en private organisaties. In 2024 zijn stappen gezet om verwerkersovereenkomsten en privacyafspraken op te stellen, maar de naleving hiervan vereist verdere verbetering. De nalevingsscore op samenwerking is 54%, waarbij met name gegevensverstrekking (36%) extra aandacht nodig heeft.

Verbeterpunten voor 2025:

- Striktere controle op naleving van verwerkersovereenkomsten en andere privacyafspraken.
- Duidelijkere afspraken over gegevensuitwisseling, met focus op risicovolle verwerkingen.
- Verbetering van AVG-rollen en verantwoordelijkheden (huidige score: 71%) om samenwerking effectiever te maken.

Door deze maatregelen wordt de naleving binnen samenwerkingen versterkt en privacyrisico's beter beheerst.

5. Gegevensbeveiliging

In 2024 heeft de gemeente vooruitgang geboekt in de beveiliging van persoonsgegevens, met een nalevingsscore van 78% voor gegevensbescherming en 80% voor informatiebeveiliging. Er zijn verbeteringen doorgevoerd in privacy by design (88%) en datalekbeheer (79%), maar verdere optimalisatie is nodig.

Verbeterpunten voor 2025:

- Risicobeheer versterken (huidige score: 50%) door systematische analyses en maatregelen.
- Standaard beveiligingsinstellingen verbeteren (75%) voor een veiliger gegevensverwerkingsproces.
- Snellere opvolging van privacy-incidenten, met focus op trendanalyse en preventie.

Met deze maatregelen streeft de gemeente naar een hogere naleving en betere bescherming van persoonsgegevens in 2025.

Conclusie en aanbevelingen

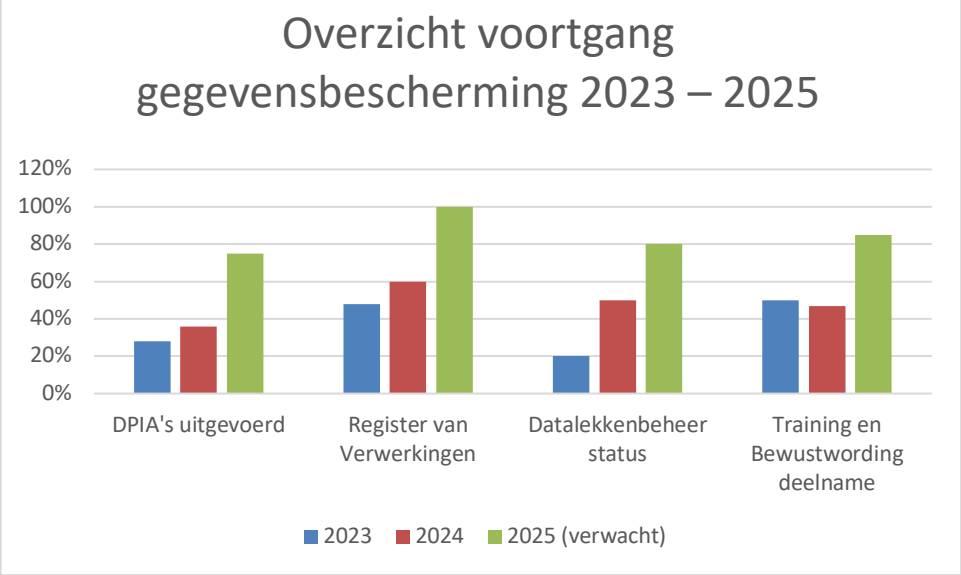
Dit verslag biedt een overzicht van de aanzienlijke vooruitgangen die in 2024 zijn geboekt met betrekking tot de naleving van de AVG, maar het benadrukt ook de gebieden waar nog werk te doen is. De Gemeente Weert heeft een solide basis gelegd, maar moet in 2025 de uitvoering van DPIA's, het actualiseren van het Register van Verwerkingen, en de verbetering van het datalekkenbeheer verder versterken. Bij het opstellen van dit verslag is gebruikgemaakt van het Borgingsproduct 3.0, een instrument dat helpt bij het monitoren en borgen van de naleving van de AVG binnen gemeenten. Gezien de ontwikkelingen en de bevindingen uit dit verslag, lijkt het wenselijk dat dit product wordt herijkt, zodat het beter aansluit bij de actuele uitdagingen.

De belangrijkste aanbevelingen voor 2025 zijn:

- Het volledig afronden van de uitvoering van DPIA’s.
- Het versterken van de privacybewustwording door verplichte trainingen.
- Het verbeteren van trendanalyses bij datalekken.

Het jaar 2025 zal zich richten op het afronden van deze achterstanden en het verder optimaliseren van de naleving van de AVG.

Overzicht voortgang gegevensbescherming 2023 – 2025



Verantwoording werkwijze FG

In 2024 ben ik halverwege het jaar aangesteld als Functionaris Gegevensbescherming (FG). Aangezien er in zowel 2023 als 2024 geen interne audits zijn uitgevoerd, heb ik het Borgingsproduct 3.0 als uitgangspunt genomen om de naleving van de AVG en Wpg te beoordelen. Dit bood een structuur om de belangrijkste processen en risico's in kaart te brengen.

Daarnaast heb ik een nulmeting uitgevoerd om te bepalen of de gemeente Weert voldoet aan de basisvereisten van de AVG en of de processen goed zijn ingericht (opzet en bestaan). Dit sluit aan bij hoofdstuk 7 van het Borgingsproduct, waarin wordt aanbevolen om periodiek een gapanalyse uit te voeren.

