Geldrop-Mierlo

GEMEENTEBLAD

Officiële uitgave van de gemeente Geldrop-Mierlo

Nr. 547606

30 december

2024

Beleidsuitwerking Privacy organisatie

Dit document beschrijft de privacy organisatie die de gemeente Geldrop-Mierlo (hierna "de gemeente") heeft ingericht. De verschillende rollen, taken en verantwoordelijkheden. En het benoemt de relatie tot lijnmanagement en bestuur: die zijn de eigenaar van de bedrijfsprocessen (met bijbehorende informatieprocessen of (informatie)systemen) de daaraan verbonden verantwoordelijkheden op gebied van privacy, inclusief privacy afspraken met externe partijen.

1. Inleiding

Dit document is een nadere uitwerking van de Privacy organisatie (hoofdstuk 3) uit de beleidsuitwerking privacy van de gemeente. Het gaat nader in op de organisatie inrichting voor de Algemene verordening Gegevensbescherming (AVG) en voor de Wet politie gegevens (Wpg).
De Wpg is van toepassing op de verwerkingen van persoonsgegevens in taken van de gemeente die gaan over de voorkoming, opsporing of vervolging van strafbare feiten, en die onze Buitengewoon Opsporing Ambtenaren (BOA's) uitvoeren.

1.1. Leeswijzer

In hoofdstuk 1 komen de definities, verplichtingen, uitgangspunten en rollen aan de orde.

In hoofdstuk 2 staan de diverse rollen inclusief de taken, verantwoordelijkheden en bevoegdheden uitgeschreven.

In hoofdstuk 3 staan de diverse overlegstructuren beschreven.

Om het document compact te houden, zijn aanvullende (detail) informatie en formulieren als link of bijlage opgenomen. Ook omdat deze documenten mogelijk aan wijziging onderhevig kunnen zijn.

1.2. Definities

De meest gebruikte definities en afkortingen treft u aan in het document "Definities en afkortingen AVG Wpg". Hieronder wordt ingegaan op de voor dit document belangrijke en specifieke definities.

Bestuurlijk verantwoordelijk: het College van B&W. Voor de taken gemandateerd aan de Gemeenschappelijke Regeling Dienst Dommelvallei (DD) is het Dagelijks Bestuur Dienst Dommelvallei (DB DD) verantwoordelijk.

Gemeentesecretaris/directeur DD: de gemeentesecretaris/ directeur DD is (ambtelijk verantwoordelijk voor privacy volgens mandaat van het organisatiebestuur.

Lijnmanagement: gemeentesecretaris (GS), concern management team (CMT) en teammanager(s) ambtelijk verantwoordelijk voor een organisatieonderdeel.

Medewerker: een medewerker in dienst van de gemeente of een persoon die werkzaamheden uitvoert in opdracht van de gemeente (bijv. inhuurkrachten, stagiaires, externe medewerkers, etc.).

Autoriteit Persoonsgegevens (AP): de Nederlandse gegevensbeschermingsautoriteit die toezicht houdt op de naleving van de privacyregels in Nederland.

1.3. Verplichtingen

Zonder een adequaat ingerichte privacy organisatie en een duidelijke indeling in functies, rollen, verantwoordelijkheden en bevoegdheden, kan niet worden voldaan aan de voorwaarden die de Algemene Verordening Gegevensbescherming (AVG) en Wpg.
Daarnaast is het belangrijk dat de functionarissen betrokken zijn en goed opgeleid, zodat ze ondersteunend zijn aan de strategische doelen van de gemeente en de beleidsuitwerking privacy.

1.4. Uitgangspunten

Voldoen aan de wet en de gevolgen en risico's voor de verwerking van persoonsgegevens voor betrokkene(n) tot een minimum en acceptabel niveau beperken.

De privacy organisatie werkt vanuit de gemeentelijke missie, visie, kernwaarden en de beleidsuitwerking privacy.

Iedere privacy rol heeft eigen taken, verantwoordelijkheden en bevoegdheden. Deze moeten voor iedereen duidelijk zijn. De privacy rollen vullen elkaar aan.

We richten de organisatie in op een efficiënte manier:
- De lijn is verantwoordelijk;
- De Privacy Officer geeft richting, advies en ondersteuning aan de lijn;
- De Functionaris Gegevensbescherming is toezichthouder, geeft zwaarwegend advies.

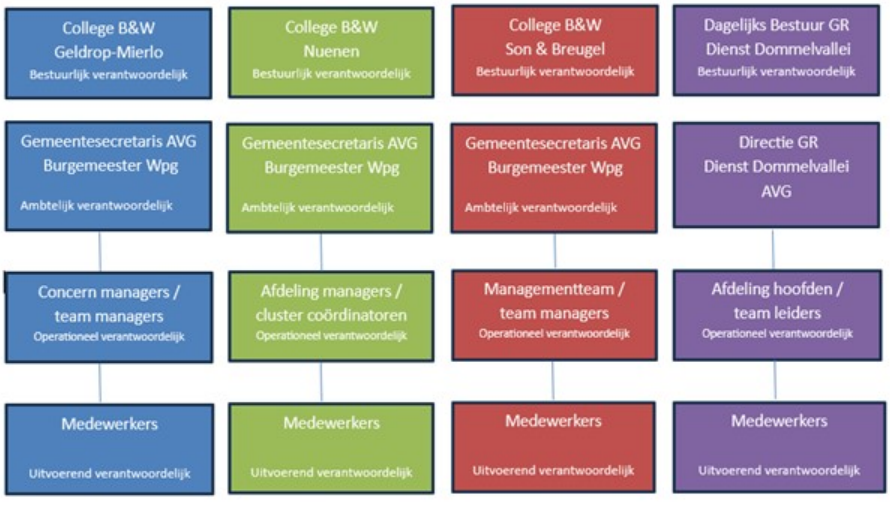
2. Rollen en verantwoordelijkheden

De bestuursorganen van de organisaties zijn verantwoordelijk voor de naleving van de AVG en de beleidsuitwerking privacy, ieder voor zover het hun bestuurlijke taken betreft.
Zij zijn verantwoordelijk voor het verwerken van persoonsgegevens door de eigen gemeente en door externe, gemandateerde organisaties, waaronder DD.

