Privacybeleid AVG/Wpg
Werkplein Drentsche Aa 2025

Werkplein Drentsche Aa

Januari 2025 **Versie 1**

Inhoudsopgave

1. Doel en scope privacybeleid

Bij Werkplein Drentsche Aa (WPDA) werken we dagelijks met persoonsgegevens van inwoners, medewerkers en (keten)partners. Deze gegevens verzamelen en verwerken we om onze publiekrechtelijke taak goed uit te kunnen voeren. Bij WPDA draait alles om vertrouwen, transparantie en samenwerking. We willen dat inwoners en medewerkers erop kunnen rekenen dat hun gegevens met de grootst mogelijke zorgvuldigheid wordt behandeld.

Onze organisatie is zich bewust van de veranderende eisen rondom privacy en gegevensbescherming. Nieuwe technologieën, samenwerking met meer partners en een steeds verder digitaliserende samenleving maken het noodzakelijk om privacy op een toekomstbestendige manier te waarborgen. Dit doen we door technische en organisatorische maatregelen te treffen op het gebied van privacy en informatiebeveiliging en het geven van regie aan gebruikers over hun eigen gegevens.

Bij WPDA werken we volgens de Algemene Verordening Gegevensbescherming (AVG) voor alle verwerkingen van persoonsgegevens, zowel digitaal als op papier. De AVG versterkt en breidt privacyrechten uit en legt extra verantwoordelijkheden bij organisaties, waaronder een risicogerichte aanpak en aandacht voor privacy in de ontwerpfase van processen. Voor specifieke situaties, zoals de verwerking van persoonsgegevens door bijzondere opsporingsambtenaren (boa’s) in het kader van strafrechtelijke taken, geldt de Wet politiegegevens (Wpg). Hoewel de AVG en Wpg elkaar uitsluiten, zijn er ook raakvlakken. Dit privacybeleid geeft invulling aan beide wetten. Specifieke richtlijnen over de Wpg worden behandeld in hoofdstuk zeven.

Binnen onze organisatie, waar samensturing en de sociocratische kringmethodiek (SKM) centraal staan, spelen bestuur en directie een cruciale rol in het waarborgen van privacy. Zij ondersteunen onze teams om verantwoordelijkheid te nemen voor veilige en transparante gegevensverwerking.

Met dit beleid geven we duidelijkheid over hoe WPDA privacy beschermt, handhaaft en borgt. Dit beleid geldt voor de gehele organisatie, inclusief alle processen, onderdelen en gegevensverzamelingen waarin persoonsgegevens worden verwerkt. Het sluit aan bij onze filosofie: we werken samen, met respect voor ieders autonomie, en streven naar duurzame verbindingen gebaseerd op vertrouwen.

2. Beleidsuitgangspunten

Zorgvuldig omgaan met persoonsgegevens is voor WPDA meer dan een wettelijke verplichting: het is een kwestie van vertrouwen. Onze uitgangspunten zijn gebaseerd op respect voor privacy en sluiten aan bij de waarden die onze organisatie kenmerken, zoals autonomie, samenwerking en duurzame verantwoordelijkheid.

1. Rechtmatigheid, behoorlijkheid en transparantie
Persoonsgegevens worden verwerkt in overeenstemming met de wet en op een zorgvuldige, respectvolle manier. WPDA stelt betrokkenen altijd op de hoogte van de verwerking van hun gegevens, zodat zij weten wat er met hun gegevens gebeurt en waarom. Transparantie is een kernwaarde in ons handelen.

2. Juistheid
Bij WPDA vinden we het belangrijk dat de gegevens van inwoners kloppen en actueel zijn. We nemen daarom alle redelijke stappen om gegevens die niet juist zijn, gezien de doelen waarvoor we ze gebruiken, snel te corrigeren of te verwijderen.