Uit deze analyse blijkt dat sommige richtlijnen in het Borgingsproduct moeten worden bijgesteld. Een concreet voorbeeld is de oorspronkelijke richtlijn dat 33% van de pre- DPIA's was uitgevoerd. In werkelijkheid zijn in 2024 96 pre-DPIA's uitgevoerd, wat aangeeft dat deze norm niet langer accuraat is. Dit onderstreept het belang van een herijking van het Borgingsproduct 3.0, zodat het beter aansluit bij de actuele stand van zaken.

Met het oog op de continuïteit van gegevensbescherming binnen de gemeente is het raadzaam dat de nieuwe FG per 1 maart 2025 deze herziening meeneemt en de opvolging van de bevindingen uit dit verslag waarborgt.

B. Deel B: WPG

Inleiding

Als Functionaris Gegevensbescherming (FG) binnen de gemeente Weert houdt de FG toezicht op de naleving van de Wet politiegegevens (Wpg). De Wpg stelt strikte eisen aan het verwerken en beschermen van politiegegevens, en het is de verantwoordelijkheid van de gemeente om ervoor te zorgen dat deze regels correct worden toegepast in alle relevante werkprocessen.

Het college van burgemeester en wethouders is verplicht erop toe te zien dat de FG tijdig en adequaat wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. Om dit te borgen, rapporteert de FG jaarlijks over de stand van zaken en de ondernomen acties in een jaarverslag. Dit verslag biedt inzicht in de naleving van de Wpg binnen de gemeente Weert in het afgelopen jaar, inclusief de uitgevoerde controles, geconstateerde risico's en verbetermaatregelen.

In dit verslag worden onder andere de volgende onderwerpen behandeld:

- De implementatie en naleving van de Wpg in de gemeentelijke werkprocessen, met name binnen leerplicht en handhaving.
- De stand van zaken rondom samenwerkingsverbanden, zoals Citycontrol en Nederweert.
- Het gebruik van systemen zoals JVS en Bastion365 ter ondersteuning van een veilige gegevensverwerking.
- De uitkomsten van (interne) audits en controles.
- Beveiligingsmaatregelen en verdere professionalisering van de werkwijze conform de Wpg.

Hoewel in het afgelopen jaar geen FG-controles of interne audits zijn uitgevoerd, is het belangrijk om in het komende jaar structureel toezicht te houden en aantoonbare maatregelen te treffen om de naleving van de Wpg te waarborgen. Dit verslag dient als evaluatie van de huidige situatie en als leidraad voor verdere verbeteringen.

8. Dashboard naleving Wet politiegegevens (Wpg) – Gemeente Weert

Thema	Status/ bevindingen	Actiepunten/ verbetermaatregelen
Borging Wpg	De werkinstructie is herzien en geactualiseerd.	Borgen van regelmatige evaluatie en bijstelling.
Beleid	Er is beleid opgesteld voor de uitvoering van de Wpg.	

Thema	Status/ bevindingen	Actiepunten/ verbetermaatregelen
Bewustwording	Medewerkers zijn geïnformeerd over Wpg, maar geen structurele bewustwordingscampagne.	Trainingen of e-learnings ontwikkelen en verplicht stellen.
Autorisatieproces	Toegangsrechten zijn beperkt tot bevoegde BOA's.	Jaarlijkse controle op juiste autorisaties uitvoeren.
Bewaartermijnen	Worden toegepast conform de Wpg.	Controle uitvoeren op naleving en automatische verwijdering.
Verstrekken van persoonsgegevens	Gegevensdeling met OM, Halt en RvdK via Bastion365.	Evalueren of gegevensuitwisseling volledig conform wetgeving plaatsvindt.
DPIA (Data Protection Impact Assessment)	Nog niet duidelijk of er een DPIA is uitgevoerd voor alle relevante processen.	DPIA uitvoeren voor processen waar dit verplicht is.
Register van Verwerkingen	Er is een register van verwerkingen, maar actuele status onbekend.	Jaarlijkse update en controle van het register inplannen. Daarnaast moet het verwerkingsregister worden aangevuld met de relevante informatie volgens de Wet bescherming persoonsgegevens (Wpg), zodat het voldoet aan de wettelijke eisen
Auditverplichting	Geen interne audits uitgevoerd, maar gepland voor dit jaar.	Structurele auditcyclus opzetten en naleving documenteren.
Logging & toezicht	Logging is aanwezig en periodieke controles zijn ingevoerd.	Uitbreiding van monitoring en rapportage over logging.

9. 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.

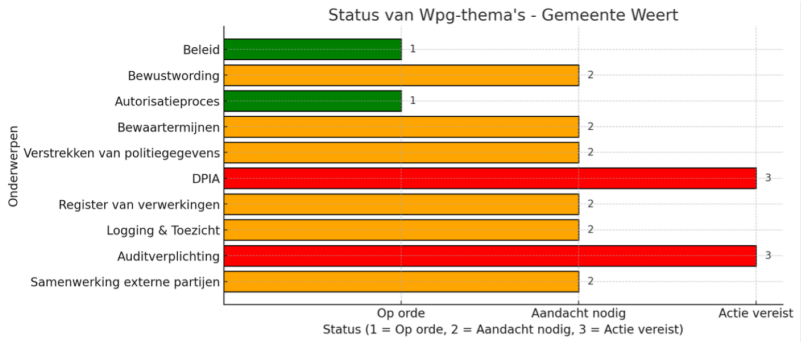
De belangrijkste taken van de FG met betrekking tot de Wpg kunnen als volgt worden samengevat:

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 Weert. 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.