	Verantwoordelijk	
R	Responsible/ Ambtelijk verantwoordelijk Feitelijk verantwoordelijk	• Gemeentesecretaris, Concern manager / Teammanagers Bij mandaat: Dagelijks Bestuur DD • De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken • De bevoegd functionaris Wpg
A	Accountable/ Bestuurlijk Eindverantwoordelijk	• Het college van B&W (voor de AVG) • De burgemeester (voor de Wpg)
C	Consulted/ Adviserend	• Privacy Officer voor privacy • Chief Information Security Officer voor informatiebeveiliging • Functionaris Gegevensbescherming voor privacy
I	Informed/ Geïnformeerd	• Gemeenteraad (privacy rechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatie-wetgeving een bestuurlijke toezichttaak) Bij mandaat: Algemeen Bestuur DD • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)

Tabel 1: RACI

De lijnverantwoordelijkheid ziet er voor de betreffende DD-organisaties als volgt uit:



Figuur 1: Verantwoordelijke lijnorganisatie

De Privacy Officers van de gemeente (die sturing, advies en ondersteuning aan de lijn geven) zitten in het team Juridische Zaken.

De gemeente is als overheidsorganisatie en verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens en heeft conform de wettelijke verplichting een Functionaris Gegevensbescherming aangesteld voor de AVG en de Wpg. De gemeente heeft deze rol en de verantwoordelijkheid voor informatiebeveiliging (Chief Information Security Officer/Eenduidig Normatiek Single Information Audit) gemandateerd aan DD.

Voor de aan de DD gemandateerde taken geldt dat de Privacy Officer van DD sturing, advies en ondersteuning geeft aan de teams binnen DD, en dit afstemt met de Privacy Officers van de gemeente wiens betrokkenen het betreft.

Figuur 2: Verantwoordelijkheden privacy organisatie

De Wpg kent de volgende rollen die voorkomen bij de teams waar BOA's werkzaam zijn, dus de teams Leefbaarheid en Veiligheid en Jeugd & Zorg.

Figuur 3: Verantwoordelijkheden Wpg

In volgende paragrafen gaan we per rol gedetailleerd in op de taken en verantwoordelijkheden. Zie bijlage 1 voor een schematische voorbeeld.

2.1. Gemeenteraad (Informed)

De gemeenteraad wordt geïnformeerd over de privacy ontwikkelingen binnen de gemeente, omdat zij een bestuurlijke toezichttaak heeft op basis van de Gemeentewet en decentralisatiewetgeving.

2.2. College van B&W resp. Burgemeester (Accountable, Verwerkingsverantwoordelijk)
Het College is als eigenaar eindverantwoordelijk voor de aantoonbare naleving van de privacywetgeving binnen de gemeente.
De Burgemeester is verantwoordelijk voor de aantoonbare naleving van de Wpg. De Wpg is van toepassing op de verwerkingen van persoonsgegevens met betrekking tot de voorkoming, opsporing of vervolging van strafbare feiten.

Het College resp. de burgemeester heeft de volgende rollen en verantwoordelijkheden:
- Bestuurlijk eindverantwoordelijk voor de naleving van de privacywetgeving resp. Wet politie gegevens binnen de gemeente;
  - Binnen het College is de portefeuillehouder privacy belegd bij de Burgemeester;
  - Het College heeft de verantwoordelijkheid op gebied van privacy gemandateerd aan de gemeentesecretaris;

- Aanstellen van een FG, die toeziet op de naleving van de AVG en de Wpg;
- Vaststellen van de beleidsuitwerking privacy (AVG en Wpg);
- Sturing geven aan de uitvoering van de beleidsuitwerking privacy;
- Stimuleren van het management om passende technische en organisatorische privacy - en Wpg-maatregelen te nemen;
- Bevorderen van een duurzame privacy cultuur;
- Evalueren van de toepassing en werking van de beleidsuitwerking privacy, op basis van de FG-rapportage AVG en Wpg;
- Beslissingsbevoegdheid ten aanzien van het wel of niet (geheel) opvolgen van (schriftelijk) advies van FG;
  - Het College licht de FG schriftelijk en onderbouwt in over het genomen besluit, waarbij met name besluiten om het advies van de FG niet (geheel) op te volgen worden voorzien van alle relevante argumenten, die tot het besluit hebben geleid;
  - Het College informeert de FG tijdig over en betrekt de FG bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens en politiegegevens;

- In overleg met de Portefeuillehouder jaarlijks informeren van de gemeenteraad over de risico's en over de getroffen beheersmaatregelen op het gebied van privacy en Wpg, op basis van de resultaten van externe audits en de FG-jaarrapportage (bijvoorbeeld via de planning & control cyclus);
- Melden van bijzonderheden ten aanzien van privacy en Wpg aan de gemeenteraad.

2.3. Gemeentesecretaris en concern managers (Responsible, Verwerkingsverantwoordelijke)
De gemandateerde verantwoordelijkheid voor privacy ligt bij de gemeentesecretaris. Deze stelt met het concern management team het gewenste niveau van privacy volwassenheid vast voor gemeente.

Het concern management team en de teammanagers zijn als proceseigenaren ambtelijk eindverantwoordelijk voor de AVG.

De gemeentesecretaris is eindverantwoordelijk voor de uitvoering van uit de beleidsuitwerking privacy en de naleving van de privacywetgeving. Deze verantwoordelijkheid kan, indien gewenst, per onderdeel toegewezen worden aan een van de concern managers. De Wpg is belegd bij de concernmanager Lijn. Voor de aan de DD gemandateerde taken is de directeur DD proceseigenaar. DD voert geen Wpg taken uit voor de gemeente.

Tot de taken en verantwoordelijkheden van de gemeentesecretaris, die niet te delegeren zijn, behoren in ieder geval:
- De eindverantwoordelijkheid voor de gemeente brede verantwoording van de implementatie en uitvoering van de beleidsuitwerking privacy aan het College;
- Het waarborgen van de onafhankelijke positie van de FG.
  Door de positionering ervan op een onafhankelijke adviserende en toezichthoudende positie binnen de organisatie (binnen de DD) en door ervoor zorg te dragen dat voor de uitoefening van de FG-functie geen aanwijzingen of instructies worden gegeven;
- Het -samen met de burgemeester- beslissen over wel/niet melden van een datalek aan de Autoriteit Persoonsgegevens.

