Privacybeleid
Welzijnsgroep Parkstad Limburg

Alcander
CMWW
Impuls
Welzijnsgroep

Inhoud

1. Inleiding 3
2. Begripsbepalingen 3
3. Visie 6
4. Doel 6
5. Reikwijdte 6
6. Principes voor de verwerking van persoonsgegevens 7
7. Rollen en Verantwoordelijken 11
8. Datum van inwerkingtreding 13

1. Inleiding

Welzijnsgroep Parkstad Limburg bestaat uit vier uitvoeringsorganisaties, namelijk: Welzijnsgroep Parkstad Limburg (bedrijfsvoering), Alcander, Impuls en CMWW (waaronder PLUK). Alcander is lid van de coöperatie JENS. Het is belangrijk om te vermelden dat JENS een eigen privacybeleid heeft en dat dit document **niet** van toepassing is op JENS.

Welzijnsgroep Parkstad Limburg werkt met (persoons)gegevens van cliënten, ondernemers, medewerkers, vrijwilligers en (keten)partners. Deze gegevens verzamelt de organisatie ten behoeve van de uitvoering van haar taken. Alle betrokkenen moeten erop kunnen vertrouwen dat de organisatie zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende wereld, maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. Welzijnsgroep Parkstad Limburg (hierna te noemen WPL) is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

Geldigheidsduur

Dit beleid is vastgesteld op 1 april 2025 door het bestuur van WPL als eindverantwoordelijke voor de gegevensverwerking. Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's/GEB's) kan het bestuur besluiten tot een tussentijdse herziening.

2. Begripsbepalingen

1. **Algemene Verordening Gegevensbescherming (AVG)**
   Europese privacywetgeving die regels stelt voor het beschermen van persoonsgegevens en de rechten van betrokkenen waarborgt.
2. **Betrokkenen**
   Natuurlijke personen van wie de persoonsgegevens worden verwerkt, zoals cliënten, medewerkers, vrijwilligers en partners.
3. **Persoonsgegevens**
   Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (bijvoorbeeld naam, adres, telefoonnummer, of IP-adres).
4. **Bijzondere persoonsgegevens**
   Gevoelige gegevens zoals gezondheidsinformatie, ras, religie, politieke voorkeur of biometrische gegevens, die extra bescherming vereisen volgens de AVG.
5. **Functionaris Gegevensbescherming (FG)**
   Een onafhankelijke toezichthouder binnen de organisatie die erop toeziet dat de AVG wordt nageleefd.

6. **Privacy Officer**
   Het eerste aanspreekpunt binnen de organisatie voor vragen en ondersteuning omtrent privacy en gegevensbescherming.
7. **Verwerkersovereenkomst**
   Een contract tussen de organisatie en een verwerker waarin afspraken worden gemaakt over de verwerking en beveiliging van persoonsgegevens.
8. **Verwerking**
   Elke handeling of reeks van handelingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen.
9. **Verwerkingsverantwoordelijke**
   De partij (in dit geval WPL) die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt.
10. **Verwerker**
    Een derde partij die persoonsgegevens verwerkt in opdracht van de verwerkingsverantwoordelijke.
11. **Data Protection Impact Assessment (DPIA)**
    Een beoordeling van de privacyrisico's van een gegevensverwerking en de maatregelen om deze risico’s te verkleinen.
12. **Gegevenseffectbeoordeling (GEB)**
    De Nederlandse term voor DPIA, gericht op het vaststellen van risico’s voor betrokkenen bij het verwerken van persoonsgegevens.
13. **Privacy by Design**
    Een principe waarbij privacy en gegevensbescherming al vanaf de ontwerpfase van een dienst, systeem of proces worden meegenomen.
14. **Privacy by Default**
    Het principe dat systemen en processen standaard zo privacyvriendelijk mogelijk zijn ingesteld.
15. **Datalek**
    Een situatie waarin persoonsgegevens onbedoeld toegankelijk zijn voor onbevoegden of verloren gaan, zoals door hacking, verlies van documenten of menselijke fouten.
16. **Autoriteit Persoonsgegevens (AP)**
    De Nederlandse toezichthouder op de naleving van privacywetgeving.
17. **Recht op inzage**
    Het recht van een betrokkene om te weten welke persoonsgegevens over hem of haar worden verwerkt en voor welke doeleinden.
18. **Recht op rectificatie**
    Het recht van een betrokkene om onjuiste of onvolledige persoonsgegevens te laten corrigeren.
19. **Recht op verwijdering**
    Ook wel het “recht om vergeten te worden”. Het recht van een betrokkene om persoonsgegevens te laten verwijderen als deze niet meer nodig zijn of onrechtmatig worden verwerkt.
20. **Recht op beperking van verwerking**
    Het recht van een betrokkene om de verwerking van persoonsgegevens tijdelijk te laten stoppen, bijvoorbeeld bij twijfel over de juistheid van gegevens.