10. Bevindingen 2024

6. Status van Wpg-thema's - Gemeente Weert



De grafiek geeft de status van de verschillende Wpg-thema's visueel weer. De kleuren geven aan:

- **Groen (1)** = Op orde
- **Oranje (2)** = Aandacht nodig
- **Rood (3)** = Actie vereist

11. Audit WPG

Op basis van de beschikbare informatie blijkt dat in het afgelopen jaar geen interne of audit is uitgevoerd**.** Voor het komende jaar is het wel de bedoeling om op alle domeinen FG-controles uit te voeren, zodat aantoonbaar wordt dat de opzet en het bestaan van de Wpg-maatregelen geborgd zijn.

In 2023 heeft de verplichte externe audit plaatsgevonden, die eens per vier jaar moet worden uitgevoerd om de naleving van de Wet politiegegevens (Wpg) te toetsen. Tijdens deze audit is beoordeeld in hoeverre de gemeente Weert voldoet aan de wettelijke verplichtingen en of de getroffen maatregelen effectief zijn in het beschermen van politiegegevens. De volgende externe audit staat gepland voor 2025.

12. Bevindingen en aanbevelingen

Onderwerp	Bevindingen	Aanbeveling
Beleid	Het beleid met betrekking tot de uitvoering van de Wpg is opgesteld en herzien.	Voortdurend evalueren en aanpassen aan nieuwe wetgeving en jurisprudentie.
Bewustwording	Medewerkers zijn bekend met de Wpg, maar structurele bewustwording en training ontbreken.	Regelmatig trainingen of e-learnings organiseren.
Autorisatieproces	Toegangsrechten zijn correct ingericht en beperkt tot bevoegde BOA's.	Jaarlijkse controle uitvoeren op autorisaties en logging.
Bewaartermijnen	Gegevens worden conform de Wpg-bewaartermijnen bewaard, maar automatische verwijdering is niet altijd geborgd.	Systematische controle en automatische verwijdering waar mogelijk implementeren.
Verstrekken van politiegegevens	Gegevensuitwisseling vindt plaats via Bastion365, maar niet altijd consequent toegepast.	Evaluatie uitvoeren over de naleving en medewerkers informeren over juiste toepassing.
DPIA	Nog niet overal een Data Protection Impact Assessment (DPIA) uitgevoerd, met name voor nieuwe systemen.	DPIA uitvoeren voor alle relevante werkprocessen en nieuwe toepassingen.

Onderwerp	Bevindingen	Aanbeveling
Register van verwerkingen	Het register van verwerkingen is aanwezig, maar wordt niet structureel geactualiseerd.	Jaarlijkse update en controle inplannen, inclusief documentatie van wijzigingen.
Logging & toezicht	Logging van toegang en verwerkingen is aanwezig, maar geen structurele analyse en rapportage.	Logging structureel monitoren en jaarlijks analyseren.
Auditverplichting	In het afgelopen jaar geen interne audits uitgevoerd.	Structurele auditcyclus opzetten en naleving documenteren.
Samenwerking externe partijen	Samenwerking met Citycontrol en Nederweert is onderwerp van discussie.	Evaluatie over samenwerking en technische scheiding uitvoeren.

Conclusie

De nieuwe Functionaris Gegevensbescherming (FG) binnen de gemeente Weert moet bijzondere aandacht besteden aan de naleving van de Wet Politiegegevens (Wpg). De Wpg stelt strikte eisen aan de verwerking en bescherming van politiegegevens, en hoewel enkele belangrijke maatregelen zijn getroffen, zijn er verschillende gebieden die verbetering behoeven.

In 2024 werd geen interne audit uitgevoerd, ondanks de noodzaak voor structureel toezicht op de naleving van de Wpg. Dit betekent dat de FG in het komende jaar dringend een structurele auditcyclus moet opzetten en ervoor moet zorgen dat de naleving van de Wpg daadwerkelijk wordt gedocumenteerd. Het ontbreken van interne audits en onvoldoende controles kan leiden tot gemiste risico's en compliance problemen.

De aanbeveling is dat de nieuwe FG periodieke controles uitvoert en actief toezicht houdt op alle relevante processen, zoals het autorisatieproces, de bewaartermijnen van politiegegevens, de uitvoering van DPIA's (Data Protection Impact Assessments) en de actualisatie van het register van verwerkingen. Ook de samenwerking met externe partijen, zoals Citycontrol en Nederweert, moet verder geëvalueerd worden om zeker te stellen dat de gegevensuitwisseling conform de Wpg-wetgeving plaatsvindt.

Kortom, de nieuwe FG moet prioriteit geven aan het opzetten van een systematische auditcyclus en de uitvoering van FG-controles om te zorgen voor een solide naleving van de Wpg binnen de gemeentelijke werkprocessen en samenwerkingsverbanden.

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 Weert. Hieronder volgt een overzicht van de belangrijkste ontwikkelingen en de impact die deze hebben op de gemeentelijke processen.