Tot de taken en verantwoordelijkheden van de gemeentesecretaris, die eventueel wel overgedragen kunnen worden naar concernmanagers, teammanagers of proceseigenaren, behoren in ieder geval binnen zijn/haar organisatieonderdeel:

- De eindverantwoordelijkheid voor de implementatie en uitvoering van uit de beleidsuitwerking privacy en de naleving van de privacywetgeving incl. het zichtbaar sturen en monitoren, binnen zijn/haar organisatieonderdeel en het zorgen voor afdoende middelen;
- De eindverantwoordelijke stelt voldoende middelen aan de FG ter beschikking om het toezicht op de naleving van de beleidsuitwerking privacy adequaat uit te kunnen voeren;
- De verantwoordelijkheid dat de personen die bij verwerkingen van persoonsgegevens zijn betrokken desgevraagd aan de FG alle inlichtingen verstrekken en overige medewerking verlenen die voor de uitoefening van de FG taak nodig is;
- Het verstrekken aan de FG op welke manier het organisatieonderdeel compliant is aan de privacywetgeving en Wpg;
- De verantwoordelijkheid voor het aanwijzen van een procesverantwoordelijke voor ieder bedrijfsproces/ informatieproces/informatiesysteem/verwerking van persoonsgegevens;
- De verantwoordelijkheid voor het bepalen van een privacy risico classificatie voor ieder bedrijfsproces/ informatieproces/informatiesysteem/verwerking van persoonsgegevens;
- Het tijdig betrekken van de PO en/of FG bij ontwikkelingen van nieuwe of gewijzigde verwerkingen van persoonsgegevens (t.b.v. behoorlijke en zorgvuldige verwerking van persoonsgegevens, risico inschatting, etc.);
- De verantwoordelijkheid voor het doen van een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens(AP) in geval er grote restrisico's over blijven bij de verwerking van persoonsgegevens (bijvoorbeeld na een DPIA);
- De verantwoordelijkheid voor het inzichtelijk maken van de werkprocessen en van de verwerkingen van persoonsgegevens;
- De verantwoordelijkheid voor het laten registreren van de gegevensverwerkingen in het verwerkingsregister en het actueel houden van het verwerkingsregister volgens de geldende procedure;
- De verantwoordelijkheid voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- De verantwoordelijkheid voor monitoring van zorgvuldig verwerken van persoonsgegevens, en bijsturing waar dat nodig is;
- De verantwoordelijkheid voor het opstellen van aanvullende (gedetailleerde) documenten zoals procedures, handreikingen en werkinstructies. In ieder geval ten behoeve van de transparantieplicht, informatieverstrekking aan betrokkenen en de rechten van betrokkenen (als bedoeld in de AVG, hoofdstuk 3 en de Wpg, paragraaf 4);
  Het college kan nadere regels stellen omtrent deze genoemde procedures en hulpmiddelen;
- Het ten minste eenmaal per jaar evalueren van de procedures en hulpmiddelen.
  Vraagt hiervoor het advies van de PO en documenteert wat er met het advies wordt gedaan;
- De verantwoordelijkheid voor de afhandeling van rechten van betrokkenen door de verantwoordelijke concern manager;
- De verantwoordelijkheid voor een duurzame privacy cultuur;
- De verantwoordelijkheid voor privacy bewustwording en privacy kennis bij medewerkers. Bijvoorbeeld door het opnemen van privacy als onderdeel van werkoverleggen (daarmee werkt men actief aan privacy bewustzijn) en het trainen van medewerkers;
- De verantwoordelijkheid om de eisen ten aanzien van gegevensverwerking in contracten of aanvullende privacy overeenkomsten te borgen bij verwerking van persoonsgegevens door een externe partij. Bijvoorbeeld een verwerkersovereenkomst[1] of samenwerkingsovereenkomst[2]. De PO ondersteunt en adviseert proceseigenaren hierbij.
  - o De gemeente hanteert de landelijke vastgestelde modellen van de Vereniging Nederlandse Gemeenten (VNG). In specifieke gevallen kan het college besluiten hiervan af te wijken;

- Als er politiegegevens verwerkt worden:
  a) Wijst voor artikel 9 verwerking een bevoegd functionaris Wpg aan en legt hiervan een register aan;
  b) Het afstemmen met de teammanagers van de Wpg-domeinen;
  c) Het vastleggen van een register voor de aangewezen BOA's;
  d) Het beleggen van de Wpg-interne auditor's rol;
  e) Het jaarlijks laten uitvoeren van een interne Wpg controle;
  f) Het 4-jaarlijks laten uitvoeren van een externe Wpg-audit door een gekwalificeerd extern bureau.

1) in geval van een externe partij die een verwerker is (artikel 28 AVG en/of artikel 6c Wpg)
2) in geval dat de externe partij een verwerkingsverantwoordelijke is (dit kan gezamenlijk of zelfstandig zijn). Ook wel een privacy convenant genoemd.

2.4. Alle medewerkers (responsible)
Alle medewerkers van de gemeente zijn betrokken bij de verwerking van persoonsgegevens en zij zijn daarom ook verantwoordelijk voor het verantwoord omgaan met persoonsgegevens die behoren bij hun taken.
De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat zij de voorschriften van de beleidsuitwerking privacy opvolgen en actief uitdragen.

Tot de taken en verantwoordelijkheden van de medewerkers werken behoren in ieder geval:
- Zich bewust te zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met persoonsgegevens (AVG en Wpg);
- Signaleert bij de manager, als hij/zij meent over onvoldoende privacy kennis te beschikken (om de benodigde kennis op te doen);
- Het respecteren van de rechten van betrokkenen;
- Ervoor zorgt te dragen dat het vertrouwen van betrokkenen in de overheid niet wordt beschaamd;
- Gedrag te vertonen dat past bij goed werknemersschap;
- Ervoor te zorgen dat de kans op financiële - en imagoschade wordt geminimaliseerd, door onder meer het tijdig melden van (mogelijke) datalekken en door (mogelijke) privacy risico's direct kenbaar te maken;
- Te werken volgens de geldende procedures.

Privacy is de verantwoordelijkheid van iedere medewerker!