21. **Recht op bezwaar**
    Het recht van een betrokkene om bezwaar te maken tegen de verwerking van persoonsgegevens, bijvoorbeeld voor direct marketing.
22. **Recht op overdraagbaarheid (dataportabiliteit)**
    Het recht van een betrokkene om persoonsgegevens in een gestructureerde, gangbare vorm te ontvangen of door te laten sturen naar een andere organisatie.
23. **Verwerkingsregister**
    Een overzicht van alle verwerkingen van persoonsgegevens binnen een organisatie, zoals beschreven in de AVG.
24. **PDCA-cyclus**
    Een managementmethode die staat voor Plan, Do, Check, Act. Gebruikt om continue verbetering van processen, waaronder privacybescherming, te waarborgen.
25. **Toestemming**
    Een uitdrukkelijke en geïnformeerde goedkeuring van de betrokkene voor de verwerking van zijn of haar persoonsgegevens.
26. **Proportionaliteit**
    Het principe dat verwerking van persoonsgegevens in verhouding moet staan tot het doel waarvoor de gegevens worden verwerkt.
27. **Subsidiariteit**
    Het principe dat het doel waarvoor persoonsgegevens worden verwerkt, niet op een minder ingrijpende manier kan worden bereikt.
28. **Transparantie**
    De verplichting van de organisatie om betrokkenen duidelijk te informeren over hoe persoonsgegevens worden verwerkt.
29. **Geautoriseerde gebruiker**
    Een persoon die door de organisatie bevoegd is om persoonsgegevens te verwerken of te raadplegen.
30. **Logbestanden (logging)**
    Automatisch vastgelegde gegevens over toegang tot of wijzigingen in systemen en persoonsgegevens, die gebruikt kunnen worden voor beveiliging en auditing.
31. **Meldplicht datalekken**
    De verplichting om datalekken binnen 72 uur te melden aan de Autoriteit Persoonsgegevens en, in bepaalde gevallen, ook aan de betrokkenen.
32. **Normenkader**
    Een set van richtlijnen en beheersmaatregelen, zoals het IBD-borgingsproduct, om privacyrisico's te beoordelen en te beheren.
33. **Belanghebbende(n)**
    Personen of organisaties die direct of indirect betrokken zijn bij de verwerking van persoonsgegevens.
34. **Informatiebeveiligingsdienst (IBD)**
    Een dienst voor gemeenten die ondersteuning biedt bij informatiebeveiliging en privacy.
35. **Bewaartermijn**
    De periode waarvoor persoonsgegevens bewaard mogen worden, afhankelijk van wettelijke of organisatorische eisen.

36. **Verantwoordingsplicht**
    De verplichting van een organisatie om aan te tonen dat zij voldoet aan de regels van de AVG.

3. Visie

Welzijnsgroep Parkstad Limburg zet zich in voor een veilig en respectvol gebruik van persoonsgegevens om de vertrouwensband met cliënten, partners en de gemeenschap te versterken. In lijn met onze missie om inclusieve, veerkrachtige gemeenschappen te bevorderen, streven we naar een integrale aanpak van privacybescherming. Alle afdelingen en medewerkers dragen bij aan een transparante en zorgvuldige omgang met gegevens, waarbij eigenaarschap en bewustzijn centraal staan. Door risicobewustzijn en gedeelde verantwoordelijkheid binnen de organisatie willen we privacy niet alleen waarborgen, maar als fundament gebruiken voor het vertrouwen en de kwaliteit van onze diensten.

4. Doel

Met dit privacybeleid geeft de organisatie een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de organisatie persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

Verantwoordelijkheid van iedere werknemer

Iedereen die werkzaam is binnen de organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De organisatie verlangt van al haar medewerkers, vrijwilligers, stagiaires en alle personen die werkzaam zijn voor de organisatie dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

5. Reikwijdte

De organisatie verzamelt en gebruikt persoonsgegevens van cliënten, leveranciers, vrijwilligers, medewerkers, stagiaires en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de organisatie, waaronder:

1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de organisatie**;**
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de organisatie aan een rechtspersoon die voor de organisatie bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

6. Principes voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. WPL onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag

Persoonsgegevens worden door de organisatie slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een organisatie voort uit een wet (wettelijke verplichting).