13. Wet- en Regelgeving

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

1. NIS2-richtlijn (Netwerk- en Informatiebeveiliging) – Ingangsdatum: 17 oktober 2024, nationale wetgeving die deze richtlijn implementeert, moet uiterlijk eind 2025 van kracht zijn.

Toelichting: Gemeenten moeten voldoen aan strengere eisen voor cyberbeveiliging en incidentbeheer. Dit betekent dat kritieke infrastructuren geïdentificeerd moeten worden en dat er een formeel incidentbeheerplan moet worden opgesteld.

Aanbeveling: Het is belangrijk om kritieke systemen te identificeren en een incidentbeheerplan te ontwikkelen.

Gemeente acties: Dit proces is meegenomen in de IT-audit, waarbij de focus lag op de risicobeoordeling van deze systemen. Daarnaast heeft de CISO een quick scan uitgevoerd om de huidige staat van de beveiliging en het incidentbeheer te evalueren.

2. E-Privacy Verordening – Nog in ontwikkeling, met verwachte goedkeuring in 2025.

Toelichting: De Europese Commissie heeft besloten het voorstel voor de E-Privacy Verordening in te trekken vanwege een gebrek aan consensus. Dit betekent dat de huidige E-Privacy Richtlijn voorlopig van kracht blijft.

Aanbeveling: Blijf voldoen aan de huidige E-Privacy Richtlijn en monitor de ontwikkelingen op dit gebied voor toekomstige wijzigingen.

3. AI Act (Europese Wetgeving Kunstmatige Intelligentie) – Verwachte goedkeuring in 2024, gefaseerde invoering met volledige impact naar verwachting in 2026.

Toelichting: De AI Act stelt regels voor het gebruik van kunstmatige intelligentie, met nadruk op risicovolle toepassingen zoals besluitvorming in jeugdzorg of fraudedetectie.

Aanbeveling: Inventariseer AI-toepassingen en voer DPIA's (Data Protection Impact Assessments) uit voor risicovolle systemen.

Gemeente acties: De gemeente heeft een inventarisatie uitgevoerd van de AI-toepassingen die binnen de organisatie worden gebruikt. Alle geïdentificeerde AI-toepassingen zijn geregistreerd in het landelijke algoritmeregister. De bijbehorende richtlijnen voor het gebruik van AI-toepassingen zijn opgesteld en gepubliceerd op okto. Deze richtlijnen dienen als kader voor het verantwoorde gebruik van AI binnen de gemeente.

4. Wet Gegevensverwerking door Samenwerkingsverbanden (WGS) – Ingangsdatum: 1 maart 2025.

Toelichting: Gemeenten werken vaak samen met andere instanties en delen persoonsgegevens. De WGS stelt strengere eisen aan de uitwisseling van gegevens binnen samenwerkingsverbanden, bijvoorbeeld in jeugdzorg, veiligheid en sociale diensten.

Aanbeveling: Controleer of gegevensuitwisseling voldoet aan de WGS-eisen en implementeer waarborgen voor de bescherming van persoonsgegevens binnen samenwerkingsverbanden.

Gemeente acties: De gemeente Weert is betrokken bij het RIEC Midden-Limburg en het Zorg- en Veiligheidshuis Midden-Limburg. De gemeente volgt de ontwikkelingen binnen Roermond, dat de regierol heeft, en monitort hoe de rol van de Coördinerend Functionaris Gegevensbescherming (CFG) wordt ingevuld.

5. Wet Digitale Overheid (Wdo) – Gefaseerde invoering vanaf 1 juli 2023, met volledige implementatie en acceptatieplicht naar verwachting in 2025.

Toelichting: De Wet Digitale Overheid verplicht gemeenten om veilige en toegankelijke digitale dienstverlening te bieden, waaronder het gebruik van DigiD en eHerkenning voor toegang tot gemeentelijke diensten.

Aanbeveling: Evalueer de naleving van DigiD en eHerkenning en werk aan het verbeteren van de digitale toegankelijkheid van gemeentelijke diensten.

Gemeente acties: Volgens de CISO voldoet DigiD aan de normeringen voor alle drie de aansluitingen. Een proces voor erkenning is geïmplementeerd.

6. Baseline Informatiebeveiliging Overheid 2.0 (BIO 2.0) – Ingangsdatum: 2025.

Toelichting: De BIO 2.0 stelt nieuwe eisen aan de informatiebeveiliging binnen de overheid. Gemeenten moeten hun informatiebeveiliging aanpassen aan de nieuwe standaarden om de veiligheid en privacy van gegevens te waarborgen.

Aanbeveling: Voer een GAP-analyse uit en pas het beveiligingsbeleid aan volgens de nieuwe BIO 2.0-richtlijnen.

Gemeente acties: De GAP-analyse is in uitvoering, en er worden verbeteringen doorgevoerd op basis van de nieuwe BIO 2.0-normen.

14. Dreigingsbeeld IBD

De Informatiebeveiligingsdienst (IBD) publiceert periodiek een dreigingsbeeld voor gemeenten. In het meest recente Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2023-2024 worden de volgende belangrijke trends en aanbevelingen genoemd:

Belangrijke trends:

- Toename van ransomware-aanvallen: Het aantal ransomware-aanvallen op gemeentelijke systemen groeit en wordt steeds professioneler uitgevoerd.
- Meer en ernstigere kwetsbaarheden in software: Er worden steeds vaker ernstige fouten in software ontdekt, die door criminelen kunnen worden misbruikt om toegang te krijgen tot gemeentelijke systemen.
- Gevaren in ketens uit het zicht: Samenwerking met externe partijen brengt risico's met zich mee, vooral als het gaat om informatiebeveiliging en privacy binnen deze ketens.