3. Risicogerichte benadering
Het beschermen van privacy is een doorlopend proces binnen WPDA. We blijven op zoek naar verbeteringen in hoe we omgaan met persoonsgegevens. De directie is verantwoordelijk voor het grote geheel, en de Functionaris Gegevensbescherming (FG) en de Security- en Privacy Officer (PO/SO) geven advies en houden toezicht.
Bij nieuwe of aangepaste processen kijken we goed of er risico's zijn voor de privacy van inwoners en medewerkers en hoe we die kunnen voorkomen. Dit doen we via een privacycheck. Ons uitgangspunt is *privacy by design* (bescherming vanaf het ontwerp) en *privacy by default* (standaardinstellingen beschermen privacy). Indien nodig voeren we een uitgebreide PRIVACYCHECK uit, met advisering door de FG.
Bij WPDA zien we privacy niet alleen als een wettelijke verplichting, maar ook als een kans om te innoveren. Onze risicogerichte benadering is erop gericht om gecontroleerd te experimenteren, waarbij we fouten zien als een waardevolle bron van verbetering. Dit sluit aan op onze visie op innovatie en verbetering van dienstverlening.
Risico's worden besproken binnen de directie, die kan besluiten deze al dan niet te accepteren. Deze keuzes worden vastgelegd in een risicoregister, en het bestuur wordt periodiek geïnformeerd over de belangrijkste privacyrisico's.

4. Grondslag en doelbinding
Persoonsgegevens worden alleen verwerkt als er een wettelijke grondslag voor is. Deze gegevens worden uitsluitend verzameld en gebruikt voor duidelijk omschreven en gerechtvaardigde doelen.

5. Dataminimalisatie
WPDA wil alleen die persoonsgegevens verwerken die noodzakelijk zijn voor het vooraf vastgestelde doel.

6. Bewaartermijnen
Gegevens worden niet langer bewaard dan strikt noodzakelijk is. Soms is een lange bewaartermijn nodig om onze publiekrechtelijke taken uit te voeren of om te voldoen aan wettelijke verplichtingen.

7. Integriteit en vertrouwelijkheid
WPDA behandelt persoonsgegevens met grote zorg en respect. Alleen medewerkers die de gegevens nodig hebben voor hun functie krijgen toegang. We zorgen voor een passend niveau van beveiliging, zoals beschreven in ons informatiebeveiligingsbeleid.

8. Delen met derden
Bij samenwerking met externe partijen maken we duidelijke afspraken over hoe zij met gegevens omgaan. Deze afspraken voldoen altijd aan de wettelijke vereisten en worden vastgelegd in contracten of verwerkersovereenkomsten.

9. Subsidiariteit
Bij WPDA kijken we altijd zorgvuldig of we het doel kunnen bereiken op een manier die minder impact heeft of met minder ingrijpende middelen. Zo verwerken we gegevens alleen wanneer dat echt nodig is.

10. Proportionaliteit
De verwerking van gegevens moet in verhouding staan tot het doel. Een eventuele inbreuk op de privacy van betrokkenen mag nooit onevenredig zijn.

11. Rechten van betrokkenen
WPDA respecteert en faciliteert de rechten van betrokkenen, zoals het recht op inzage, correctie, beperking en verwijdering van hun persoonsgegevens. Binnen de wettelijke kaders voldoen we aan verzoeken.

12. Beveiligingsincidenten en datalekken
Een beveiligingsincident is een verstoring van de beschikbaarheid, integriteit of vertrouwelijkheid van informatie, zoals een storing, verlies van gegevens of een verkeerd verzonden e-mail. Als hierbij persoonsgegevens betrokken zijn, spreken we van een mogelijk datalek. WPDA heeft een duidelijk protocol voor de aanpak van datalekken en evalueert deze procedure regelmatig om te blijven leren en verbeteren

3. Rollen en verantwoordelijkheden

Bij WPDA ligt de nadruk op vertrouwen als basis voor samenwerking. Controlemechanismen, zoals audits en risicoregisters, worden ingezet om teams te ondersteunen in plaats van aan te sturen. Deze aanpak sluit aan bij onze kernwaarden van autonomie en duurzame verbindingen. Door teams verantwoordelijkheid te geven over privacybescherming, vergroten we eigenaarschap en betrokkenheid.

We hanteren hierbij het Three Lines of Defense-model:

- **Eerste lijn**: De projectleiders en proceseigenaren binnen de kolommen zijn verantwoordelijk voor hun eigen processen, inclusief het borgen van privacyvereisten.
- **Tweede lijn**: De Privacy Officer/Security Officer (PO/SO) ondersteunt en adviseert de eerste lijn bij privacyvraagstukken.
- **Derde lijn**: De Functionaris Gegevensbescherming (FG) beoordeelt onafhankelijk in hoeverre WPDA voldoet aan de privacywetgeving en het privacybeleid.