2.5. Boa's (Responsible)
De gemeente heeft gecertificeerde en aangewezen Buitengewoon Opsporing Ambtenaren (BOA's) aangesteld. De BOA's mogen politiegegevens verwerken conform de Wpg voor de uitvoering van de politietaak. Oftewel ten behoeve van de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. De politiegegevens, die worden opgeslagen, betreffen gegevens over strafbare feiten, overtredingen en misdrijven.

Tot de taken en verantwoordelijkheden van de BOA's in het kader van de Wpg behoren in ieder geval:
- Te zijn gecertificeerd en aangewezen als BOA (akte van opsporingsbevoegdheid);
- Kennis te hebben van het volgende en zich hiernaar te gedragen:
  - De Wpg is niet van toepassing op de verwerking van politiegegevens ten behoeve van activiteiten met uitsluitend persoonlijke doeleinden en ten behoeve van de interne bedrijfsvoering;
  - De Wpg geldt niet voor de verwerking van gegevens bij de uitvoering van de Vreemdelingenwet en de grensbewakingstaak. Hiervoor geldt de AVG;
  - De Wpg is wel van toepassing op de gegevensverwerkingen in het kader van de wet Administratiefrechtelijke handhaving verkeersvoorschriften (verkeersboetes). Deze wet staat ook wel bekend als de wet Mulder (zie artikel 1a);
  - Aanvullende documenten zoals 'het handboek Wpg BOA gemeente Geldrop-Mierlo (voor BOA's Leefbaarheid en Veiligheid) en 'regionale ambtinstructie leerplicht/ Doorstroompunt' (voor BOA's Jeugd) en eventuele privacy convenanten.
- De verantwoordelijkheid voor de registratie van handhavingshandelingen, waarnemingen, waarschuwingen en maatregelen in het gecertificeerd politiesysteem;
- De verantwoordelijkheid voor het labelen van strafrechtelijke politiegegevens, zodat alleen geautoriseerde mensen[3] erbij kunnen;
- De verantwoordelijkheid voor afstemming met de Bevoegd Functionaris in geval van verstrekkingen aan andere teams of externe partijen.

2.6. Bevoegd functionaris Wpg (Responsible)
De gemeente heeft, als werkgever van de buitengewoon opsporingsambtenaar, de [Manager] van de teams, waarin de BOA's werkzaam zijn, vastgesteld als Bevoegd Functionaris Wpg[4]. De Bevoegd Functionaris Wpg is de 'hoeder' van de politiegegevens, die zorg draagt voor de opsporing van strafbare feiten en belast is met de voorbereiding van de eventuele vervolging van deze feiten.

Tot de taken en verantwoordelijkheden van de Bevoegd Functionaris Wpg behoren in ieder geval:
- Ervoor zorg te dragen zelf geen Wpg-taken uit te voeren;

3) niet boa's zoals bijvoorbeeld een administratief medewerker mogen geautoriseerd worden obv Bpg artikel 3
4) Verbeterplan Wpg audit, vastgesteld door MT dd 19-april-2023. Conform Bpg artikel 2:10 lid 2.

- De verantwoordelijkheid voor het hebben van voldoende kennis en vaardigheden van de Wpg en bijbehorende wetgeving;
- De verantwoordelijkheid voor het (tijdig) beschrijven en vastleggen van het doel van de artikel 9-verwerkingen;
- De verantwoordelijkheid voor het autoriseren van personen tot politiegegevens en het verwerken ervan;
- Het bepalen of gegevens voor andere doeleinden mogen worden gebruikt, bijvoorbeeld of politiegegevens voor onderzoek verder verwerkt mogen worden (Wpg artikel 9 lid 3, artikel 11 lid 1 en 4, artikel 13 lid 3) en of ze verstrekt kunnen worden aan een samenwerkingspartner;
- Ervoor te zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen worden vastgelegd (artikel 3, lid 5);
- Te toetsen en bewaken dat gegevens rechtmatig worden verkregen en verwerkt (o.a. aandacht voor bewaartermijnen, doelbinding en dataminimalisatie);
- De verantwoordelijkheid om de concernmanager Lijn te ondersteunen met het beheer van het 'aangewezen bevoegd functionaris' register, met daarin de als bevoegd functionaris aangewezen medewerkers.

2.7. Privacy Officer (Consulted)
De Privacy Officer is het interne aanspreekpunt voor medewerkers van de gemeente voor (praktische invulling van) privacy gerelateerde vraagstukken, heeft een monitorende en ondersteunende functie met betrekking tot het naleven en uitvoeren van de beleidsuitwerking privacy, en is belast met de coördinatie en uitvoering ervan. Daarnaast ondersteunt de Privacy Officer de lijn (support) bij de uitwerking van privacy vraagstukken.

Tot de taken en verantwoordelijkheden van de Privacy Officer behoren in ieder geval:
- Rapporteren en informeren:
  - Informeert en adviseert (proactief) de medewerkers en het college over ontwikkelingen die relevant zijn voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens, en beantwoordt vragen over privacy;
  - Functioneert als interne contactpersoon voor zaken betreffende de verwerking van persoonsgegevens;
  - Communiceert met en rapporteert rechtstreeks aan de verwerkingsverantwoordelijke Gemeentesecretaris en Burgemeester (bijvoorbeeld via PoHo-overleg);
  - Communiceert met en rapporteert aan de concernmanager Lijn over de Wpg en over zaken en risico's die de dienstverlening van DD betreffen;
  - Communiceert met en informeert zo nodig de FG over privacy gerelateerde zaken;
  - Legt verantwoording af ten aanzien van privacy processen in zijn/haar beheer, in het kader van de planning en control cyclus.

- Beleid uitwerken, plannen opstellen en evalueren:
  - Stelt op, beheert, evalueert en monitort de beleidsuitwerking privacy, procedures, formats en standaard overeenkomsten, zoals de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
  - Stelt op, beheert, evalueert en monitort privacy - en Wpg ((meer)jaren)plannen.

- Coördineren:
  - Is het eerste aanspreekpunt voor privacy gerelateerde onderwerpen binnen de organisatie;
  - Coördineert de uitvoering van privacy en Wpg (meer)jaarplannen.
  - Coördineert en assisteert (wanneer nodig) bij de afhandeling van verzoeken in het kader van de rechten van de betrokkene, zoals bij domein overstijgende rechtenverzoeken;
  - Coördineert de uitvoering van data protection impact assessments (DPIA's);
  - Coördineert, ondersteunt en faciliteert de verwerkingsverantwoordelijke bij het afhandelen van datalekken (conform geldende procedure);
  - Bewaakt en borgt de rechten van betrokkenen en de uitvoering van procedures die hiermee verband houden;
  - Onderhoudt een overlegstructuur (zie hoofdstuk 3).