Aanbevelingen om deze dreigingen te minimaliseren:

- Versterken van Cybersecuritymaatregelen: Het is belangrijk om de cybersecuritymaatregelen continu te verbeteren. Dit omvat het versterken van de monitoring en het regelmatig uitvoeren van penetratietests om kwetsbaarheden te identificeren en snel te verhelpen.
    - Dit wordt door de ICT-NML uitgevoerd met behulp van TPM om de uitvoering te waarborgen.
- Uitvoeren van bewustwordingscampagnes: Medewerkers moeten regelmatig getraind worden en bewust worden gemaakt van de verschillende cyberdreigingen die zij kunnen tegenkomen. Door hen beter te informeren over phishingpogingen en andere vormen van cyberaanvallen, kunnen zij deze tijdig herkennen en voorkomen.

    - Hiervoor is Sir Askelot ingezet, die verantwoordelijk is voor de trainingen en bewustwordingssessies voor medewerkers.
- Samenwerken met de IBD en andere Gemeenten: Gemeenten kunnen hun weerbaarheid tegen cyberdreigingen aanzienlijk vergroten door samen te werken en kennis en best practices te delen.
    - Er wordt actief gebruik gemaakt van CISO-overleggen, waarbij de CISO in contact staat met de IBD (Informatie Beveiligingsdienst) en deelneemt aan regionale CISO-overleggen om de collectieve kennis en aanpak te versterken.

15. Ontwikkelingen in AI en Algoritmes

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

AI-systemen die persoonsgegevens verwerken moeten transparant en rechtsgeldig zijn. Gemeenten dienen duidelijk te communiceren over de werking van hun AI-systemen, vooral bij geautomatiseerde besluitvorming. AI-systemen worden op risiconiveau ingedeeld, waarbij hoog-risicosystemen, zoals die in jeugdzorg of fraudecontrole, striktere privacy- en beveiligingsmaatregelen vereisen om discriminatie of onterechte uitsluiting te voorkomen. Gemeenten moeten AI-systemen regelmatig evalueren en auditen om te garanderen dat ze voldoen aan de wettelijke en ethische normen. Daarnaast moeten AI-systemen van externe leveranciers voldoen aan de privacy- en beveiligingseisen van de AI Act, wat om duidelijke verwerkersovereenkomsten en regelmatige controles vraagt.

De gemeente Weert heeft al stappen gezet door AI-toepassingen te registreren in het landelijke algoritmeregister en richtlijnen voor ethisch gebruik van AI te ontwikkelen. Toch zijn aanvullende maatregelen nodig, zoals het verbeteren van de transparantie via privacyverklaringen, het vastleggen van rechtsgrondslagen voor AI-systemen, het uitvoeren van DPIA's voor hoog-risicosystemen, en het instellen van regelmatige audits en leverancierscontroles. Hiermee kan de gemeente volledig voldoen aan de AI Act en de daaraan verbonden ethische en juridische normen.

Conclusie en aanbevelingen

Hoewel de gemeente Weert aanzienlijke vooruitgang heeft geboekt in de voorbereiding op de nieuwe wet- en regelgeving, is volledige naleving nog niet bereikt. De gemeente heeft al belangrijke stappen gezet, zoals het inventariseren van AI-toepassingen en het registreren daarvan in het landelijke algoritmeregister, en het opstellen van richtlijnen voor ethisch gebruik van AI. Ook worden maatregelen genomen om te voldoen aan de NIS2-richtlijn, waaronder het identificeren van kritieke systemen en het opstellen van een

incidentbeheerplan, wat onderdeel is van de lopende IT-audit. Er is al gewerkt aan het verbeteren van de digitale toegankelijkheid van gemeentelijke diensten in lijn met de Wet Digitale Overheid en een GAP-analyse wordt uitgevoerd om de informatiebeveiliging te verbeteren volgens de BIO 2.0.

Echter, de gemeente moet nog verdere stappen zetten, zoals het versterken van de cyberbeveiliging, het uitvoeren van DPIA's voor AI-systemen en het optimaliseren van de gegevensuitwisseling binnen samenwerkingsverbanden. De volledige implementatie en naleving van de wet- en regelgeving worden verwacht in 2025.

Bijlagen (3)

