Jaarverslag Gegevensbescherming Gemeente Heerlen 2023

GEMEENTE HEERLEN Jaarverslag 2023

Functionaris Gegevensbescherming: C.H.M van de Wert / A.P.J. van Alphen

Heerlen

Inhoudsopgave

1. Voorwoord en verantwoording

De Functionaris Gegevensbescherming (FG) is de interne toezichthouder van de gemeente Heerlen en houdt toezicht op de naleving van de wet- en regelgeving rond de bescherming van de privacy en de verwerking van persoonsgegevens. De Algemene verordening gegevensbescherming (Avg) en de Wet politiegegevens (Wpg) zijn de wettelijke basis voor het toezicht van de FG. De FG controleert of betrokkenen hun privacyrechten kunnen uitoefenen en ziet toe op een correcte afhandeling van privacy-klachten over en -incidenten bij het verwerken van persoonsgegevens, waaronder datalekken

1.1 Vertraging jaarverslag

Het opstellen van het jaarverslag gegevensbescherming 2023 heeft meer tijd in beslag genomen omdat de vorige Functionaris Gegevensbescherming (FG) eind april 2023 ontslag heeft genomen en er enkele discussiepunten waren qua feitelijkheid en context van het destijds opgestelde concept jaarverslag.
Per 1 juli is een deeltijd FG aangesteld die al eerder, eind 2021 tot en met 2023, bij de gemeente Heerlen had gewerkt in de rol van Privacy Officer. Hij is daarnaast deeltijd FG is bij een zorginstelling. De nieuwe FG heeft het verslag beoordeeld en aangepast waarbij de feiten de feiten zijn gebleven.

1.2 Lopende verbeteringen in 2024

Een aantal benoemde verbetervoorstellen in het jaarverslag 2023 zijn opgepakt in 2024:

1) Register van Verwerkingen[1]
2) Proces-beschrijvingen
3) Actualiseren en daar waar nodig vaststellen beleidsdocumenten (privacy en informatiebeveiliging)
4) Document-management
5) Bewustwording en awareness
6) Eigenaarschap informatiesystemen en processen met beschreven verantwoordelijkheden voor de eigenaar
7) Identificeren/actualiseren kritische informatiesystemen en processen (kroonjuwelen)
8) Capaciteit
9) Gebruik Djuma voor inzagerecht betrokkenen.

1.3 Context

Het cluster privacy komt van ver. In 2021 en 2022 was er een aanzienlijk personeelsverloop van Privacy Officers en FG wat leidde tot een fors verlies van de aanwezige kennis, ervaring en inzicht. Dit had nadelige gevolgen voor de tijdigheid afhandeling van incidenten, verzoeken, projecten en compliancy. Daarom werd begin 2022 een verbeterprogramma opgestart met externe ondersteuning om nieuwe medewerkers te coachen, achterstallig werk in te halen en verbeteringen door te voeren op operationeel, tactisch en strategisch niveau. Dit heeft geleid tot verbeterde werkwijze, rapportage, inzichten en maatregelen.

Nog niet alle verbetermaatregelen zijn geheel geëffectueerd, waarbij beter inzicht soms juist leid tot meer verbetermaatregelen.

Het gezegde “het glas halfvol of halfleeg” is een mooie analogie voor dit jaarverslag.
Met de doorgevoerde verbeteringen, inzicht en verbeterplannen is het glas zich aan het vullen; de optimistische benadering. Maar de FG als toezichthouder ziet dat het glas nog niet vol is en daar ligt de nadruk op in dit jaarverslag.

A.P.J. van Alphen CIPP/E CIPM FIP

---

[1] Het verwerkingsregister is een verplichting uit de AVG en Wpg en dient te bevatten:

- verwerkingsdoeleinden
- verwerkingsgrondslag
- categorieën betrokkenen
- categorieën persoonsgegevens
- categorieën ontvangers
- informatie over eventuele doorgifte van persoonsgegevens naar een derde land
- bewaartermijnen
- beveiligingsmaatregelen

2. Management samenvatting

De management samenvatting van dit rapport biedt een grondige analyse van de privacy- en gegevensbeschermingspraktijken binnen de gemeente Heerlen in het jaar 2023 voor de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Het rapport benadrukt de uitdagingen en aandachtspunten die zijn geconstateerd, en biedt aanbevelingen om deze aan te pakken en te verbeteren voor het jaar 2024.

Terugblik op 2023:

- Het privacy- en informatiebeveiligingsteam heeft hard gewerkt, maar er blijven uitdagingen bestaan, met name door de toename van gegevensverwerkingen en incidenten die veel tijd en energie vergen. Bij optredende piekbelastingen zijn er prioriteiten gesteld.
- Er zijn 148 nieuwe privacy casussen geïdentificeerd, maar de registratie is niet volledig, wat suggereert dat het werkelijke aantal hoger kan zijn.
- Er zijn problemen met de bekendheid van gegevensverwerkingsprocessen, waardoor wettelijke controle en toezicht niet adequaat kunnen worden uitgevoerd. Het fundament daarvoor zou het verwerkingsregister (I-navigator) dienen te zijn.
- Het privacybeleid is niet altijd correct geïmplementeerd en vertaald naar werkprocessen, waardoor de naleving van de wetgeving in gevaar komt.
- Er zijn verschillende datalekken en inbreuken op de gegevensbeveiliging geweest, waarbij niet altijd adequaat is gereageerd.
- Verplichte DPIA's worden niet altijd uitgevoerd.

Aanbevelingen en vooruitzichten voor 2024:

- Herziening en actualisering van privacybeleid om te voldoen aan relevante wet- en regelgeving.
- Verbetering van documentbeheer om transparantie te garanderen en verouderde beleidsstukken te voorkomen.
- Duidelijke definities van verantwoordelijkheden van het management met betrekking tot privacy.
- Versterking van procesbeschrijvingen en betrokkenheid van afdelingen.
- Uitbreiden van het privacyteam en/of privacytaken meer beleggen in de organisatie.
- Verbetering van bewustwording door middel van training en campagnes.
- Optimalisatie van processen binnen informatiemanagement en portfoliomanagement.
- Bijwerken van de privacyverklaring om te voldoen aan de vereisten van transparantie en naleving.

Conclusie:
De FG erkent de vooruitgang die is geboekt, maar benadrukt dat er nog veel werk moet worden verzet om volledig compliant te zijn aan de AVG, UAVG[2] en de Wpg. Het jaarverslag biedt concrete aanbevelingen om de privacy- en gegevensbeschermingspraktijk te verbeteren die aansluit bij toekomstige ontwikkelingen waaronder AI. CISO en FG werken nauw samen om persoonsgegevens afdoende veilig te beschermen middels technische en organisatorische maatregelen.

C.H.M. van de Wert

3. Inleiding

Deze rapportage is bedoeld om het college van burgemeester en wethouders, de burgemeester en de gemeenteraad van de Gemeente Heerlen te informeren omtrent de borging van gegevensbescherming binnen de gemeente. De rapportage is organisatie breed opgesteld en niet gespecificeerd op de verschillende teams.

De rapportage is een wettelijke verplichting vanuit de Wpg (art 36) terwijl die voor de AVG wordt aanbevolen door de toezichthouder Autoriteit Persoonsgegevens.