- Adviseren:
  - Adviseert het bestuur en de ambtelijke organisatie over privacy ontwikkelingen en de toepassing van privacy gerelateerde wet- en regelgeving;
  - Adviseert en ondersteunt de verwerkingsverantwoordelijke ten aanzien van het opstellen, naleven en uitvoeren (implementeren) van de beleidsuitwerking privacy;
  - Adviseert bij specifieke privacy gerelateerde reglementen, beleid, procedures en werkinstructies en over de positionering van privacy in werkprocessen;

- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen en de wijziging of uitbreiding van bestaande systemen;
- Adviseert over de rechtmatigheid van verwerkingen, bijv. over de verwerkingsgrondslag, doelbinding, subsidiariteit en proportionaliteit;
- Adviseert over privacy gerelateerde zaken, zoals bewustwording, opleiding van management en medewerkers en over communicatie naar betrokkenen;
- Adviseert over af te sluiten verwerkersovereenkomsten en overeenkomsten voor gegevensdeling met derden (o.a. convenanten);
- Adviseert over mechanismen voor uitwisseling van persoonsgegevens met landen buiten de Europese Economische Ruimte (EER) en met internationale organisaties;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van DPIA's en over de maatregelen om de daaruit naar voren komende risico's te beperken tot een acceptabel niveau;
- Adviseert over te nemen technische en organisatorische maatregelen, onder andere naar aanleiding van datalekken;
- Adviseert over en assisteert bij de registratie van verwerkingen in het verwerkingsregister.

- Uitvoeren:
  - Behandelt datalekmeldingen (conform geldende procedure), waaronder de registratie van datalekken in het datalekkenregister en het melden van datalekken bij de Autoriteit Persoonsgegevens en de betrokkenen (AVG artikel 33, en Wpg artikel 4c);
  - Beheert het datalekkenregister;
  - Beheert het verwerkingsregister (AVG art. 30);
  - Controleert het verwerkingsregister op juridische juistheid en volledigheid;
  - Ondersteunt bij de uitvoering van risicoclassificaties en risicoanalyses (DPIA's);
  - Registreert risico's in het risicoregister;
  - Participeert in projectgroepen;
  - Adviseert ten aanzien van bewustmakingsprogramma's- en privacy trainingen voor medewerkers;
  - Geeft introductietraining privacy aan nieuwe medewerkers, organiseert privacy bewustwordingsactiviteiten, sluit ad-hoc aan bij team overleggen;
  - Plaatst en beheert privacy nieuwsberichten op de daarvoor beschikbare gremia, zoals het intranet van de gemeente;
  - Volgt de (maatschappelijke) ontwikkelingen, inzichten, wet- en regelgeving en jurisprudentie met betrekking tot privacy en vertaalt deze naar toepasbare privacy-waarborgen;
  - Is de contactpersoon voor privacy gerelateerde zaken voor de Informatiebeveiligingsdienst van de VNG (IBD) en voor andere overheidsinstanties. (zoals voor het ontvangen van de Maandmonitor Privacy);
  - Onderhoudt structurele contacten met de Privacy Officers van ketenpartners en regiogemeenten.

Vanuit zijn functie beschikt de PO over ten minste de volgende bevoegdheden (conform mandaatregister):
- Het melden van datalekken bij de Autoriteit Persoonsgegevens (back-up: de teammanagers).

Relatie tot de Privacy Officer Dienst Dommelvallei:
- Voor de aan de DD gemandateerde taken geldt dat de Privacy Officer Dienst Dommelvallei richting, advies, uitvoering en ondersteuning aan de teams binnen DD geeft, en dit afstemt af met de Privacy Officers van de betreffende gemeente wiens betrokkenen het betreft.
  Dit geldt ook voor de stukken die naar B&W, het College of de Raad van de gemeente gaan;
- De DD is een zelfstandige verwerkingsverantwoordelijke voor de eigen interne bedrijfsvoering (bijv. voor het in dienst nemen van DD medewerkers) en eigen privacy activiteiten, die worden zelfstandig uitgevoerd. Daarover kan gecommuniceerd worden met de gemeentelijke PO's (ten behoeve van advies en coördinatie).

2.8. Functionaris Gegevensbescherming (Consulted en Informed)
Op basis van de art. 36 en art. 37 Wpg is het aanwijzen van een interne toezichthouder, de Functionaris Gegevensbescherming (FG), verplicht voor de gemeente.

De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie, geniet ontslagbescherming voor het uitvoeren van zijn FG-taken, en ondervindt geen ander nadeel van de uitoefening van zijn FG-taak.

Tot de taken en verantwoordelijkheden van de FG behoren in ieder geval:
- Is verplicht tot geheimhouding van al hetgeen hem vanuit de uitoefening van zijn functie bekend is geworden, tenzij de betrokkene in bekendmaking toestemt;

- Toezicht houden:
  - Zorgt ervoor geen aanwijzingen of instructies te ontvangen voor de uitoefening van zijn FG functie;
  - Zorgt ervoor onderstaande bevoegdheden alleen te gebruiken voor zover dit voor de uitoefening van de FG-taak noodzakelijk is;
  - Is de interne toezichthouder, die erop toeziet dat de AVG en Wpg intern worden toegepast en nageleefd, ook bij samenwerking met anderen, waarin de gemeente (gezamenlijk) verwerkingsverantwoordelijk is, waaronder:
    - Toetst de juistheid en volledigheid van het verwerkingenregister;
    - Houdt toezicht op de verplichting om DPIA's en audits uit te voeren;
    - Houdt toezicht op de meldplicht van datalekken, en de volledigheid van het datalekkenregister;
    - Houdt toezicht op de afhandeling van verzoeken en klachten van betrokkenen;
    - Ziet toe op de verplichting om medewerkers bewust te maken en op te leiden;
    - Ziet toe op de wijze van implementatie van (risico-)maatregelen door de verwerkingsverantwoordelijke;
    - Ziet er samen met de verantwoordelijke portefeuillehouder op toe dat er een (Wpg-) privacy auditplan wordt opgesteld en uitgevoerd;
  - Adviseert gevraagd of ongevraagd over de verwerking van persoonsgegevens.