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

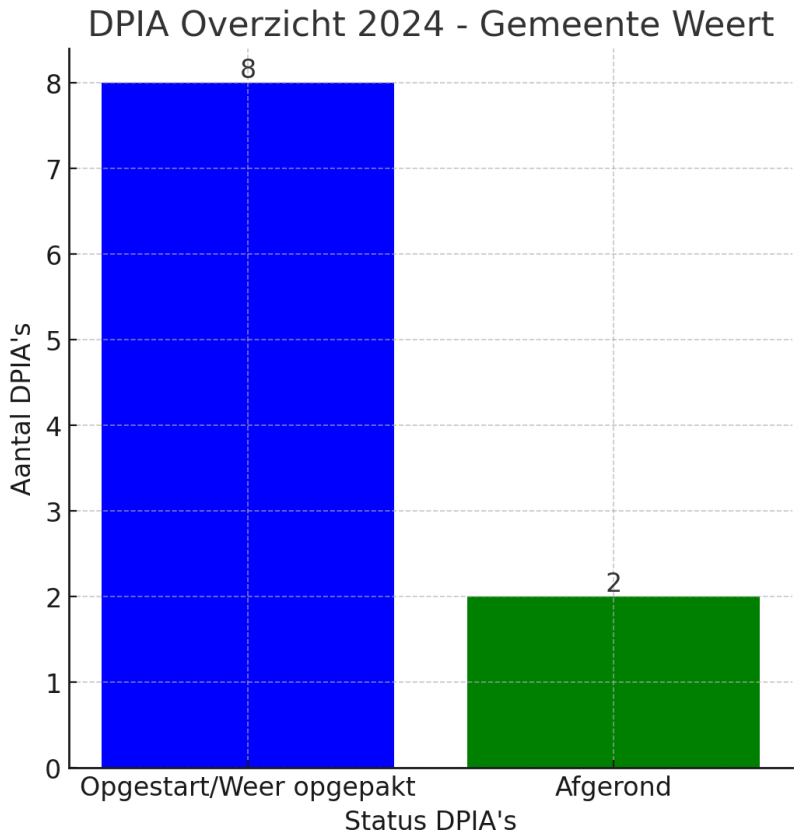
Bijlage 1 - DPIA Overzicht 2024 - Gemeente Weert

DPIA's opgestart/weer opgepakt:

1. Act! Midden-Limburg (regionaal opgepakt)
2. Vangnetoverleg
3. Maatschappelijke opvang
4. Wonen plus
5. Wagenpark (rittenregistratiesysteem)
6. Jeugdzorg facturatiesysteem (regionaal opgepakt)

DPIA's afgerond:

1. Woonkans (regionaal opgepakt)
2. Datamask koppeling Djuma



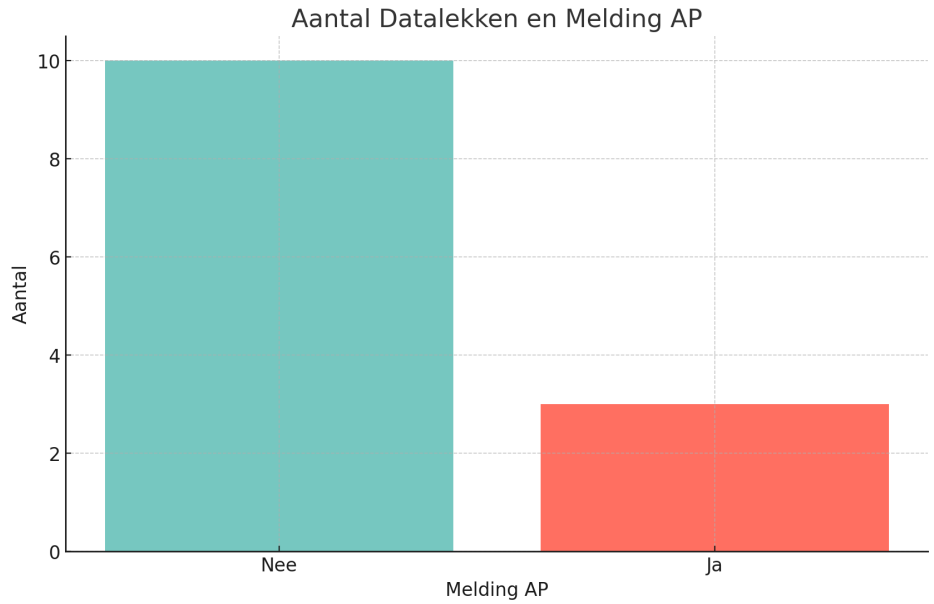
Deze grafiek geeft het DPIA-overzicht van 2024 weer. Het toont het aantal DPIA's dat is opgestart of weer opgepakt en het aantal dat is afgerond.