3.1 Bestuur

Het dagelijks bestuur (DB) van WPDA is het verantwoordelijke bestuursorgaan voor alle verwerkingen van persoonsgegevens en fungeert als verwerkingsverantwoordelijke in de zin van de AVG en de Wpg. Het DB draagt eindverantwoordelijkheid en zorgt ervoor dat WPDA voldoet aan de geldende wet- en regelgeving.

3.2 Ambtelijke rollen en verantwoordelijkheden

Directie

De directie is de uitvoerende schakel tussen het bestuur en de ambtelijke organisatie. Zij is verantwoordelijk voor de implementatie van de AVG, de Wpg en het privacybeleid en adviseert het DB hierover.

Privacy Officer/Security Officer (PO/SO)

De PO/SO is het eerste aanspreekpunt voor privacy binnen WPDA en heeft de volgende taken:

- Adviseren van teams, projectleiders en proceseigenaren over privacy.
- Ondersteunen bij risicoanalyses, beleidsontwikkeling en de implementatie van beveiligingsmaatregelen.
- Beheren van het datalekkenregister en coördineren van datalekprocedures.
- Coördineren van verzoeken van betrokkenen, zoals inzage- of verwijderverzoeken.
- Organiseren van bewustwordingstrainingen over de AVG en de Wpg.
- Levert input aan de FG voor rapportages aan de directie over privacyrisico’s en -prestaties.
- Bijhouden risicoregister.

Proceseigenaren
Proceseigenaren zijn verantwoordelijk voor de naleving van het privacybeleid in hun processen. Zij zorgen voor het uitvoeren van privacycheck en worden daarbij ondersteund door de PO/SO. Binnen WPDA zijn de teams uit het primaire proces de belangrijkste proceseigenaren. Ze leggen periodiek verantwoording af over hoe ze dit inhoud geven.

Medewerkers
Alle medewerkers van WPDA spelen een belangrijke rol bij het beschermen van privacy. Dit betekent dat zij:

- Privacy-incidenten melden bij de servicedesk.
- Meedoen aan trainingen om meer te leren over privacy.
- De afspraken over het omgaan met gegevens volgen.
- Hulp vragen aan de PO/SO als ze twijfelen over iets.

Functionaris Gegevensbescherming (FG)
De FG is de onafhankelijke toezichthouder binnen WPDA en heeft de volgende verantwoordelijkheden:

- Toezien op naleving van de AVG, de Wpg en het privacybeleid.
- Jaarlijks een rapport opstellen over privacygerelateerde bevindingen met aanbevelingen. Dit rapport wordt met een reactie van de organisatie voorgelegd aan het DB.
- Onafhankelijk adviseren over privacyvraagstukken, zowel op verzoek als op eigen initiatief.
- Coördineren bij datalekken en ervoor zorgen dat de organisatie de privacywetgeving correct naleeft.
- Een zwaarwegende zienswijze geven bij interpretatie van de privacywetgeving.

Chief Information Security Officer (CISO)
De CISO werkt samen met de andere privacy-experts om de directie te adviseren over en toezicht te houden op de beveiliging van informatie.

4. Sturing en verantwoording

Bij Werkplein Drentsche Aa (WPDA) is het waarborgen van privacy niet alleen een wettelijke verplichting, maar ook een belangrijk onderdeel van onze visie op betrouwbare en transparante dienstverlening. De sturing en verantwoording rond privacy zijn daarom stevig verankerd in onze organisatie, waarbij duidelijkheid en samenwerking centraal staan.

4.1 Sturing

Het privacybeleid wordt door het dagelijks bestuur (DB) vastgesteld en geldt voor de hele organisatie, voor zover de AVG en de Wpg op verwerkingen van toepassing zijn. Indien specifieke situaties dit vereisen, kunnen aanvullende procedures worden opgesteld. De toepassing van dit beleid wordt regelmatig geëvalueerd.