- Bewustwording stimuleren:
  - Informeert het verantwoordelijke bestuursorgaan, management en medewerkers over hun verplichtingen t.a.v. gegevensbescherming;
  - Draagt de beleidsuitwerking privacy actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming.

- Adviseren en informeren:
  - Monitort veranderingen in (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming, neemt de leiding bij het interpreteren hiervan, stelt de impact van deze wijzigingen vast, en adviseert de gemeente bij de implementatie hiervan;
  - Geeft de verwerkingsverantwoordelijke gevraagd en ongevraagd advies over passende wijzen om hun verplichtingen ten aanzien van gegevensbescherming in hun taakuitvoering, bedrijfsvoering en dienstverlening in te vullen en te integreren, waaronder over:
    - De activiteiten m.b.t. de beleidsuitwerking privacy en de prioritering ervan.
    - De noodzaak om DPIA's uit te voeren en de wijze van het uitvoeren van DPIA's of enige andere gegevensbescherming gerelateerde risicoanalyse.
    - Het verkleinen of volledig wegnemen van privacy risico's, en de adequaatheid van gedefinieerde maatregelen. Bijvoorbeeld bij hoog-risico dossiers of uitgevoerde risicoanalyses (zoals DPIA's of risicoanalyses ten aanzien van de toepassing van algoritmen, geautomatiseerde besluitvorming of doorgifte naar landen buiten de Europese Economische Zone).
    - De afhandeling van datalekken (volgens de geldende procedure).
    - Het afhandelen van privacy klachten, uitoefenen van rechten van betrokkenen, en adresseren van verzoeken of knelpunten die de inwoner/betrokkene signaleert.

- Onderzoeken:
  - Beschikt over controle- en monitoringbevoegdheden en voert zelfstandig controles uit;
  - Kan ambtshalve een onderzoek instellen naar de wijze waarop wordt voldaan aan de AVG/Wpg en de beleidsuitwerking privacy. De FG doet mededeling van de voorlopige bevindingen aan het college en de belanghebbenden die bij het onderzoek zijn betrokken en stelt hen in de gelegenheid hun zienswijze daarop te geven. Doet FG mededeling van zijn conclusies en aanbevelingen aan het college en de belanghebbenden die bij het onderzoek zijn betrokken. De FG kan een mededeling aan belanghebbende als bedoeld in lid 2 en lid 3 achterwege laten vanwege dringende redenen.

- Rapporteren:
  - Stelt periodiek een toezichtplan op;
  - Stelt jaarlijks een FG-toezichtrapportage op ten behoeve van het College van B&W, waarin wordt gerapporteerd over de stand van de Gegevensbescherming volgens de AVG en de Wpg, en geeft daarin aanbevelingen over te nemen maatregelen die een rechtmatige verwerking van persoonsgegevens helpen waarborgen.

- Communiceren:

- o Treedt op als contactpunt voor en pleegt overleg met de Autoriteit Persoonsgegevens over aangelegenheden t.a.v. gegevensbescherming, en werkt in die hoedanigheid met de AP samen ten behoeve van de versterking van haar systeemtoezicht;
- o Treedt op als contactpunt voor inwoners en medewerkers over aangelegenheden ten aanzien van gegevensbescherming, en ziet in die hoedanigheid toe op de afhandeling door de organisatie van privacy klachten en andere knelpunten die betrokkenen signaleren.

De FG is als volgt te bereiken:
Per post: Dienst Dommelvallei, Dorpsstraat 210, 5731 JL Mierlo
Per e-mail: FG@dienstdommelvallei.nl
Per telefonisch: 088 1631000 (alleen tijdens kantoortijden)

Vanuit zijn onafhankelijke toezichthoudende functie beschikt de FG over ten minste de volgende bevoegdheden, conform titel 5.2 van de algemene wet bestuursrecht:

- De FG heeft (na formeel verzoek) toegang tot alle ruimten en alle informatie, systemen, processen waarin persoonsgegevens (kunnen) worden verwerkt. FG mag zich daarbij laten vergezellen door personen die daartoe door hem zijn aangewezen;
- De FG is bevoegd apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen tonen, en indien noodzakelijk mee te nemen;
- De FG kan een onderzoek instellen naar de manier waarop, in een bepaald geval of in het algemeen belang, de persoonlijke levenssfeer wordt beschermd;
- Als de FG dit nodig acht, kan FG voor onderzoek gebruikmaken van de diensten van derden. Daarvoor vraagt FG voorafgaand aan de inzet toestemming aan de verwerkingsverantwoordelijke;
- De FG is bevoegd inlichtingen te vorderen van een ieder die onder gezag of in opdracht van de verwerkingsverantwoordelijke werkzaam is of ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
- De FG is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin persoonsgegevens zijn verwerkt;
- De FG is bevoegd van gegevens en bescheiden kopieën te maken. Als het maken van kopieën niet ter plekke kan gebeuren, is hij bevoegd de gegevens en bescheiden voor maximaal één werkdag mee te nemen;
- De FG is bevoegd opdracht te geven tot vernietiging van persoonsgegevens waarvan de bewaartermijn is overschreden of waarvan de verwerking onrechtmatig is.

2.9. Chief Information Security Officer (Consulted)
De gemeente heeft de functie Chief Information Security Officer (CISO) en tevens Eenduidige Normatiek Single Information Audit (ENSIA) coördinator belegd binnen DD. De rollen CISO en ENSIA-coördinator zijn beide gericht op informatiebeveiliging, maar hebben verschillende verantwoordelijkheden en focuspunten. De CISO is een strategisch adviseur in het kader van informatiebeveiliging en de ENSIA-coördinator is gericht op het coördineren van het verantwoordingstraject informatiebeveiliging (ENSIA). De taken, verantwoordelijkheden en bevoegdheden van de CISO rol zijn verder uitgewerkt in het informatiebeveiligingsbeleid.