Deze rapportage is voortgekomen uit ervaringen en onderzoeken die de FG zelf heeft verricht en de door de FG afgenomen interviews met medewerkers. Hierdoor is een beeld ontstaan wat de gemeente Heerlen heeft bereikt op het gebied van gegevensbescherming en welke maatregelen er zijn genomen om te voldoen aan de AVG en de Wpg.

De criteria die in zowel het jaarverslag als het jaarplan worden genoemd zijn afkomstig van het borgingsproduct 3.0 Toetsingskader en documentatie van de Informatiebeveiligingsdienst (VNG) en dienen als een standaard voor deze rapportages. In dit borgingsproduct worden criteria en maatregelen omschreven die de AVG en de Wpg vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen.

7 thema's
De rapportage is opgebouwd aan de hand van de zeven thema's:

- Beleid
- Organisatorische inbedding
- Processen
- Rechten van betrokkenen
- Samenwerking
- Gegevensbescherming
- Verantwoording

[2]UAVG Uitvoeringswet AVG

Dit jaarverslag bestaat uit 3 onderdelen:
Deel A: het verslag over de AVG;
Deel B: de bevindingen over de Wpg;
Deel C: relevante ontwikkelingen op het gebied van gegevensbescherming.

Aangezien zowel de AVG als de Wpg gaan over het beschermen van persoonsgegevens is er één jaarverslag. De opbouw van het verslag is grotendeels hetzelfde:

- Dashboard: stoplichtrapportage op basis van de thema's uit de AVG en Wpg. Voor de AVG wordt hierbij verwezen naar de thema's uit het AVG borgingsproduct.
- Vervolgens worden per thema de bevindingen en aanbevelingen beschreven.
- In de bijlage wordt een nadere onderbouwing gegeven aan het verslag door middel van onder meer verdieping per thema en kengetallen.

4. Deel A: AVG

4.1. AVG-dashboard

De bedoeling van dit dashboard is om in één oogopslag een beeld te geven van de stand van zaken rondom de naleving van de AVG.

Thema:	2019	2023	2024
Borging AVG	**Jaarverslag**	**Resultaat**	**Verwacht**
Beleid			
Processen			
Organisatorische inbedding			
Rechten van betrokkenen			
Samenwerking			
Gegevensbescherming			
Verantwoording			

Legenda:
AANDACHT VEREIST VAN MANAGEMENT
IN TE HALEN ACHTERSTAND
OP SCHEMA

4.2. Deel 1. Terugblik op 2023

Het is de taak van de FG om terug te kijken naar wat de gemeente Heerlen in 2023 heeft bereikt, en te evalueren welke werkzaamheden en bevindingen de FG heeft gedaan als toezichthouder. Ik zie dat iedereen met veel toewijding en inzet werkt om ervoor te zorgen dat we de controle krijgen over onze processen met wisselend succes.

Naast de reguliere taken op het gebied van privacy en informatiebeveiliging, zijn er ook extra situaties geweest waarop de privacy- en informatiebeveiligingsafdeling moest reageren, zowel in 2023 als in voorgaande jaren. Deze situaties hebben veel tijd en energie van het team gevraagd. Er zijn in 2023 in totaal 148 nieuwe casussen aangeleverd bij het privacyteam waarbij de tijdsbesteding per casus enorm verschilt en afhandeling kan soms enkele weken in beslag nemen. De registratie is niet volledig en dit aantal is hoger. Zie bijlage 2 voor een nadere uitwerking van deze casussen.

Binnen de gemeente Heerlen zijn er 1104 geregistreerde processen voor gegevensverwerking (bron: INavigator 2024). Echter, er zijn processen die niet bekend zijn bij de afdeling privacy en informatiebeveiliging, waardoor mogelijk de wettelijke controle en toezichttaken niet kunnen worden uitgevoerd. De rechtmatigheid van deze verwerkingen wordt niet voldoende gegarandeerd en gecontroleerd. Van deze 1104 processen bevatten 792 verwerkingen persoonsgegevens, waaronder normale, bijzondere, gevoelige en strafrechtelijke persoonsgegevens. Informatiebeveiliging is van toepassing op alle 1104 processen.

Er zijn 10 Data Privacy Impact Analyses (DPIA's) uitgevoerd op nieuwe processen of op wijzigingen in bestaande processen. Het totaal aantal te verrichten DPIA’s is nog niet compleet vastgesteld en zal nader onderzocht moeten worden.

De FG heeft 5 onderzoeken uitgevoerd waarbij de privacy op een bepaalde manier was geschonden. Er zijn 6 adviezen opgesteld voor het management. De FG heeft zijn toezichthoudende taken gecombineerd met de ondersteunende werkzaamheden richting het privacyteam.

4.2.1. Beleid

Het privacybeleid van de gemeente Heerlen dient als leidraad voor de verwerking van persoonsgegevens, waarin de principes en maatregelen worden vastgelegd die de gemeente hanteert om te voldoen aan relevante wet- en regelgeving, zoals de AVG, UAVG, Gemeentewet, Jeugdwet, WMO 2015, Politiewet 2012 en de Wpg. In het begin van 2020 heeft het college een nieuw intern privacybeleid vastgesteld na goedkeuring van de OR. Naast dit specifieke beleid bestaan er diverse protocollen binnen verschillende beleidsregels die direct betrekking hebben op privacy en worden uitgewerkt in procesbeschrijvingen.

Gezien de toenemende en voortdurende verwerking van persoonsgegevens, evenals de nieuwe vereisten die de gemeente Heerlen nog te wachten staan in 2024 en verder, is het

naleven van deze wetgevingen een aanzienlijke uitdaging. Door de introductie van de Djuma-applicatie zijn er echter stappen gezet om werkprocessen en procedures adequaat vast te leggen, wat heeft bijgedragen aan verdere professionalisering. Hoewel dit proces bestuurlijk is geoptimaliseerd is, blijft er nog ruimte voor verbetering.

Het is van cruciaal belang dat privacy- en informatiebeveiligings-beleidsdocumenten vindbaar worden opgeslagen met een adequaat versiebeheer, iets waar momenteel onvoldoende aandacht aan wordt besteed. Het vinden van de actuele versie van intern beleid is een uitdaging en er bestaat behoefte aan meer structuur. Bovendien wordt er verwezen naar beleidsstukken die niet officieel zijn vastgesteld of verouderd zijn of waarvan de status onduidelijk is.

Het valt op dat het privacybeleid niet altijd correct is geïmplementeerd en vertaald naar werkprocessen binnen de verschillende afdelingen. De herziening van het privacybeleid, gepland voor 2023, heeft niet volledig plaatsgevonden, waardoor verwerkingen binnen de Wpg bijvoorbeeld niet zijn opgenomen, hoewel dit wel vereist is. Mede hierdoor voldoet het privacybeleid momenteel niet volledig aan de gestelde eisen.

Binnen het privacybeleid is onvoldoende vastgelegd dat het management verantwoordelijk is voor het behalen van de doelstellingen. Deze verantwoordelijkheden zijn niet duidelijk gedefinieerd en geformaliseerd. Hoewel verantwoordelijken/management soms betrokken zijn bij privacy- en informatiebeveiligingsvraagstukken, ontbreekt het aan voortgangsrapportages en een overlegstructuur om dit te ondersteunen.