Welbepaalde doeleinden

De organisatie verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de organisatie alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De organisatie ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken.

Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De organisatie voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de organisatie bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de organisatie bij voorkeur voor die mogelijkheid.

Juiste en actuele gegevens

De organisatie zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. De organisatie neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Gegevens worden op tijd vernietigd

De organisatie stelt de bewaartermijn van een verwerking vast voor persoonsgegevens met als uitgangspunt de wettelijke bepalingen:

- **Belastingwetgeving:** Financiële gegevens (zoals loonadministratie) moeten 7 jaar worden bewaard.
- **Arbeidsrecht:** Arbeidsovereenkomsten en gerelateerde documenten kennen vaak ook een bewaarplicht van 5 jaar.
- **AVG:** Volgens de Algemene Verordening Gegevensbescherming mogen gegevens niet langer worden bewaard dan noodzakelijk.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de organisatie de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De organisatie bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Integriteit en vertrouwelijkheid

De organisatie neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking.

Privacy by Default en Privacy by Design

De organisatie houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt *Privacy by Design* (PbD) genoemd. De organisatie draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de organisatie *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Toegang tot gegevens

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de organisatie geldend beleid voor toegang tot gegevens. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De organisatie hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Inbreuk in verband met persoonsgegevens

Bij toegang tot, verlies of wijziging van persoonsgegevens bij de organisatie, zonder dat dit de bedoeling is, is er sprake van een **datalek**. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en/ of bij de getroffen betrokkenen. De organisatie registreert datalekken, zet de bevindingen om in verbeterpunten

en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in het protocol Datalekken.

Samenwerking

De organisatie schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de organisatie. De AVG verplicht organisatie tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

Verder kan het voorkomen dat de organisatie samenwerkt met andere organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De organisatie maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de organisatie.

Transparantie

De organisatie informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de organisatie van deze informatieplicht af.

Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de organisatie over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen:

Recht op inzage
De medewerker mag opvragen welke persoonsgegevens de werkgever bewaart. Dit omvat bijvoorbeeld naam, adres, salarisinformatie en eventuele aantekeningen in het personeelsdossier.

Recht op rectificatie
Als bepaalde gegevens onjuist of onvolledig zijn (zoals een verkeerd adres of een fout in persoonlijke gegevens), kan de medewerker vragen om deze te laten corrigeren.

Recht op verwijdering (recht om vergeten te worden)
De medewerker kan in bepaalde situaties vragen om persoonsgegevens te verwijderen. Dit kan bijvoorbeeld als de gegevens niet meer nodig zijn of als deze onterecht worden verwerkt. Let op: sommige gegevens moeten wettelijk worden bewaard (bijvoorbeeld voor salarisadministratie).

Recht op bezwaar
Als de medewerker het niet eens is met hoe persoonsgegevens worden verwerkt, bijvoorbeeld voor een bepaald doel (zoals interne analyses), kan hij of zij bezwaar maken. De werkgever moet dan stoppen met die verwerking, tenzij er zwaarwegende redenen zijn om door te gaan.

Recht op beperking van verwerking
De medewerker kan vragen om het gebruik van persoonsgegevens tijdelijk te beperken, bijvoorbeeld als er twijfel is over de juistheid van de gegevens of als er bezwaar is gemaakt tegen de verwerking. In zo'n geval mogen de gegevens alleen worden opgeslagen, maar niet meer actief worden gebruikt.
Recht op overdraagbaarheid
Als de medewerker wil dat persoonsgegevens naar een andere partij worden overgedragen (bijvoorbeeld bij een overstap naar een nieuwe werkgever), kan hij of zij vragen om de gegevens in een gestructureerde, gangbare vorm te ontvangen.

Geschillenbeslechting

Indien de betrokkene van mening is dat de organisatie niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij dit melden bij de Privacy Officer. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording

Onder de verantwoordelijkheid van WPL vindt verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. WPL heeft een Privacy Officer in dienst. De Privacy Officer waarborgt dat de organisatie voldoet aan privacywetten en beschermt persoonlijke gegevens door het implementeren van beleid, procedures en nalevingscontroles. Daarnaast beschikt de organisatie over een toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd.