Het DB en de directie sturen op privacy aan de hand van de volgende uitgangspunten:

1. Het DB stelt het privacybeleid vast en bewaakt de naleving ervan.
2. Het DB informeert het algemeen bestuur over het gevoerde privacybeleid.
3. De directie zorgt voor de middelen die nodig zijn om het privacybeleid goed uit te voeren.
4. Het privacybeleid vormt, samen met het informatiebeveiligingsbeleid, de basis voor een betrouwbare informatievoorziening.
5. Privacy- en informatiebeveiligingsbeleid zijn geïntegreerd in het controlsysteem van WPDA, waarmee zij een belangrijk onderdeel vormen van de organisatiebrede sturing.

Binnen WPDA spelen teams een belangrijke rol in het ontwikkelen en naleven van privacywaarborgen. Dat betekent dat teams zelf beslissingen nemen over privacy binnen hun werkprocessen met ondersteuning van de PO/SO. Hiermee wordt eigenaarschap bevorderd en wordt privacy een gedeelde verantwoordelijkheid.

4.2 Verantwoording

De verantwoordingsplicht uit de AVG betekent dat WPDA niet alleen de regels naleeft, maar dit ook aantoonbaar moet maken. Hiervoor maken we gebruik van wettelijk verplichte hulpmiddelen en een werkwijze die aansluit bij onze organisatorische processen.

Wettelijke hulpmiddelen

1. Verwerkingsregister: een overzicht van alle verwerkingen van persoonsgegevens.
2. Privacycheck: onderzoek naar privacyrisico’s bij gegevensverwerkingen.
3. Overzicht van uitgevoerde privacychecks en rapportages.
4. Privacy by design en privacy by default: gegevensbeschermingsprincipes bij ontwerp en standaardinstellingen.
5. Risicoregister: een overzicht van actuele privacyrisico’s en de beheersing daarvan.
6. Incidentregister: een overzicht van incidenten die betrekking hebben op de AVG en Wpg.
7. Periodieke controles: onderzoek of genomen maatregelen effectief werken.

Werkwijze Werkplein Drentsche Aa

Om privacy structureel te borgen, hanteert WPDA de volgende aanpak:

1. Operationeel overleg: FG, CISO en PO/SO bespreken risico's de opvolging van maatregelen. De notulen van dit overleg worden maandelijks samengevat en gedeeld met de directie en de concerncontroller.
2. Tertaalgesprekken: Medewerkers van In Control bespreken privacyvraagstukken met sturingsteams en projectleiders, om privacy binnen teams en projecten te waarborgen.
3. Halfjaarlijkse gesprekken: De FG en CISO evalueren samen met de directie de maandelijkse verslagen en voortgang op privacy en informatiebeveiliging.
4. Jaarlijkse gesprekken: De directie bespreekt met het DB de voortgang en aandachtspunten.
5. Jaarstukken: Het DB legt jaarlijks verantwoording af aan het algemeen bestuur over de naleving van de AVG en Wpg, opgenomen in de paragraaf bedrijfsvoering van de jaarstukken. Hiermee wordt de verantwoording ingebed in de reguliere controlcyclus.

5. Overige elementen AVG en Wpg

De AVG en de Wpg geven personen meer controle over en invloed op hun persoonsgegevens. Deze rechten, bekend als de rechten van betrokkenen, vormen een belangrijk onderdeel van ons privacybeleid. Bij WPDA staan de rechten van betrokkenen en de beveiliging van persoonsgegevens centraal. We informeren betrokkenen helder, faciliteren hen in het uitoefenen van hun rechten en nemen alle mogelijke stappen om gegevens te beschermen. Zo waarborgen we de privacy op een manier die recht doet aan onze kernwaarden van vertrouwen, transparantie en samenwerking.

5.1 Informatieplicht

WPDA informeert betrokkenen duidelijk en transparant over de verwerking van hun persoonsgegevens. Dit gebeurt onder andere via de privacyverklaring AVG en Wpg, die beschikbaar is op onze website. Hierin staat onder meer:

- Welke gegevens worden verwerkt.
- Voor welke doeleinden deze gegevens worden gebruikt.
- Wat de rechten van betrokkenen zijn en hoe zij hiervan gebruik kunnen maken.