De privacyverklaring richting medewerkers en inwoners van de gemeente Heerlen is onvolledig, waardoor transparantie en naleving van wettelijke bepalingen niet gegarandeerd is.

Bovendien is in het privacybeleid niet duidelijk vastgelegd dat het management verantwoordelijk is voor het realiseren van de doelstellingen ervan, wat tot onduidelijkheid leidt over wie welke verantwoordelijkheden draagt.

4.2.2. Processen

De verwerkingen van persoonsgegevens door de gemeente Heerlen dienen te voldoen aan de AVG, de Wpg en alle andere van toepassing zijnde wetgevingen. Dit houdt in dat je de werkprocessen waarin persoonsgegevens verwerkt worden moet toetsen en inrichten volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid.
Verder kan de gemeente in bepaalde gevallen verplicht zijn om een (pré) DPIA uit te voeren.

De gemeente Heerlen erkent dat er nog aanzienlijke inspanningen nodig zijn om de processen adequaat te beschrijven. Binnen het team informatiemanagement wordt actief gestuurd op deze ontwikkeling binnen de verschillende afdelingen.
In de applicatie Engage worden de processen per afdeling verder uitgewerkt, onder begeleiding van het informatiemanagementteam. Echter, er lijkt een zekere mate van vrijblijvendheid te zijn ten aanzien van deze inspanningen, wat het proces vertraagt. Een

heldere beschrijving van de processen biedt direct meer inzicht en stelt de gemeente Heerlen in staat om beter te voldoen aan de eisen van de AVG. Deze processen kunnen namelijk worden gekoppeld aan INavigator, dat fungeert als verwerkingsregister en het versnelt de afhandeling van alle casussen die zijn genoemd in het cijfermatige overzicht. Zie bijlage 2.

4.2.3. Organisatorische inbedding

Het privacyteam speelt een cruciale rol in het waarborgen van de privacy binnen onze organisatie, maar helaas is het team momenteel onderbezet. De dagelijkse uitdagingen en het beheren van incidenten vergen zoveel tijd dat de taken die nodig zijn voor verdere professionalisering niet kunnen worden uitgevoerd. Deze situatie heeft geleid tot een reactieve aanpak waarbij we voornamelijk bezig zijn met het managen van incidenten, in plaats van proactief te werken aan een robuust privacykader.

Gemeente Heerlen heeft de keuze gemaakt om de FG geen onderdeel te laten zijn van de bestuursdienst maar in te bedden bij het Team Informatie Management. De onafhankelijke positie met bevoegdheden vanuit de Awb is gewaarborgd door een aanwijzingsbesluit FG[3] van het college. Van de FG wordt verwacht dat hij tijdig en adequaat de juiste functies informeert bij voorkeur in de lijn maar kan met eigen discretie daarvan afwijken.
Het aanwijzingsbesluit dient voor wat betreft de verantwoordelijkheid voor het bijhouden van het verwerkingsregister te worden geactualiseerd naar de actualiteit: de FG kan niet verantwoordelijk zijn voor een activiteit waar hij vanuit de AVG toezicht op dient te houden.

Voor een effectieve naleving van de AVG is het van vitaal belang dat alle medewerkers binnen de gemeentelijke organisatie vertrouwd zijn met de beginselen van de AVG, de Wpg en het belang van privacy. Dit vereist een duidelijke organisatorische inbedding waarbij taken, verantwoordelijkheden en bevoegdheden worden toegewezen en bewustwording wordt gecreëerd op alle niveaus.

Op dit moment ontbreekt het aan een heldere toewijzing van taken en verantwoordelijkheden binnen onze organisatie, wat de verdere professionalisering op het gebied van AVG en Wpg belemmert, evenals de algemene naleving van wet- en regelgeving. Het formeel toewijzen van taken en verantwoordelijkheden is van essentieel belang om bewustwording op alle niveaus te bevorderen en een cultuur van privacybescherming te bevorderen.

In 2023 zijn er enkele stappen ondernomen om het bewustzijn te vergroten, waaronder bewustwordingssessies bij verschillende afdelingen om bijvoorbeeld een privacyverklaring op te stellen die inzicht geeft in gegevensverwerkingen. In 2024 zal er nog meer nadruk liggen op bewustwording door middel van gerichte campagnes en zal er ondersteuning komen in 2025 door middel van een softwarepakket om de naleving van privacyregelgeving te vergemakkelijken.

4.2.4. Rechten van betrokkenen

De gemeente is verplicht om zowel actief als passief de personen van wie zij persoonsgegevens verwerkt (de betrokkenen) te informeren over hoe hun gegevens worden

[3] Gemeenteblad 2020, 7722 | Overheid.nl > Officiële bekendmakingen

verwerkt, de wettelijke basis hiervoor, en welke maatregelen worden genomen om ongeoorloofde toegang en verwerking te voorkomen. Bovendien geeft de AVG betrokkenen een aantal rechten waarmee ze controle kunnen uitoefenen over hun persoonsgegevens. Het is de verantwoordelijkheid van de gemeente om betrokkenen op deze rechten te wijzen en ervoor te zorgen dat zij deze rechten ook kunnen uitoefenen.

Helaas voldoet de gemeente Heerlen maar gedeeltelijk aan deze verplichtingen. Onze gemeentewebsite geeft niet duidelijk aan welke persoonsgegevens we verwerken en voor welke doeleinden, zoals vereist in een privacyverklaring. Deze vindbare verklaring moet onder andere de identiteit en contactgegevens van de verantwoordelijke voor de gegevensverwerking bevatten, evenals de contactgegevens van de FG, de doeleinden van de verwerking en de bewaartermijn van de gegevens.

Er zijn 21 verzoeken binnengekomen bij de afdeling privacy die betrekking hadden op de rechten van betrokkenen. Het verwerken van deze verzoeken heeft een aanzienlijke impact gehad op het privacyteam en alle betrokken afdelingen. Bovendien is niet alle informatie over gegevensverwerkingen binnen de gemeente Heerlen duidelijk in kaart gebracht, wat resulteert in een zoektocht naar beschikbare informatie. Tijdens dit proces is geconstateerd dat bewaartermijnen niet worden nageleefd, verwerkingen niet zijn opgenomen in INavigator en de opslagmethode niet gedocumenteerd is. Daarnaast wordt de applicatie Microsoft Outlook mail soms gebruikt als een soort database, waarbij geen controle plaatsvindt op bewaartermijnen, evenals bij de mappenstructuur.
Hierdoor kan men niet volledig voldoen aan de rechten van betrokkenen en is het essentieel dat het verwerkingsregister INavigator prioriteit krijgt en de daaronder gekoppelde processen juist worden omschreven.

4.2.5. Samenwerking

De gemeente Heerlen werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: het ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt hieronder. Deze verwerkingen dienen dan te voldoen aan de AVG en Wpg. De gemeente Heerlen maakt hierover afspraken met deze andere partijen door verwerkersovereenkomsten, gegevensleveringsovereenkomsten, convenanten of andere overeenkomsten waarin compliant (AVG en/of Wpg) persoonsgegevens al dan niet eenzijdig worden gedeeld of uitgewisseld. Alleen als er een wettelijke plicht is voor uitwisselen van persoonsgegevens kan hiervan worden afgeweken.