Register van verwerkingsactiviteiten

De organisatie beschikt over een register van verwerkingsactiviteiten (verwerkingsregister), waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

Gegevenseffectbeoordeling (GEB)

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de organisatie een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De organisatie voert in dat geval een gegevenseffectbeoordeling (ook wel Data Processing Impact Assessment of DPIA genoemd). Als uit de GEB blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de organisatie voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de organisatie met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd.

Functionaris gegevensbescherming (FG)

De organisatie is een stichting met een publieke functie die structureel persoonsgegevens verwerkt. De organisatie is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG presenteert jaarlijks aan het managementteam en het bestuur over zijn werkzaamheden, bevindingen en aanbevelingen.

PDCA Cyclus

De organisatie streeft ernaar om rondom de verwerking van persoonsgegevens *in control* te zijn en daarover op professionele wijze verantwoording af te leggen. *In control* betekent in dit verband dat de organisatie weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

Daarnaast gebruikt de organisatie het borgingsproduct van de IBD[1] is het beoordelingskader voor het waarborgen van privacy compliance binnen de organisatie. Het borgingsproduct is een normenkader wat door de organisatie gebruikt wordt voor het duiden van privacy risico's en de daarbij behorende beheersmaatregelen binnen de organisatie.

Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

7. Rollen en Verantwoordelijken

Hieronder is een beschrijving van de taken en verantwoordelijkheden van de diverse relevante personen/ groepen binnen de organisatie.

	Verantwoordelijk	
R	Responsible/ Feitelijk verantwoordelijk	• Managers • De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken • Vrijwilligers
A	Accountable/ Eindverantwoordelijk	• Het bestuur van WPL

[1] Informatiebeveiligingsdienst

C	Consulted/ Adviserend	• Privacy Officer • Functionaris Gegevensbescherming
I	Informerend/ Geïnformeerd	• Ondernemingsraad • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)

Het bestuur van WPL

Het bestuur is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de organisatie. Het bestuur heeft de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de organisatie;
- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert een duurzame privacycultuur.

Management

Het management is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid.
De managers hebben de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;
- Verantwoordelijk voor (laten) volgen van een verplichte training door werknemers binnen de eigen afdeling;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op de eigen afdeling;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Bevordert een duurzame privacy cultuur;
- Betrekt de Privacy Officer en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris gegevensbescherming (FG)

De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de organisatie:

- Toezicht houden op de naleving van de AVG en het adviseren van de organisatie over de implementatie van de wetgeving.

- Monitoren van veranderingen in privacywetgeving en het adviseren over de impact hiervan.
- Leiding nemen in het interpreteren van privacywetgeving en het adviseren van de organisatie bij de implementatie van nieuwe wetgeving.
- Advies geven bij het verminderen van privacyrisico's, zoals bij het uitvoeren van DPIA's (Data Protection Impact Assessments).
- Advies geven bij datalekken en het beheren van het datalekkenregister.
- Controleren en monitoren van de naleving van privacyrichtlijnen, inclusief het recht om interne onderzoeken uit te voeren.

Privacy Officer

De Privacy Officer is het eerste aanspreekpunt voor de organisatie rondom privacy gerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:

- **Beleidsontwikkeling en ondersteuning:**
  - Opstellen en onderhouden van een basisprivacybeleid en bijbehorende modellen, zoals verwerkersovereenkomsten.
  - Ondersteunen van verwerkingsverantwoordelijken bij het begrijpen en toepassen van het privacybeleid.
- **Afhandelen van datalekken:**
  - Monitoren en ondersteunen bij het melden en afhandelen van datalekken volgens de wettelijke meldplicht.
- **Advies geven:**
  - Adviseren over de verwerkingsgrondslag en belangrijke privacyvraagstukken.
- **Bewustwording:**
  - Organiseren van bewustmakingssessies of het beschikbaar stellen van informatie om medewerkers te informeren over privacyregels.

Overlegstructuur

Er is een privacy team bestaande uit:

- Privacy Officer
- Functionaris Gegevensbescherming
- Beleidsmedewerker Kwaliteit
- Manager Bedrijfsvoering

Het privacy team of een afvaardiging hiervan komt eenmaal per maand samen om lopende zaken te bespreken en af te stemmen over eventuele ontwikkelingen.

8. Datum van inwerkingtreding

1 april 2025