Bijlage 2 Overzicht Datalekken 2024

Registratie datum	Zaaknummer	Omschrijving	Feiten omtrent inbreuk	Gevolgen	Genomen maatregelen	Melding AP	Melding betrokkenen
9 februari 2024	2371148 (Djuma)	Digitale inbraak bij CLZ	Onbevoegde toegang tot emailboxen CLZ door phishingaanval.	CLZ heeft melding gedaan, gemeente Weert niet verantwoordelijk.	CLZ heeft melding gedaan, geen verdere actie vereist.	Nee	Nee
16 mei 2024	2496768 (Djuma)	Verkeerde bijlagen bij een mail	Verkeerde vergunningen per e-mail naar een andere aanvrager gestuurd.	Onbevoegde heeft persoonsgegevens ingezien.	Foutieve ontvanger heeft documenten verwijderd.	Nee	Nee
8 mei 2024	2486834 (Djuma)	Brief naar verkeerde adres verstuurd	Inwoner ontving per abuis een brief van een andere inwoner.	Verkeerde inwoner zag naam van andere inwoner.	Brief retour gestuurd, foutieve ontvanger heeft deze niet geopend.	Nee	Nee
21 februari 2024	2383586 (Djuma)	Mail met te veel gegevens verstuurd	Te veel persoonsgegevens per mail naar een externe gestuurd via Zivver.	Mail tijdig ingetrokken, geen inzage door externe.	Mail tijdig ingetrokken, geen verdere actie nodig.	Nee	Nee
8 maart 2024	2404710 (Djuma)	Verkeerd gestuurde brieven (jaaropgaven)	14 brieven dubbelzijdig afgedrukt, waardoor 7 inwoners jaaropgave van een ander ontvingen.	Onbevoegde ontvangers hebben persoonsgegevens gezien.	Ontvangers gevraagd foutieve documenten te vernietigen, nieuwe opgaven verstrekt.	Ja	Ja
28 maart 2024	2430016 (Djuma)	Verkeerde bijlage bij e-mail	Door fout in bijlage verkeerde persoonsgegevens naar een inwoner gestuurd.	Persoonsgegevens van een andere inwoner ingezien.	Betrokkene geïnformeerd, foutieve ontvanger heeft mail verwijderd.	Nee	Ja
26 februari 2024	2387375 (Djuma)	Intern mail verkeerd gestuurd	E-mail naar verkeerd afdelingshoofd gestuurd.	Onbedoelde ontvanger zag interne informatie.	Onjuiste ontvanger gevraagd de mail te verwijderen.	Nee	Nee
18 maart 2024	2415634 (Djuma)	Verkeerde bijlage bij e-mail	Verkeerde bijlage in e-mail, persoonsgegevens bij verkeerde ontvanger.	Verkeerde persoon heeft persoonsgegevens van een ander ingezien.	Betrokkene geïnformeerd, foutieve ontvanger heeft document verwijderd.	Nee	Ja
16 augustus 2024	M2408-1671 (Topdesk)	Medewerker gemeente Weert is Ipad verloren in vliegtuig	Ipad van medewerker verloren, maar beveiligd met MFA en pincode.	Geen impact, device volledig gewist.	Device gewist en verwijderd uit MDM en CMDB.	Nee	Nee
19 juni 2024	M2406-2228 (Topdesk)	Veel bestanden zichtbaar op open netwerkschijf	Veel interne bestanden met persoonsgegevens toegankelijk voor medewerkers.	Interne medewerkers hadden toegang tot gevoelige gegevens.	Bestanden verwijderd, migratie en autorisatiecontrole ingepland.	Ja	Nee

Registratie datum	Zaaknummer	Omschrijving	Feiten omtrent inbreuk	Gevolgen	Genomen maatregelen	Melding AP	Melding betrokkenen
30 september 2024	M2410-2861 (Topdesk)	Brief naar verkeerde adres verstuurd	Onderzoeksverslag met verkeerde begeleidende brief naar inwoner gestuurd.	Inwoner zag onderzoeksverslag van een andere inwoner.	Brief retour gestuurd, correcte brief alsnog toegestuurd.	Ja	Ja
7 augustus 2024	M2408-0898 (Topdesk)	Verkeerd gestuurde brieven	Drie brieven naar verkeerde ontvangers gestuurd.	Drie inwoners zagen gegevens van een ander.	Afdeling geadviseerd controles te verbeteren.	Nee	Nee
1 november 2024	M2411-0034	Ransomware JCC software	Ransomware-aanval op JCC software, beperkte impact op gemeentegegevens.	Beperkte impact, mogelijk alleen basisgegevens buitgemaakt.	Geen actie nodig, JCC had eigen lek.	Nee	Nee

1. Aantal datalekken en melding AP
2.



Deze grafiek toont het aantal datalekken (13), verdeeld over de meldingen (3) naar de Autoriteit Persoonsgegevens (AP).

Bijlage Nulmeting n.a.v. verplichtingen AVG

Onderdeel	Vraag	Bron (Document)	Beoordeling
1. Beleid en procedures	Is er een formeel en actueel gegevensbeschermingsbeleid?	Privacybeleid Gemeente Weert 2023-2026	Ja, het beleid is vastgesteld en gepubliceerd op de website.
	Zijn er procedures voor datalekken, DPIA's en verzoeken van betrokkenen?	Privacybeleid Gemeente Weert 2023-2026, Datalekkenoverzicht 2023	Ja, er zijn procedures voor datalekken en DPIA's, maar naleving moet structureler worden gecontroleerd.
	Zijn de procedures bekend en toegankelijk voor medewerkers?	Privacybeleid Gemeente Weert 2023-2026	Ja, medewerkers zijn zich bewust van het beleid en hebben toegang tot de procedures.
2. Gegevensverwerkingen en verwerkingsregister	Is er een volledig en actueel verwerkingsregister?	Openbaar Verwerkingsregister	Ja, er is een register, maar periodieke controle en updates ontbreken.
	Welke soorten persoonsgegevens worden verwerkt, en wat is het doel ervan?	Openbaar Verwerkingsregister	Diverse gegevens (NAW, BSN, financiële data) worden verwerkt voor wettelijke taken.
	Is er een wettelijke basis voor alle verwerkingen?	Openbaar Verwerkingsregister	Ja, alle verwerkingen zijn gekoppeld aan een wettelijke basis zoals de AVG.
	Hoe wordt de verwerking van gevoelige gegevens gemanaged?	Privacybeleid Gemeente Weert 2023-2026	Er zijn extra beveiligingsmaatregelen voor gevoelige persoonsgegevens zoals gezondheidsgegevens.
3. Toestemming en Rechten van Betrokkenen	Wordt er op de juiste wijze toestemming gevraagd?	Privacybeleid Gemeente Weert 2023-2026	Ja, toestemming wordt gevraagd waar nodig, bijvoorbeeld voor marketing of cameratoezicht.