In 2023 zijn er minimaal 10 DPIA's gemaakt, een aantal convenanten en ettelijke verwerkersovereenkomsten opgesteld met organisaties waarmee wij samen werken. Ook hier is sprake van een grote impact op de beschikbare tijd (met name bij het opstellen of beoordelen van convenanten en DPIA's) van het team en voldoen we nog niet aan de minimale eis. Ook van bestaande verwerkingen moeten er DPIA's worden opgemaakt maar het ontbreekt aan beschikbare tijd. Aan het advies van de AP om periodiek (minimaal 3 jaar) een DPIA uit te voeren op risicovolle gegevensverwerkingen komen we in het geheel niet aan toe.

4.2.6. Gegevensbescherming

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente Heerlen passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Bovendien geldt er onder de AVG een meldplicht voor inbreuken met persoonsgegevens (privacyincidenten).

Dit houdt in dat incidenten, waaronder inbreuken op de beveiliging, onder bepaalde omstandigheden gemeld dienen te worden aan de Autoriteit Persoonsgegevens (AP) en/of de betrokkenen. Dit proces is binnen het privacyteam goed ingericht, waarbij de verantwoordelijkheden en het bijbehorende proces zijn beschreven. Meldingen kunnen op verschillende manieren worden doorgegeven aan het team, waarna zij direct actie ondernemen.

In 2023 hebben er 23 "geregistreerde" datalekken plaatsgevonden. 10 datalekken werden als hoog risico beschouwd voor de betrokkenen, waarbij meldingen zijn gedaan aan de betrokkenen. Het aantal personen dat is geïnformeerd, overschrijdt de 100. Daarnaast heeft de gemeente Heerlen 19 incidenten gemeld aan de AP, waarbij 3 incidenten nadere vragen zijn gesteld en bij een datalek een verplichting werd opgelegd aan de gemeente Heerlen om betrokkenen in te lichten.

Informatiebeveiliging is een zeer belangrijk onderdeel van de gegevensbescherming en de normeringen zijn duidelijk. De implementatie van al deze maatregelen staat onder druk. De Baseline Informatiebeveiliging Overheid (BIO) bevat een set van standaarden en richtlijnen voor informatiebeveiliging die specifiek zijn ontwikkeld voor de Nederlandse overheid. De BIO is gebaseerd op internationale standaarden voor informatiebeveiliging, zoals ISO 27001 en ISO 27002, maar is aangepast aan de specifieke behoeften en omstandigheden van de Nederlandse overheid. Je moet dan opzet, bestaan, werking en effectiviteit kunnen aantonen.

Deze eisen worden dit jaar al opgelegd binnen de ENSIA-DigiD scope en er wordt gelet op onderstaande punten.

- Toegangsbeheer: Vereist is het aanleveren van een overzicht van alle autorisatiemutaties binnen de DigiD-scope gedurende de controleperiode, inclusief een tweedelijns controlerapport of een alternatief.
- Beveiligingsincidentenbeheer: Vereist is het aanleveren van een overzicht van alle beveiligingsincidenten binnen de DigiD-scope, inclusief bewijs van opvolging en rapportages, evenals een tweedelijns controlerapport of een alternatief.
- Monitoring systemen: Vereist is het aanleveren van een overzicht van alle alarmeringen, periodieke controles en analyses binnen de DigiD-scope, met betrekking tot wijzigingen aan de configuratie, verdachte gebeurtenissen, toegangslogs en incidentopvolging, evenals een tweedelijns controlerapport of een alternatief.
- Wijzigingsbeheer: Vereist is het aanleveren van een overzicht van alle wijzigingen binnen de DigiD-scope gedurende de controleperiode, inclusief wijzigingsverzoeken, testplannen, testrapporten en formele acceptatie van wijzigingen, evenals een tweedelijns rapport of een alternatief.

- Patchbeheer: Vereist is het aanleveren van een overzicht van alle patches binnen de DigiD-scope gedurende de controleperiode, inclusief informatie over de uitvoering van patches, evenals een tweedelijns rapport of een alternatief.

Er ligt veel werk wat verricht moet worden en er is een achterstand. Terwijl de eisen en verplichtingen de neiging hebben elk jaar toe te nemen.

Ook hier zal een keuze gemaakt moeten worden om zodoende mensen en middelen vrij te maken om de achterstand weg te werken en de nieuwe ontwikkelingen aan te kunnen.

4.2.7. Verantwoording

De verantwoordelijkheid om aan te tonen of en in welke mate wordt voldaan aan de privacyregels ligt bij de gemeente zelf. Dit is in de AVG zo geregeld. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Aan deze verantwoordingsverplichting kan de gemeente Heerlen niet altijd voldoen.
Het ontbreekt nu aan periodieke evaluaties waarin de naleving van de AVG bij de uitvoering van taken wordt beoordeeld. De FG heeft een toezichtplan om als toezichthouder de naleving van de AVG te controleren en er worden daadwerkelijk controles uitgevoerd op de naleving van de AVG.
Geconstateerde afwijkingen bij de naleving van de AVG worden niet structureel opgevolgd door de organisatie. Bij informatiebeveiliging wordt niet altijd de uitvoering van het informatiebeveiligingsbeleid en de naleving van processen, procedures en standaarden beoordeeld. Ook hier speelt de personele bezetting een belangrijke rol. Het informatiebeveiligingsbeleid van 2017 is niet vastgesteld.
Onze informatiesystemen worden niet door of namens de gemeente Heerlen jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's met betrekking tot de feitelijke veiligheid, bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.
Het management en het bestuursorgaan is niet altijd adequaat geïnformeerd over de naleving van de AVG door de organisatie.

4.2.8. Conclusie

Ik zie dat binnen het vakgebied van Informatiemanagement veel aandacht wordt besteed aan privacykwesties. Er zijn processen ontwikkeld waarbij via intakes, portfolio-overleggen en projecten een grondiger inzicht wordt verkregen in alle gegevensverwerkingen binnen de gemeente Heerlen. De complexiteit van deze processen is aanzienlijk en zowel het privacyteam maar nog meer het management spelen hierbij een cruciale rol.

De uitdagingen om te voldoen aan de AVG en de Wpg zijn aanzienlijk en zullen naar verwachting alleen maar toenemen. Denk hierbij aan de implementatie van kunstmatige intelligentie (AI) en andere technologische ontwikkelingen die de komende jaren bij de gemeente Heerlen zullen worden geïntroduceerd. Daarnaast groeit de behoefte aan data voor het sturen van beleid gestaag. Het is dan ook van cruciaal belang om een duidelijke strategische koers te bepalen voor de uitdagingen op het gebied van compliance.

De gemeente Heerlen heeft aangegeven te streven naar naleving van wet- en regelgeving en naar het herstel van het vertrouwen van burgers in de overheid. De jaarrapportage geeft een beeld van waar we nu staan en in de onderliggende documenten Borgingsproduct 3.0 Toetsingskader en Documentatie zijn de normen waaraan moete worden voldaan nader uitgewerkt. Er is verbetering waarneembaar maar er is nog een lange weg te gaan voordat we überhaupt voldoen aan de huidige geldende normeringen.