De CISO werkt nauw samen met de Privacy Officers van de gemeente onder andere:

- Afstemming op raakvlakken tussen informatiebeveiliging en privacybescherming, en fysieke beveiliging van gemeente Geldrop-Mierlo
- Ondersteuning bij de afhandeling van datalekken van gemeente (conform procedure);
- Adviseert (gevraagd en ongevraagd) bij de reactie op ernstige informatieveiligheid- en ICT-incidenten (indien persoonsgegevens zijn betrokken dan is sprake van datalek);
- Voor de beantwoording van ENSIA-privacy vragen van gemeente geeft de Privacy Officer van gemeente input.

Daarnaast werkt de CISO nauw samen met de toezichthouder FG DD.

2.10. Overige rollen met relatie tot privacy (intern & extern)
De hieronder benoemde rollen hebben ieder voor zich een meer of mindere (indirecte) relatie ten aanzien van de verwerkingen van persoonsgegevens van onze inwoners en ondernemers. En medewerkers.

Team	Betrokkenheid
Informatiemanager GM en informatievoorziening DD	Inrichten van de informatievoorziening. Beoordeelt welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden. Hierbij is de privacy risicoclassificatie richtinggevend en wordt dit Privacy by

	Design en Privacy by default ingericht. Laat zich adviseren door de PO's van de gemeente. Stemt af met de informatiemanagers-contactpersonen bij de andere gemeenten.
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van communicatie van de gemeente betrokken. Adviseren van de gemeente over de communicatie bij datalekken (conform procedure Datalek melden).
Juridische Zaken	Ondersteunen van PO's ten aanzien van overige wetgeving privacyvraagstukken en adviseren over privacy-gerelateerde bepalingen in overeenkomsten.
Audit / Concern Control	In het verantwoordingstraject informatiebeveiliging (=ENSIA) wordt de AVG (gedeeltelijk) meegenomen. Voor de Wpg geldt dat de interne jaar controles door een auditor wordt uitgevoerd die Wpg-getraind is: voor 2023 t/m 2025 is dit belegd bij een extern bureau.

3. Overlegstructuur

De betrokkenen in de privacy organisatie zullen in verschillend verband overleg dienen te voeren, binnen de eigen organisatie, met de andere DD- organisaties, en ook met externe partijen, bijvoorbeeld in regionaal verband. Onderstaand schema wordt als richtinggevend gehanteerd, zie bijlage 2 voor detailbeschrijving van de overleggen.

Overleg	**Rollen**	**Tenminste**	**Inhoud**
Poho overleg informatiebeveiliging en privacy	Portefeuillehouder, Gemeentesecretaris, Juridisch controller, FG (voorzitter), PO's GM en CISO (om toerbeurt notulist)	4x per jaar	Ontwikkelingen informatiebeveiliging en privacy aansluitend op organisatorische ontwikkelingen & actualiteiten, en hoge risico's.
Overleg met Concern manager Lijn	Concern manager Lijn, PO GM (voorzitter, notulist)	4x per jaar	Opdrachtgever – opdrachtnemer overleg. m.b.t. Wpg verbeterplan. Informeren over AVG. Risico aanpak en escalaties (AVG, Wpg)
Privacy Officers GM overleg	PO's GM	1x per week	Afstemming en werkverdeling van privacy vragen, datalekken en bewustwording, berichten, kennisdeling, voortgang uitvoering privacy jaarplan, voorbereiding PoHo overleggen en verantwoording PDCA.
Privacy Officers overleg DD	FG (voorzitter), PO DD, PO's GM, PO NU, PO SB, CISO (notulist om toerbeurt)	1x per maand	Kennisdeling t.a.v. informatiebeveiliging en privacy, (organisatie)ontwikkelingen, datalekken, risico's, jaarplannen. Klankbord voor (individuele leden). Samenwerken als jaarplannen en actualiteiten dit toestaan.
Overleg met Informatiemanager	Informatiemanager, PO's GM (geen voorzitter, en geen notulist) Ontbreken IDV en IM (gecancelled door DD)	1x per maand	Kennisdeling over ontwikkelingen binnen de gemeente, delen van ieders jaarplan, afstemmen en de samenwerking opzoeken in belang van de lijn ten aanzien van vragen, risico's en ambitieformulieren etc. Vernieuwd overleg met IM, privacy, IDV en informatievoorziening over privacy GM.
Regionaal Privacy Officers overleg	FG Peelgemeenten, PO's GM, PO's Peelgemeenten (notulist en voorzitter)	1x per 3 maanden	Kennisdeling m.b.t. algemene privacy zaken en wettelijke ontwikkelingen, afstemming over gezamenlijke onderwerpen, eventueel met elkaar ontwikkelen van nieuwe procedures etc.
Regionaal FG-overleg	FG (voorzitter en notulist om toerbeurt)	1x per 3 maanden	Kennisdeling. Afstemming over gezamenlijke onderwerpen.
Weekstart FG-CISO	FG en CISO	1x per week	Afstemmen lopende zaken

Bijlage 1: Schematisch voorbeeld verantwoordelijkheden

Bijlage 2: Overleggen

2.1 PoHo -overleg informatiebeveiliging en privacy

1. Tenminste 2 keer per jaar is er een overleg met de Portefeuillehouder (PoHo) over informatiebeveiliging en privacy, en aanpalende thema's (bijvoorbeeld ethiek, artificial intelligence).
2. Aan het PoHo-overleg nemen in ieder geval de volgende functionarissen deel: Portefeuillehouder Burgemeester, Gemeentesecretaris, Juridisch controller, PO's en CISO, (om toerbeurt notulist), FG (voorzitter).
3. Het PoHo-overleg heeft de volgende doeleinden:
   - Het informeren over de huidige stand van zaken met betrekking tot het uitvoeren van het bij of krachtens de wet AVG en Wpg en over de informatiebeveiliging;
   - Het informeren over (urgente) ontwikkelingen op deze vakgebieden privacy en informatiebeveiliging;
   - Het informeren en adviseren over hoge risico's die geconstateerd zijn;
   - Het aangeven van de richting met betrekking van (de borging van) privacy en informatiebeveiliging.