Door deze informatieplicht te vervullen, zorgen we ervoor dat betrokkenen weten wat er met hun gegevens gebeurt, wat bijdraagt aan vertrouwen en transparantie.

5.2 Rechten van betrokkenen

Betrokkenen kunnen gebruikmaken van hun rechten door een verzoek in te dienen bij WPDA, schriftelijk of via de website. We behandelen deze verzoeken zorgvuldig en binnen de wettelijke termijn:

- WPDA beoordeelt binnen een maand of het verzoek gerechtvaardigd is en communiceert binnen die termijn wat er met het verzoek gebeurt.
- Bij complexe verzoeken kan de afhandelingstermijn worden verlengd met maximaal twee maanden. Betrokkenen worden binnen vier weken op de hoogte gesteld van de verlenging en de reden hiervoor.
- Als WPDA besluit een verzoek niet in te willigen, geldt dit als een besluit in de zin van de Algemene wet bestuursrecht. Betrokkenen kunnen bezwaar maken en, indien nodig, beroep instellen.

Als betrokkenen vermoeden dat WPDA persoonsgegevens verwerkt in strijd met de wet, kunnen zij ook een klacht indienen bij de Autoriteit Persoonsgegevens.

5.3 Beveiligingsmaatregelen

WPDA zorgt er voor dat persoonsgegevens goed beveiligd zijn. Dit houdt in dat we:

- Technische, procesmatige, communicatieve en organisatorische maatregelen nemen.
- Rekening houden met de stand van de techniek, uitvoeringskosten, en wat praktisch haalbaar is.
- Maatregelen aanpassen aan de mogelijke risico’s voor mensen van wie we gegevens verwerken.

Wanneer WPDA persoonsgegevens verwerkt of door derden laat verwerken, zorgen we ervoor dat passende beveiligingsmaatregelen worden genomen. Hierbij baseren we ons op:

1. Baseline Informatieveiligheid Overheid (BIO): Dit biedt een breed toepasbare basis voor informatieveiligheid binnen de overheid.
2. Network and Information Security directive (NIS2): Dit zorgt voor aanvullende richtlijnen voor beveiliging van netwerken en informatie.

Deze maatregelen zijn bedoeld om persoonsgegevens te beschermen tegen verlies, ongeautoriseerde toegang of andere risico's. WPDA ziet beveiliging niet alleen als een technische verplichting, maar als een integraal onderdeel van een betrouwbare en respectvolle omgang met gegevens.

6. Verwerkers en gegevensuitwisseling

Of WPDA nu een externe verwerker inschakelt, als verwerker optreedt, of gegevens uitwisselt met andere partijen, onze aanpak is altijd gericht op transparantie, zorgvuldigheid en bescherming van persoonsgegevens.

We zorgen ervoor dat afspraken duidelijk zijn en dat alle betrokken partijen voldoen aan de vereisten van de AVG en Wpg. Hoewel WPDA werkt binnen duidelijke wettelijke kaders, blijft maatwerk altijd mogelijk. In complexe situaties wordt samen met betrokkenen gezocht naar oplossingen die recht doen aan hun unieke omstandigheden, zonder daarbij de privacywaarborgen te schenden. Dit sluit aan bij onze filosofie om inwoners op een persoonlijke en respectvolle manier te ondersteunen. Hiermee blijft WPDA een betrouwbare partner voor inwoners, medewerkers en ketenpartners.

Dit hoofdstuk beschrijft de verantwoordelijkheden en afspraken die WPDA maakt bij dergelijke verwerkingen, in lijn met de AVG en Wpg.

6.1 Inschakelen van een verwerker

Wanneer WPDA een externe partij inschakelt om namens de organisatie persoonsgegevens te verwerken en het verwerken van die gegevens de primaire taak van deze partij is, wordt deze partij beschouwd als een verwerker.

Om de privacy te waarborgen:

- Selecteert WPDA uitsluitend verwerkers die afdoende garanties bieden dat zij passende maatregelen nemen voor de bescherming van persoonsgegevens.
- Worden afspraken vastgelegd in een verwerkersovereenkomst, die:
  - De verantwoordelijkheden en verplichtingen van de verwerker omschrijft.
  - Voldoet aan de wettelijke eisen.
- Worden verwerkersovereenkomsten getoetst voordat de dienstverlening start en daarna periodiek geëvalueerd om naleving te waarborgen.