4.3. Deel 2. Aanbevelingen en vooruitkijken naar 2024

4.3.1. Beleid

Herziening en actualisering van privacybeleid: Het is essentieel dat het privacybeleid van de gemeente Heerlen wordt herzien en bijgewerkt om te voldoen aan alle relevante wet- en regelgeving, inclusief de AVG, Uitvoeringswet AVG (UAVG), Gemeentewet, Jeugdwet, Wmo 2015, Politiewet 2012 en de Wpg. Deze herziening moet ook de implementatie van het beleid in werkprocessen binnen verschillende afdelingen waarborgen.

Verbetering van documentbeheer: Beleidsdocumenten moeten centraal worden opgeslagen met een adequaat versiebeheer, om te zorgen voor transparantie en om te voorkomen dat verouderde of niet-officiële beleidsstukken worden gebruikt. Het is belangrijk om een gestructureerde aanpak te hanteren om de toegang tot en het gebruik van actuele beleidsdocumenten te vergemakkelijken voor alle afdelingen.

Duidelijke definities van verantwoordelijkheden: Het is van cruciaal belang om de verantwoordelijkheden van het management met betrekking tot privacy(beleid) duidelijk te definiëren en te formaliseren. Dit omvat ook het betrekken van verwerkersverantwoordelijken bij privacy- en informatiebeveiligingsvraagstukken en het instellen van een duidelijke overlegstructuur en voortgangsrapportages om deze verantwoordelijkheden te ondersteunen.

Verbetering van de privacyverklaring: De privacyverklaring gericht op medewerkers en inwoners van de gemeente Heerlen moet worden herzien en bijgewerkt om te zorgen voor volledige transparantie en naleving van wettelijke bepalingen. Hierbij moet duidelijk worden vastgelegd welke persoonsgegevens worden verwerkt, voor welke doeleinden, en hoe betrokkenen hun rechten kunnen uitoefenen.

Door deze stappen te nemen, kan de gemeente Heerlen haar privacybeleid verbeteren en ervoor zorgen dat zij voldoet aan alle relevante wet- en regelgeving op het gebied van privacy en gegevensbescherming. Dit zal niet alleen zorgen voor transparantie en naleving, maar ook het vertrouwen van medewerkers en bewoners in de gemeente vergroten.

4.3.2. Processen

Versterking van procesbeschrijvingen: Het is van cruciaal belang om de werkprocessen waarin persoonsgegevens worden verwerkt adequaat te beschrijven. Dit omvat het toetsen en inrichten van processen volgens de beginselen van behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Door deze beginselen centraal te stellen bij het ontwikkelen en implementeren van processen, kan de gemeente Heerlen voldoen aan de eisen van de AVG en andere wetgevingen.

Stimuleren van betrokkenheid en naleving: Het is belangrijk om actief te sturen op de ontwikkeling van processen binnen de verschillende afdelingen. Dit kan worden bereikt door betrokkenheid te stimuleren en duidelijke richtlijnen en deadlines vast te stellen voor het

uitwerken van processen. Het management moet het belang van naleving van wet- en regelgeving benadrukken en de noodzaak van het adequaat beschrijven van processen communiceren naar alle betrokkenen.

Gebruik van tools en systemen: De gemeente Heerlen maakt gebruik van de applicatie Engage om processen per afdeling verder uit te werken. Het is echter belangrijk om ervoor te zorgen dat deze inspanningen niet vrijblijvend zijn en dat er een duidelijk plan van aanpak is om alle processen adequaat te beschrijven. Bovendien moet worden overwogen om deze processen te koppelen aan INavigator, dat fungeert als verwerkingsregister. Dit zal helpen bij het versnellen van de afhandeling van alle casussen en het bieden van meer inzicht in gegevensverwerkingen binnen de gemeente.

4.3.3. Organisatorische inbedding

Versterking van het privacyteam: Gezien de belangrijke rol van het privacyteam en de huidige onderbezetting, is het cruciaal om het team te versterken. Door het aanstellen van extra personeel kan de dagelijkse problematiek beter worden beheerd en kan er meer aandacht worden besteed aan taken die gekoppeld zijn aan verdere professionalisering, zoals bewustwordingscampagnes en het ontwikkelen van een privacyverklaring.

Heldere toewijzing van taken en verantwoordelijkheden: Het ontbreken van een heldere toewijzing van taken en verantwoordelijkheden remt de verdere professionalisering en naleving van wet- en regelgeving. Het is van essentieel belang om officieel taken en verantwoordelijkheden toe te wijzen binnen de organisatie, met name met betrekking tot privacy en gegevensbescherming. Dit zal het bewustzijn op alle niveaus bevorderen en ervoor zorgen dat alle medewerkers bekend zijn met de principes van de AVG en de Wpg.

Verbetering van bewustwording: De bewustwording binnen de gemeentelijke organisatie kan worden vergroot door middel van bewustwordingssessies, campagnes en ondersteuning door middel van softwarepakketten. Het is belangrijk om alle medewerkers op te leiden en hen bewust te maken van het belang van privacy en gegevensbescherming. Dit zal bijdragen aan een cultuur waarin privacy hoog in het vaandel staat en naleving van wet- en regelgeving de norm is.

Optimalisatie van processen: Het aanpassen van processen binnen de afdeling Informatiemanagement en het opzetten van een portfoliomanagementproces zijn positieve stappen om meer controle te krijgen over gegevensverwerkingen, inclusief die waarbij persoonsgegevens worden verwerkt. Het is belangrijk om deze initiatieven voort te zetten en te blijven streven naar verbetering en optimalisatie van processen om te voldoen aan de AVG en andere relevante wet- en regelgevingen.

4.3.4. Rechten van betrokkenen

Privacyverklaring updaten: Het is van cruciaal belang dat de gemeente Heerlen haar privacyverklaring bijwerkt en ervoor zorgt dat deze voldoet aan de vereisten van de AVG. Dit omvat het verstrekken van duidelijke informatie over welke persoonsgegevens worden verwerkt, voor welke doeleinden, de identiteit en contactgegevens van de verantwoordelijke

voor gegevensverwerking, de contactgegevens van de FG, de doeleinden van de verwerking en de bewaartermijn van de gegevens.

Afhandeling van verzoeken van betrokkenen: Het privacyteam moet de verzoeken van betrokkenen grondig en tijdig afhandelen. Dit omvat het wijzen van betrokkenen op hun rechten onder de AVG en ervoor zorgen dat zij deze rechten kunnen uitoefenen. Het is belangrijk om voldoende middelen en ondersteuning te bieden aan het privacyteam en andere betrokken afdelingen om een efficiënte afhandeling van deze verzoeken te garanderen.

Verbetering van gegevensbeheerprocessen: Het is noodzakelijk om de gegevensbeheerprocessen binnen de gemeente Heerlen te verbeteren. Dit omvat het in kaart brengen van alle gegevensverwerkingen, het waarborgen van naleving van bewaartermijnen, het documenteren van de opslagmethoden en het vermijden van het gebruik van ongeschikte platforms zoals Microsoft Outlook mail als een databasemethode.