2.2 Overleg met concern manager Lijn

1. Elk kwartaal is er overleg over de AVG en de Wpg met de concern manager Lijn die ook nog projectopdrachtgever van het Wpg verbeterplan is.
2. Aan het overleg nemen in ieder geval deel de concern manager Lijn (opdrachtgever Wpg verbeterplan) en de PO (opdrachtnemer Wpg verbeterplan);
3. Het overleg heeft de volgende doeleinden:
   - Het informeren over de huidige stand van zaken met betrekking tot de Wpg onder andere het uitvoeren van het Wpg verbeterplan;
   - Het bespreken van risico's die PO constateert binnen GM en bij de DD.
     De concern manager Lijn beslist hierover of escaleert deze richting CMT of het DOD, en koppelt besluitvorming hierover terug;
   - Het informeren en adviseren over de AVG.

2.3 Privacy Officers Geldrop-Mierlo overleg

1. Elke week is er overleg over de AVG en de Wpg tussen de PO's Geldrop-Mierlo ;
2. Het overleg heeft de volgende operationele en tactische doeleinden:
   - (Operationeel) Het overleggen over en verdelen van de actuele privacy vragen en datalekken en andere uit te voeren werkzaamheden zoals bewustwording;
   - De PO die projectopdrachtnemer Wpg verbeterplan is, informeert de andere PO hierover;
   - Het gezamenlijk opstellen van het privacy jaarplan (incl. auditplan), verdelen van de activiteiten, evalueren van datalekken, benoemen en oppakken van risico's, actualiseren van contentkalender;
   - Het evalueren/actualiseren van de beleidsuitwerking privacy, procedures;
   - Het onderling sparren en kennisoverdracht m.b.t privacy vraagstukken, AVG en Wpg ontwikkelingen;
   - De gezamenlijke voorbereiding van het PoHo overleg, FG overleg, en periodieke verantwoording van de PDCA-cyclus.

2.4 Privacy Officers DD overleg

1. 1x per maand komt de Privacy Officers overleggroep bij elkaar;
2. De overleggroep bestaat uit de FG (voorzitter), PO's van de drie gemeenten, de PO van de DD en de CISO (allen notulist om toerbeurt);
3. Tot de taken en verantwoordelijkheden van de werkgroep privacy behoren in elk geval:
   - Kennisdeling t.a.v. privacy en informatiebeveiliging, nieuwe wetgevingen en nieuwe ontwikkelingen;
   - Kennisdeling t.a.v. datalekken met impact voor meerdere organisaties;
   - Kennisdeling t.a.v. informatiebeveiliging jaarplan en privacy jaarplannen van de organisaties;
   - Oppakken van gezamenlijke risico's (en eventuele escalaties);
   - Samenwerking indien jaarplannen op elkaar afgestemd kunnen worden (uitwerkingen gebeuren buiten dit overleg), zoals:

i. aan ontwikkeling en actualisering van privacy formats/sjablonen bijvoorbeeld de beleidsuitwerking privacy, procedures, werkinstructies, hulpmiddelen betreffende de verwerking van persoonsgegevens, DPIA's;
ii. ambitieformulieren ICT;
iii. het organiseren van gezamenlijke activiteiten die een voortdurende bewustwording ten aanzien van privacy en informatiebeveiliging ten doel hebben;

– Functioneren als klankbord voor medewerkers en (individuele) leden van dit overleg.

2.5 Overleg met Informatiemanager

1. 1x per maand is er overleg tussen Informatiemanager en PO's ;
2. Tot de taken en verantwoordelijkheden van de leden in dit overleg behoren in elk geval:
   – het informeren van elkaar en afstemmen met elkaar m.b.t. ontwikkelingen binnen de organisatie en het afstemmen van de (verbeter)jaarplannen;
   – in belang van de lijn (1x afstemmen met lijn i.p.v. iedere afzonderlijk) door:
     i. het informeren van elkaar en afstemmen met elkaar m.b.t. ontwikkelingen op ieders vakgebied en (verbeter)jaarplannen;
     ii. Het afstemmen en samenwerken ten aanzien van ambitieformulieren (projecten/grote wijzigingen), privacy maatregelen, activiteiten Informatievoorzieningen;
     iii. het organiseren van gezamenlijke (bewustwording)activiteiten en/of bij vragen die over vakgebieden heen gaan.

   – Vernieuwde afstemming met DD informatievoorziening en IDV. Vervanger van het ' Overleg met Informatievoorziening, PO GM, FG en CISO'. Er wordt momenteel nagedacht over hoe de afstemming eruit gaat zien ten aanzien van hieronder benoemde onderwerpen en waarbij de PO's Geldrop-Mierlo betrokken zijn voor de privacy van de gemeente Geldrop-Mierlo .
     Er was: 1x per maand is er overleg tussen Informatievoorziening, IDV, PO GM, CISO en FG;
     Tot de taken en verantwoordelijkheden van deze groep behoorden in elk geval:
     a. het informeren van elkaar en afstemmen met elkaar m.b.t. ontwikkelingen op ieders vakgebied en (verbeter)jaarplannen;
     b. Het afstemmen en samenwerken ten aanzien van ambitieformulieren (projecten/grote wijzigingen), privacy en informatiebeveiligingsmaatregelen, ICT en Informatievoorziening activiteiten;
     c. het organiseren van gezamenlijke activiteiten en/of bij vragen die over vakgebieden heen gaan. Bijv. bij nieuwe ontwikkelingen 1x afstemmen met de lijn i.p.v. ieder afzonderlijk. Bijv. RHCE's voorstel t.a.v. anonimiseren (richtlijnen).

2.7 Regionaal Privacy Officers overleg

1. 1x per 3 maanden is er overleg met Privacy Officers in de regio (Peelland gemeenten);
2. Tot de taken en verantwoordelijkheden van deze groep behoren in elk geval:
   – Kennisdeling m.b.t. algemene privacy zaken en wettelijke ontwikkelingen;
   – Afstemming over gezamenlijke onderwerpen
     Bijvoorbeeld gegevensdeling met (regionale) samenwerkingsverbanden, elkaar kunnen voorzien van voorhanden procedures, werkinstructies, geanonimiseerde DPIA's enzovoorts.
   – Eventueel met elkaar ontwikkelen van nieuwe procedures, werkinstructies of DPIA's enzovoort.

2.8 Regionaal FG-netwerkoverleg

1. 1x per 3 maanden is er overleg met de FG's in de regio;
2. Tot de taken en verantwoordelijkheden van deze groep behoren in elk geval:
   – Kennisdeling;
   – afstemming over gezamenlijke onderwerpen.

2.9 Weekstart FG-CISO

Afstemming lopende zaken