6.2 Werkplein Drentsche Aa als verwerker

In sommige gevallen kan WPDA optreden als verwerker voor derden die als verwerkingsverantwoordelijke optreden. In dergelijke situaties:

- Stelt WPDA duidelijke voorwaarden op om de verwerking zorgvuldig en transparant te laten verlopen.
- Geeft WPDA garanties dat persoonsgegevens worden verwerkt volgens de geldende privacywetgeving, met behulp van passende technische en organisatorische maatregelen.
- Worden de afspraken schriftelijk vastgelegd in een verwerkingsovereenkomst, die wordt ondertekend voordat de dienstverlening start.

Deze aanpak benadrukt de zorgvuldigheid waarmee WPDA omgaat met gegevens die namens derden worden verwerkt.

6.3 Gegevensuitwisseling

Bij gegevensuitwisseling met externe partijen die als zelfstandige verwerkingsverantwoordelijken optreden, gelden de volgende uitgangspunten:

- De externe partij verwerkt gegevens uitsluitend in het kader van haar eigen wettelijke of publieke taak.
- Voorafgaand aan de uitwisseling wordt een gegevensuitwisselingsovereenkomst opgesteld, waarin:
  - De te delen gegevens worden gespecificeerd.
  - Het doel van de gegevensuitwisseling duidelijk wordt omschreven.
- De uitwisseling vindt pas plaats nadat de overeenkomst door beide partijen is goedgekeurd.

Deze afspraken zorgen ervoor dat WPDA inzichtelijk maakt welke gegevens worden gedeeld en waarom, en dat de privacy van betrokkenen ook bij gegevensuitwisseling gewaarborgd blijft.

7. Uitvoering Wet politiegegevens

WPDA werkt met bijzondere opsporingsambtenaren (boa's) en is verantwoordelijk voor het zorgvuldig verwerken van politiegegevens volgens de Wet politiegegevens (Wpg).
Hierbij staan rechtmatigheid, transparantie en veiligheid centraal. Ons beleid zorgt ervoor dat inwoners en medewerkers erop kunnen vertrouwen dat gegevens correct worden verwerkt.

7.1 Specifiek Wpg-beleid

WPDA hanteert het volgende beleid voor het verwerken van politiegegevens:

1. Raamwerk beheersmaatregelen
    - WPDA gebruikt het door Wpg-auditoren gehanteerde raamwerk uit de NOREA-handreiking privacy audit Wpg voor boa's als basis voor de beheersmaatregelen.
2. Verwerkersovereenkomsten en TPM
    - Bij gebruik van een informatiesysteem dat door een externe leverancier wordt beheerd, sluit WPDA een verwerkingsovereenkomst af. De leverancier moet een Third Party Memorandum (TPM) opleveren volgens de NOREA-handreiking.
3. Grondslag voor verwerking
   Politiegegevens worden verwerkt op basis van:
    - Artikel 8 Wpg: Voor dagelijkse politietaken of verstrekking volgens artikelen 9, 10 en 12 Wpg.
    - Artikel 9 Wpg: Voor langdurig onderzoek of verstrekking volgens artikelen 15-21, 23 en 24 Wpg.
    - Artikel 15 Wpg: Voor gegevensuitwisseling bij onderzoeken onder verantwoordelijkheid van politie of andere opsporingsdiensten.
4. Toegangsbeveiliging
    - Alleen boa's en geautoriseerde medewerkers hebben toegang tot politiegegevens.
5. Beveiligde verzending
    - Politiegegevens worden altijd versleuteld verzonden.
6. Informatievoorziening aan inwoners
    - Inwoners worden via de privacyverklaring geïnformeerd over de verwerking van politiegegevens en, indien van toepassing, via de eerste brief die zij ontvangen over strafrechtelijke handhaving.

7.2 Rollen, taken en bevoegdheden in het kader van de Wpg

Dagelijks bestuur (DB)

Het DB is verantwoordelijk voor besluiten over toegang tot informatiesystemen met politiegegevens, waaronder het vaststellen van de autorisatiematrix.