Prioriteit geven aan het verwerkingsregister INavigator: Het verwerkingsregister INavigator moet prioriteit krijgen, en alle relevante processen moeten correct worden beschreven en gekoppeld aan dit register. Dit zal helpen om een overzicht te krijgen van alle gegevensverwerkingen binnen de gemeente Heerlen en zal bijdragen aan een betere naleving van de AVG.

4.3.5. Samenwerking

Prioriteren van DPIA's: Gezien het belang van DPIA's voor het identificeren en beoordelen van privacyrisico's, is het essentieel om deze analyses prioriteit te geven. Het is raadzaam om een proces op te zetten om de meest kritieke samenwerkingsverbanden en verwerkingen van persoonsgegevens te identificeren, zodat DPIA's gericht kunnen worden uitgevoerd waar ze het meest nodig zijn.

Beschikbaar stellen van extra middelen: Het team dat belast is met het opstellen van DPIA's, convenanten en verwerkersovereenkomsten heeft mogelijk extra middelen nodig om aan de eisen te voldoen. Dit kan inhouden het toewijzen van meer personeel, het investeren in training en ontwikkeling, of het gebruik van externe expertise om de werklast te verlichten.

Herziening van bestaande verwerkingen: Hoewel het ontbreekt aan beschikbare tijd, is het van groot belang om prioriteit te geven aan het opstellen van DPIA's voor bestaande verwerkingen van persoonsgegevens. Het identificeren en beoordelen van privacyrisico's in deze verwerkingen is noodzakelijk om te voldoen aan de AVG en om mogelijke kwetsbaarheden aan te pakken.

4.3.6. Gegevensbescherming

Prioriteiten stellen: Gezien de toenemende complexiteit en de eisen van de AVG en de BIO, is het essentieel om prioriteiten te stellen. Identificeer kritieke gebieden waar verbeteringen dringend nodig zijn en richt daar eerst de aandacht op.

Toewijzing van middelen: Zorg voor voldoende personeel en middelen om de achterstand weg te werken en te voldoen aan nieuwe ontwikkelingen. Dit kan inhouden dat er extra personeel wordt aangetrokken of dat bestaand personeel wordt vrijgemaakt van andere taken.

Efficiëntie verbeteren: Evalueer de efficiëntie van de huidige processen en procedures voor informatiebeveiliging. Identificeer mogelijke knelpunten en zoek naar manieren om deze te verbeteren, bijvoorbeeld door automatisering van bepaalde taken of het stroomlijnen van processen.

Training en bewustwording: Investeer in training en bewustwording van medewerkers op het gebied van informatiebeveiliging. Zorg ervoor dat alle medewerkers op de hoogte zijn van de vereisten en procedures met betrekking tot gegevensbescherming, zodat ze effectief kunnen bijdragen aan het naleven van de normen.

Continue monitoring en rapportage: Zet een systeem op voor continue monitoring en rapportage van incidenten, nalevingsniveaus en verbeteringen op het gebied van informatiebeveiliging. Op deze manier kan proactief worden gereageerd op eventuele problemen en kan de voortgang worden bijgehouden.

4.3.7. Verantwoording

Implementeer periodieke evaluaties van de naleving van de AVG: Het is essentieel om periodieke evaluaties uit te voeren waarin de naleving van de AVG bij de uitvoering van taken wordt beoordeeld. Dit helpt om mogelijke tekortkomingen te identificeren en corrigerende maatregelen te nemen.

Versterk de rol van de FG: Zorg ervoor dat de FG voldoende middelen en bevoegdheden heeft om als effectieve toezichthouder op te treden en de naleving van de AVG te controleren. Stimuleer actieve controles en opvolging van geconstateerde afwijkingen.

Verbeter het informatiebeveiligingsbeleid: Stel een gedegen informatiebeveiligingsbeleid op en implementeer dit binnen de organisatie. Zorg ervoor dat dit beleid periodiek wordt beoordeeld en geëvalueerd, en dat naleving van processen, procedures en standaarden regelmatig wordt gecontroleerd.

Voer regelmatige controles uit op informatiesystemen: Zorg ervoor dat informatiesystemen jaarlijks worden gecontroleerd op technische naleving van beveiligingsnormen en risico's met betrekking tot de feitelijke veiligheid. Gebruik hiervoor bijvoorbeeld (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.

Verbeter de rapportage aan het management en het bestuursorgaan: Zorg ervoor dat het management en het bestuursorgaan regelmatig worden geïnformeerd over de naleving van de AVG door de organisatie via een jaarverslag. Dit verschaft inzicht in de stand van zaken en stimuleert verantwoording en transparantie.

4.3.8. Conclusies

Eerder genoemde adviezen geven een totaalbeeld van de te nemen maatregelen om als gemeente Heerlen meer controle te verkrijgen over de verplichtingen die voortvloeien uit de AVG en de Wpg.

5. Deel B: Wpg

5.1. Inleiding

De FG ziet erop toe dat de Wpg wordt nageleefd. Het college dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van politiegegevens. De FG rapporteert jaarlijks de bevindingen aan de hand van een jaarverslag. In dit jaarverslag staat beschreven welke acties en maatregelen in 2023 zijn genomen om de doelstellingen en beginselen uit de Wpg te behalen en te waarborgen.

5.2. WPG-dashboard

Thema:	2019	2023	2024
Borging WPG	**Jaarverslag**	**Resultaat**	**Verwacht**
Beleid			
Bewustwording			
Autorisatieproces			
Bewaartermijnen			
Verstrekken van persoonsgegevens			
DPIA			
Register van verwerkingen			
Auditverplichting			

Legenda:

- AANDACHT VEREIST VAN MANAGEMENT
- IN TE HALEN ACHTERSTAND
- OP SCHEMA

5.3. Taak van de FG

De taken van de FG (artikel 36 van de Wpg) aangaande de Wpg kunnen als volgt worden samengevat:
De FG voert periodiek controles uit op het naleven van de wettelijke verplichtingen die voortkomen uit de Wpg, waaronder de controle op:

1. Het hebben van een beleid aangaande de uitvoering van de Wpg;
2. De bewustwordingsverplichting;
3. Het autorisatieproces met betrekking tot het vastleggen van politiegegevens;
4. De kwaliteit en waarborging van de juistheid van de nauwkeurigheid van politiegegevens;
5. Het verwerken van politiegegevens;
6. De bewaartermijnen;
7. Het ter beschikking stellen en verstrekken van politiegegevens;
8. De controle op de informatiebeveiliging en de controle op het uitvoeren van een risicoanalyse;
9. Het register voor verwerkingen;
10. De verplichtingen ten aanzien van de audit.

5.4. Bevindingen 2023

In het afgelopen jaar heeft onze security officer zich ingespannen om de verplichtingen van de Wpg in kaart te brengen en een initiële stap gezet om verbeteringen te realiseren. Hoewel de FG betrokken was, bleek deze inzet onvoldoende om aanzienlijke voortgang te boeken. Door de hoge werkdruk binnen het privacyteam, problemen met betrekking tot informatiebeveiliging en personeelstekorten, is er geen verdere vooruitgang geboekt bij het uitwerken van de Wpg-verplichtingen. Alle aandacht is gegaan naar de AVG.