Onderdeel	Vraag	Bron (Document)	Beoordeling
	Hoe worden betrokkenen geïnformeerd over hun rechten (privacyverklaringen)?	Privacybeleid Gemeente Weert 2023-2026	Privacyverklaringen zijn beschikbaar en toegankelijk via de website.
	Hoe worden verzoeken van betrokkenen (inzage, correctie, verwijdering) afgehandeld?	Privacybeleid Gemeente Weert 2023-2026	Er is een proces voor verzoeken van betrokkenen, maar de opvolging en registratie kunnen verbeterd worden. Informatie is beschikbaar op de website.
4. Datalekken en Incidentmanagement	Is er een formeel protocol voor het melden en afhandelen van datalekken?	Datalekkenoverzicht	Ja, een protocol is aanwezig en datalekken worden geregistreerd.
	Worden medewerkers getraind om datalekken te herkennen en te melden?	Recourse - Sir Askelot	Trainingen worden aangeboden via Sir Askelot, maar deelname is te laag.
	Worden datalekken binnen 72 uur gemeld aan de Autoriteit Persoonsgegevens?	Datalekkenoverzicht	Ja, meldplicht wordt nageleefd volgens het datalekregister.
5. Data Protection Impact Assessments (DPIA's)	Worden DPIA's uitgevoerd voor risicovolle projecten?	Overzicht (pré) DPIA's	Ja, maar er is een achterstand in de uitvoering van DPIA's.
	Bestaat er een procedure voor het uitvoeren en beoordelen van DPIA's?	Privacybeleid Gemeente Weert 2023-2026	Ja, maar naleving en structurele evaluatie kunnen verbeterd worden.
	Hoe worden de resultaten van DPIA's opgevolgd?	Overzicht (pré) DPIA's	Uitkomsten leiden tot actiepunten, maar structurele opvolging ontbreekt soms.
6. Toegang en Autorisatiebeheer	Wordt er gewerkt met rolgebaseerde toegang?	Informatiebeveiligingsbeleid 2025-2026	Ja, toegang is gebaseerd op rollen en functies.
	Hoe wordt toegang geregeld en geëvalueerd?	Informatiebeveiligingsbeleid 2025-2026	Toegang wordt beheerd, maar periodieke evaluaties ontbreken.
	Zijn er procedures voor het intrekken van toegang?	Informatiebeveiligingsbeleid 2025-2026	Ja, maar naleving wordt niet altijd goed gedocumenteerd.

Onderdeel	Vraag	Bron (Document)	Beoordeling
7. Beveiliging van Persoonsgegevens	Worden persoonsgegevens versleuteld?	Informatiebeveiligingsbeleid 2025-2026	Ja, encryptie wordt toegepast.
	Worden back-ups veilig beheerd en opgeslagen?	Informatiebeveiligingsbeleid 2025-2026	Ja, back-ups worden beveiligd en getest.
	Is er een informatiebeveiligingsbeleid dat regelmatig wordt geëvalueerd?	Informatiebeveiligingsbeleid 2025-2026	Ja, het beleid volgt BIO en ISO 27001-normen.
8. Verwerkersovereenkomsten en Derde Partijen	Zijn er verwerkersovereenkomsten met alle derde partijen?	Privacybeleid Gemeente Weert 2023-2026	Ja, maar structurele controle op naleving ontbreekt.
	Worden verwerkers periodiek gecontroleerd?	Privacybeleid Gemeente Weert 2023-2026	Er is geen structurele audit op verwerkers.
	Hoe worden verwerkers gemonitord?	Privacybeleid Gemeente Weert 2023-2026	Monitoring is niet structureel gedocumenteerd.
9. Bewaartermijnen en Geautomatiseerde Verwijdering	Zijn er bewaartermijnen vastgesteld?	Openbaar Verwerkingsregister	Ja, bewaartermijnen zijn vastgesteld in het register.
	Worden gegevens verwijderd na het verstrijken van de termijn?	Privacybeleid Gemeente Weert 2023-2026	Gegevens worden verwijderd, maar automatisering ontbreekt.
10. Training en Bewustwording	Worden medewerkers regelmatig getraind?	Plan van Aanpak FG 2024	Ja, maar deelnamegraad moet verbeterd worden.
	Is er een bewustwordingsprogramma?	Plan van Aanpak FG 2024	Ja, maar effectiviteit is niet structureel gemeten.
15. Internationale Gegevensoverdracht	Worden persoonsgegevens overgedragen buiten de EU?	20250 124 - AVG - verwerkingsregister	Geen documentatie beschikbaar over internationale overdracht.
	Zijn er waarborgen zoals BCR's?	20250 124 - AVG - verwerkingsregister	Geen documentatie over BCR's of andere waarborgen.

Deze nulmeting/gapanalyse beoordeelt de mate waarin de gemeente Weert voldoet aan de privacy- en gegevensbeschermingsverplichtingen, zoals vastgelegd in de AVG.

Algemene conclusie en aanbevelingen nulmeting

De gemeente voldoet deels aan de wettelijke verplichtingen, maar er zijn duidelijke verbeterpunten:

1. Privacyverklaring: Harmoniseer en actualiseer de verklaringen om consistentie en volledigheid te waarborgen.
2. Register van verwerkingen: Actualiseer het document en voeg ontbrekende details toe.
3. Incidentenregeling: Ontwikkel een aparte regeling met gestructureerde stappen en verantwoordelijkheden.
4. DPIA-procedure: Implementeer een gestandaardiseerde aanpak en werk achterstanden weg.