Directie

De directie neemt autorisatiebesluiten op grond van artikel 6, lid 3, 4 en 5 van de Wpg met behulp van een specifiek formulier.

Privacy Officer/Security Officer (PO/SO)

- Jaarlijkse inventarisatie van wijzigingen in de verwerking van politiegegevens.
- Analyse van logbestanden.
- Aanpassing van het verwerkingsregister of Wpg-beleid indien nodig.
- Ondersteunen van interne en externe Wpg-audits.

Bevoegd functionaris Wpg

De rol van bevoegd functionaris is toegewezen aan de langst in dienst zijnde boa en omvat:

- Handhaving van gedragsregels en bijhouden van een overzicht met geautoriseerde medewerkers.
- Opstellen van een lijst met veelvoorkomende verstrekking en de bijbehorende grondslag.
- Bewaking van artikel 9 Wpg-gegevens, waaronder:
  - Verwijdering van gegevens binnen zes maanden na veroordeling of verjaring van het delict (voor audits of klachtenprocedures).
  - Definitieve vernietiging van gegevens vijf jaar daarna.
- Documentatie van doel, noodzaak, herkomst en vastlegging van gegevens.
- Overleg met de Officier van Justitie.
- Toezicht op rechtmatige verkrijging en verwerking van gegevens.
- Instemming met verdere verwerking en terbeschikkingstelling van gegevens op basis van de Wpg.
- Coördineren van interne en externe Wpg-audits.

7.3 Privacy audits Wpg

WPDA voert periodieke audits uit om te voldoen aan de Wpg:

- **Externe privacy audit**
  - Eens per vier jaar wordt een externe audit uitgevoerd, waarbij de naleving van de Wpg wordt beoordeeld. De resultaten worden gerapporteerd aan de Autoriteit Persoonsgegevens (AP).
- **Interne privacy audit**
  - Jaarlijks wordt een interne audit uitgevoerd om te toetsen of WPDA voldoet aan de wettelijke eisen. Deze audit vormt de basis voor eventuele verbeteringen in de verwerking van politiegegevens.

8. Inwerkingtreding, evaluatie en herziening

Dit privacybeleid treedt in werking na vaststelling door het dagelijks bestuur (DB) van Werkplein Drentsche Aa en vervangt daarmee het eerder vastgestelde Wpg-beleid. Het beleid is leidend voor de omgang met persoonsgegevens en vormt een essentiële basis voor het waarborgen van privacy binnen de organisatie. Met de vaststelling, evaluatie en eventuele herziening van dit beleid blijft WPDA flexibel en toekomstgericht inspelen op ontwikkelingen rondom privacy. Door heldere kaders te scheppen en regelmatig te toetsen of deze nog effectief en doelmatig zijn, behouden we een betrouwbare en transparante organisatie waarin privacy vooropstaat.

8.1 Inwerkingtreding

Het privacybeleid geldt vanaf de datum van vaststelling door het DB. Het beleid is van toepassing op alle onderdelen van WPDA en omvat zowel de verwerking van persoonsgegevens onder de AVG als de verwerking van politiegegevens onder de Wpg.

8.2 Afwijken van het beleid

Afwijkingen van dit beleid zijn in beginsel niet toegestaan. Indien een specifieke situatie afwijking noodzakelijk maakt, dient dit:

- Gemotiveerd te worden beschreven.
- Voorafgaand te worden goedgekeurd door het DB of een door het DB aangewezen verantwoordelijke.

8.3 Periodieke evaluatie

De Functionaris Gegevensbescherming (FG) bekijkt regelmatig samen met de andere privacy-experts of ons beleid nog goed werkt. Ze letten daarbij op:

1. Of we de doelen van het beleid bereiken
2. Of onze maatregelen voldoende bescherming bieden.
3. Of we rekening houden met nieuwe wetten en ontwikkelingen in de maatschappij.

8.4 Herziening

Op basis van de evaluatie kan het beleid worden aangepast. Herzieningen worden door de FG voorbereid en ter goedkeuring aan het DB voorgelegd. Na vaststelling wordt het herziene beleid gecommuniceerd naar alle betrokkenen binnen WPDA.