Er is in 2023 wel een audit afgenomen waarbij de auditor heeft geconstateerd dat er over het algemeen onvoldoende zicht is waar in de organisatie politiegegevens verwerkt worden. Politiegegevens worden veelal binnen, maar ook buiten de “Wpg-proof” informatiesystemen verwerkt zoals in netwerkmappen, e-mail en whatsapp.
Medewerkers zijn betrokken, echter missen zij handvatten om conform de wetgeving te kunnen handelen. In veel gevallen ontbreken vastlegging in beleid, procedures, richtlijnen en werkinstructies. Binnen de afdelingen is de bewustwording en het kennisniveau van de wet en regelgeving onvoldoende.

Vanwege het feit dat er onvoldoende procedures/beleid/werkinstructies zijn wordt vaak géén vastlegging gemaakt over hoe en waarom op een bepaalde manier gewerkt wordt. Hier moet verandering in komen door éérst een basis kennis en bewustwording te implementeren bij de betrokken én verantwoordelijke teams.

5.5. Audit Wpg

De audit heeft zich gericht op domein 1 en 3 en op de 17 verwerkingen die volgens INavigator worden verricht binnen de gemeente Heerlen waarop de Wpg van toepassing is. Deze verwerkingen vinden plaats in onderstaande domeinen. Het domein 5 is in het geheel

niet meegenomen in de audit en is er nog geen goed beeld van de verwerkingen die daar plaatsvinden.

Domein	Functie	Omschrijving	Veelvoorkomende taken
I Openbare ruimte	Parkeercontroleur APV-controleur Gemeentelijk opsporingsambtenaar Controleur openbare ruimte Tunnelwachter Brandweercommandant	Boa's openbare ruimte hebben een breed pakket aan bevoegdheden om overlast en kleine ergernissen binnen de openbare ruimte aan te pakken.	staande houding opmaken procesverbaal aanhouding en verhoor
III Onderwijs	Leerplichtambtenaar	Boa's onderwijs handhaven de leerplichtwet en alle daaraan gerelateerde wet- en regelgeving. Dit zijn de huidige leerplichtambtenaren.	onderzoek naar mogelijk ongeoorloofd verzuim huisbezoeken gesprekken met betrokkene(n) opmaken procesverbaal
V Werk, inkomen en zorg	Sociaal rechercheur Inspecteur arbeidsomstandigheden Belastinginspecteur	Boa's in dit domein zorgen voor de strafrechtelijke handhaving op het gebied van werk, inkomen, belastingen en sociale zaken. Onder dit domein vallen alle regelingen die gemeenten uitvoeren binnen de sociale zekerheid.	huisbezoek buurtonderzoek verhoor betrokkene(n) opmaken procesverbaal

Er is een auditrapport opgesteld waarin deze bevindingen zijn opgenomen. Hieronder een korte samenvatting van deze bevindingen. Deze bevindingen zijn:

- Onvoldoende zicht op politiegegevens verwerkingen (verwerkingsregister);
- Onvoldoende zicht op systemen waarin politiegegevens verwerkt worden (inventarisatie van systemen);
- Onvoldoende beleid/procedures/werkinstructies/richtlijnen m.b.t. de Wpg;
- Onvoldoende controle op:

- Doelbinding van politiegegevens (met welke doel worden gegevens gebruikt) ○ noodzakelijkheid & rechtmatigheid (de noodzakelijkheid van om de gegevens te gebruiken en de manier waarop de gegevens verkregen zijn);
- juistheid en volledigheid (van de gegevens); ○ uitvoering rectificatie/verwijdering van politiegegevens; ○ Logging van politiegegevens (enkel voor domein 1); ○ Politiegegevens worden gebruikt voor taken waarbij er geen noodzaak blijkt te bestaan.

- Onvoldoende (periodieke) controles op de doeltreffendheid van organisatorische- en technische maatregelen;
- Onvoldoende bewerkstelling op “privacy by default” in informatiesystemen en administratieve processen;
- Onvoldoende uitvoering van DPIA’s op hoge risico verwerkingen;
- Onvoldoende toegangsbeheersprocedures tot politiegegevens verwerkende systemen.
- “niet Wpg gecertificeerde” systemen dienen niet meer gebruikt te worden door de organisatie. Indien dit niet mogelijk is dient er onderscheid gemaakt te worden tussen AVG en WPG gegevens, niet Boa’s géén toegang verlenen en handmatig Wpg gegevens verwijderen zodra het bewaartermijn verstreken is;
- Géén procedures en werkinstructies m.b.t. Bewaartermijnen richtlijnen;
- Politiegegevens worden soms buiten de BOA applicaties opgeslagen (waaronder netwerkschijven, e-mail en whatsapp)
- Onvoldoende inrichting op rechten van betrokkenen m.b.t. politiegegevens;
- De FG heeft onvoldoende toezicht uitgevoerd op:
  - Het naleven van de Wpg; ○ Het beleid van verwerkingsverantwoordelijke m.b.t. de bescherming van persoonsgegevens;
  - De toewijzing van de autorisaties zoals bedoelt in artikel 6 van de Wpg; ○ Bewustmaking en opleiding van de Boa’s en andere functionarissen die betrokken zijn bij de verwerking van politiegegevens;
  - (interne) audits; ○ Uitvoering van DPIA’s (op het gebied van bestaan).

5.6. Vooruitblik jaar 2024

Het beeld van informatiebeveiliging en privacy binnen de AVG en Wpg voor 2024 is dat het een voortdurende uitdaging blijft voor organisaties, waaronder gemeenten zoals die van Heerlen. De steeds nieuwe technologieën en het groeiende belang van gegevens maken het noodzakelijk om voortdurend de beveiligingsmaatregelen aan te scherpen en te voldoen aan nieuwe wet- en regelgeving, zoals de AI-verordening en NIS2-richtlijn[4].

In 2024 zal er waarschijnlijk een grotere nadruk liggen op proactieve benaderingen van informatiebeveiliging en privacy, waarbij organisaties meer investeren in preventieve maatregelen, bewustmakingsprogramma's voor medewerkers en continue monitoring van

[4] Verordening is een wet die van toepassing is op alle EU-lidstaten. Ze zijn onderdeel van de nationale wetgeving en kunnen worden afgedwongen via de nationale rechtbanken van elke lidstaat vanaf het moment dat ze van kracht worden. Richtlijnen zijn EU-wetten die doelen stellen die lidstaten moeten implementeren in nationale wetgeving.

gegevensstromen. Dit zal worden aangevuld met een toenemende vraag naar geavanceerde technologische oplossingen zoals AI-gestuurde beveiligingssystemen en geautomatiseerde compliance-tools.

Bovendien zullen organisaties zoals de gemeente Heerlen meer nadruk moeten leggen op transparantie en verantwoording aan belanghebbenden, inclusief burgers en regelgevende instanties. Dit omvat het regelmatig rapporteren over privacy- en informatiebeveiligingsincidenten, nalevingsstatus en de genomen maatregelen.

Over het algemeen zal het beeld van informatiebeveiliging en privacy voor 2024 gericht zijn op het vinden van een balans tussen het vrijmaken van budgetten, het beschermen van gegevens, het waarborgen van privacy en het faciliteren van innovatie en digitale transformatie.

Om de voortgang te waarborgen, is het nu van cruciaal belang om te zorgen voor voldoende personeel en middelen om de achterstand weg te werken en te voldoen aan de Wpg-verplichtingen. Dit kan betekenen dat extra personeel moet worden aangetrokken of dat bestaand personeel wordt vrijgemaakt van andere taken. Het is van belang om deze kwestie met prioriteit aan te pakken om de naleving van de Wpg en de veiligheid van politiegegevens te waarborgen.

6. Deel C: Ontwikkelingen

De trends op het gebied van informatiebeveiliging volgens de IBD (Informatiebeveiligingsdienst voor gemeenten) voor 2024 kunnen onder andere de volgende aspecten omvatten:

- Toenemende complexiteit van bedreigingen: De dreigingen op het gebied van cyberbeveiliging worden steeds geavanceerder en complexer. Hackers en kwaadwillenden passen continu hun tactieken aan, waardoor het voor organisaties moeilijker wordt om zich te verdedigen.
- Focus op preventie en proactieve maatregelen: Organisaties zullen meer nadruk leggen op het implementeren van preventieve maatregelen om beveiligingsincidenten te voorkomen. Dit omvat het gebruik van geavanceerde beveiligingsoplossingen, regelmatige security awareness training voor medewerkers en het implementeren van beveiligingsbeleid en -procedures.
- Toename van privacy-gerelateerde wetgeving: Met de groeiende bezorgdheid over privacy en gegevensbescherming zullen er waarschijnlijk meer wetten en voorschriften worden ingevoerd om de privacy van individuen te beschermen. Organisaties zullen zich moeten aanpassen aan deze veranderende regelgevende omgeving en ervoor zorgen dat ze voldoen aan alle relevante voorschriften.
- Adoptie van opkomende technologieën: Technologische ontwikkelingen zoals kunstmatige intelligentie (AI), machine learning, Internet of Things (IoT) en blockchain zullen steeds meer worden geïntegreerd in bedrijfsprocessen. Het is belangrijk dat organisaties deze technologieën op een veilige en verantwoorde manier implementeren om potentiële beveiligingsrisico's te minimaliseren.

- Samenwerking en informatie-uitwisseling: Gezien de toenemende complexiteit van bedreigingen zullen organisaties meer samenwerken en informatie uitwisselen met andere partijen in de sector, zoals overheidsinstanties, cybersecuritybedrijven en brancheorganisaties. Deze samenwerking kan helpen bij het identificeren van nieuwe dreigingen en het delen van best practices op het gebied van beveiliging.

Door rekening te houden met deze trends en zich proactief aan te passen aan de veranderende beveiligingsomgeving, kan de gemeente Heerlen beter voorbereid zijn om cyberdreigingen het hoofd te bieden en de gegevens van hun burgers effectief te beschermen.

Bijlagen

Bijlage 1 - Stand van zaken AVG per thema
Bijlage 1.1 Borgingsproduct 3.0 Toetsingskader
Bijlage 1.2 Borgingsproduct 3.0 Documentatie
Bijlage 2 – Kengetallen AVG

Bijlage 1 - Stand van zaken AVG per thema

Zie bijlage 1.1 Borgingsproduct 3.0 Toetsingskader
Zie bijlage 1.2 Borgingsproduct 3.0 Documentatie

Beleidsstukken

Omschrijving	Datum inwerkingtreding	Opmerking 2024
Privacybeleid	23 juni 2020	Driejaarlijkse controle niet uitgevoerd.
Privacyreglement	23 juni 2020	Driejaarlijkse controle niet uitgevoerd.
Intern privacybeleid	23 juni 2020	Driejaarlijkse controle niet uitgevoerd.
Gedragscode voor de publicatie van persoonsgegevens door de raad	27 mei 2020	Driejaarlijkse controle niet uitgevoerd.
Informatiebeveiligingsbeleid Suwinet	12 oktober 2020	Jaarlijkse controle niet uitgevoerd.
Informatiebeveiligingsbeheer Suwinet	12 oktober 2020	Jaarlijkse controle niet uitgevoerd.
Informatiebeveiligingsplan Suwinet	12 oktober 2020	Jaarlijkse controle niet uitgevoerd.
Sanctiebeleid bij oneigenlijk gebruik Suwinet	12 oktober 2020	Jaarlijkse controle niet uitgevoerd.

Bijlage 2 Kengetallen

Overzicht (pré)DPIA's

Onderwerp DPIA	Wet	Datum	Status
Aanpak Parkstad Integrale Jeugdaanpak Jeugd preventie platform	AVG UAVG Gemeentewet Jeugdwet WMO 2015 Politiewet 2012 WPG		In behandeling en wachtend op verdere goedkeuring Verwerkersverantwoordelijken
Aanpak Parkstad Lokale Jeugdaanpak	AVG WPG		In behandeling en wachtend op verdere goedkeuring Verwerkersverantwoordelijken
Aanpak Parkstad Kernteamoverleg	AVG WPG		In behandeling en wachtend op verdere goedkeuring Verwerkersverantwoordelijken

Casussen

Aantal	Casus
3	Vragen betreffende beleid en de invulling daarvan binnen de gemeente Heerlen
56	Informatie advies grondslagen van verwerkingen en samenwerkingsvraagstukken
5	Klachten over verwerking van persoonsgegevens
5	Vragen betreffende nieuw te gebruiken systemen - privacy by design
17	Ondersteuning bij projecten
7	Vragen over nieuwe partners en de daaraan te koppelen eisen
34	Incidenten • 23 datalekken ○ 4 intern afgehandeld ○ 19 gemeld aan de Autoriteit Persoonsgegevens, waarvan 10 gemeld aan de Autoriteit Persoonsgegevens én betrokkenen • 11 geregistreerde beveiligingsincidenten
21	Verzoeken op grond van rechten van betrokkenen

Overzicht rechten van betrokkenen

Aantal verzoeken	2021	2022	2023
	12	9	21

INavigator als verwerkingsregister

Kenmerk	Aantal 2023
Totaal aantal (geregistreerde) werkprocessen	**1104**
Niet goedgekeurd	1037
Werkprocessen met persoonsgegevens	**851**
- Basispersoonsgegevens	849
- Burgerservicenummer	668
- Inkomensgegevens	226
- Ras of etnische afkomst	46
- Politieke opvattingen	31
- Religieuze of levensbeschouwelijke overtuiging	24
- Lidmaatschap van een vakbond	13
- Genetische of biometrische eigenschappen	30
- Gezondheid	115
- Seksuele identiteit en oriëntatie	22
- Strafrechtelijke veroordelingen en strafrechtelijke feiten	107
- Gegevens mbt kind(eren)	110
Gebruikte AVG grondslag	**733**
- Wettelijke verplichting	570
- Algemeen belang	125
- Overeenkomst	150
- Toestemming	7
- Vitaal belang	0
- Gerechtvaardigd belang	6
Privacy (risico) classificering	**1104**
- Laag	255
- Midden	602
- Hoog	247