Regionale Sociale Dienst
KROMME RIJN HEUVELRUG

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 496
4 mei
2023

Officiële uitgave van de gemeenschappelijke regeling Regionale Dienst Werk en Inkomen Kromme Rijn Heuvelrug

Privacybeleid 2022-2024 v1.1

Definities en afkortingen

Begrip	Betekenis
AVG	Algemene Verordening Gegevensbescherming; gebaseerd op een Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de gehele Europese Unie standaardiseert.
AP	Autoriteit Persoonsgegevens; de onafhankelijke Nederlandse toezichthouder op de naleving van de Europese en nationale regels voor de bescherming van persoonsgegevens.
Betrokkene	Individu van wie persoonsgegevens worden verwerkt, bijvoorbeeld de klant, leverancier of medewerker.
DPIA	Data protection impact assessment; een instrument om te kunnen aantonen dat de organisatie voldoet aan de verplichtingen uit de AVG. Wordt uitgevoerd bij een nieuwe verwerking of bij de wijziging van een bestaande verwerking die naar verwachting een hoog risico voor de rechten en vrijheden van betrokkene met zich meebrengt.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, bijvoorbeeld naam, adres, woonplaats, telefoonnummer, geboortedatum, mailadressen, financiële persoonsgegevens, bankrekeningnummers, paspoortkopieën, foto's, bijzondere persoonsgegevens zoals medische gegevens, strafrechtelijke persoonsgegevens en bij wet voorgeschreven identificatienummers (BSN).
RDWI	Regionale Dienst Werk en Inkomen; is ingesteld door de gemeenten De Bilt, Bunnik, Utrechtse Heuvelrug, Wijk bij Duurstede en Zeist om de werkzaamheden op de terreinen van werk, inkomen, sociale werkvoorziening, re-integratie, schuldhulpverlening, inburgering en andere daarmee verband houdende onderwerpen gezamenlijk uit te voeren.
RSD	In de communicatie naar buiten toe maakt de RDWI tevens gebruik van de naam Regionale Sociale Dienst (RSD).
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming; geeft invulling aan bepalingen die in de AVG niet (volledig) zijn uitgewerkt.
Verwerken	Elke handeling met betrekking tot persoonsgegevens valt onder het verwerken van persoonsgegevens, bijvoorbeeld het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op een andere manier beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen of vernietigen van gegevens.
Verwerker	De verwerker is de persoon of de organisatie die de persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke.
Verwerkings-verantwoordelijke	De verwerkingsverantwoordelijke is een persoon of organisatie die het doel van en de middelen voor het verwerken van persoonsgegevens bepaalt.
Wpg	Wet politiegegevens; gebaseerd op een Europese verordening die de regels voor de verwerking van politiegegevens regelt.

1 Inleiding

De Regionale Dienst Werk en Inkomen (RDWI) is ingesteld door de gemeenten De Bilt, Bunnik, Utrechtse Heuvelrug, Wijk bij Duurstede en Zeist om de werkzaamheden op de terreinen van werk, inkomen, sociale werkvoorziening, re-integratie, schuldhulpverlening, inburgering en andere daarmee verband houdende onderwerpen gezamenlijk uit te voeren. In de communicatie naar buiten gebruikt de RDWI tevens de naam Regionale Sociale Dienst (RSD).

De RSD biedt een vangnet voor inwoners van de deelnemende gemeenten die tijdelijk niet of onvoldoende in hun inkomen kunnen voorzien. Dit vangnet bestaat uit begeleiding en hulp bij het vinden van werk, bij het aanvragen van een uitkering, begeleiding bij het oplossen van schulden en andere vormen van inkomensondersteuning. Om dit vangnet te kunnen bieden, verwerkt de RSD verschillende soorten persoonsgegevens. De verwerking van deze persoonsgegevens valt onder de bescherming van de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) en de Wet politiegegevens (Wpg). Dit beleid is een uitwerking van de uitgangspunten, regels en verplichtingen die afkomstig zijn uit deze wetgeving.

1.1 Doel en reikwijdte

Het doel van dit beleid is het stellen van kaders voor een verantwoorde omgang met persoonsgegevens en het waarborgen van de rechten die betrokkenen hebben bij de verwerking van hun persoonsgegevens door de RSD. De uitgangspunten die in dit beleid zijn beschreven zijn verder uitgewerkt en geborgd in verschillende procedures en richtlijnen. Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens door de RSD en op alle voorzieningen, ruimten en apparaten waarbinnen of waarmee de verwerking van persoonsgegevens plaatsvindt en hangt nauw samen met het strategisch informatieveiligheidsbeleid[1] van de RSD.

1.2 Verantwoordelijkheden

- Iedere medewerker dient kennis genomen te hebben van dit beleid en is verantwoordelijk voor de naleving hiervan.
- Unitmanagers zijn verantwoordelijk voor de controle op de naleving van dit beleid door de medewerkers van de eigen unit.
- De privacy officer is verantwoordelijk voor de actualiteit van dit beleid en werkt deze bij als zich grote wijzigingen voordoen in de wetgeving of de omgeving van de organisatie.
- De functionaris gegevensbescherming houdt intern toezicht op de toepassing en naleving van dit beleid.

1.3 Vaststelling

Dit beleid treedt in werking na vaststelling door het dagelijks bestuur van de RSD en wordt jaarlijks beoordeeld om te controleren of zij nog in voldoende mate aansluit op de realiteit. Ten minste één keer per drie jaar wordt het beleid volledig herzien.

2 Juridisch kader en uitgangspunten

Inwoners die zich als klant aanmelden bij de RSD moeten erop kunnen vertrouwen dat de RSD zorgvuldig met hun persoonsgegevens omgaat. Uitgangspunt hierbij is dat de RSD zich bij de uitoefening van haar taken houdt aan alle relevante wet- en regelgeving. Het juridische kader voor het verwerken van persoonsgegevens en de uitgangspunten die hieruit voortvloeien zijn in dit hoofdstuk verder uitgewerkt.

2.1 Juridisch kader

Allereerst is de RSD bij het verwerken van persoonsgegevens gebonden aan de AVG, de UAVG en de Wpg. Daarnaast is de RSD als bestuursorgaan gebonden aan de algemene regels van het bestuursrecht, zoals onder meer vastgelegd in de Algemene wet bestuursrecht (Awb), de Wet openbaarheid van bestuur (Wob) en per 1 mei 2022 de Wet open overheid (Woo). Ook is de RSD gebonden aan onder andere de Archiefwet, met het oog op het bewaren en vernietigen van gegevens.

Tot slot zijn er nog verschillende specifieke wet- en regelgeving die van toepassing zijn op de verwerking van persoonsgegevens door de RSD, waaronder onder meer de:

- Wet politiegegevens (Wpg);
- Besluit politiegegevens (Bpg);
- Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg boa);
- Participatiewet (Pw);
- Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW);
- Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ);
- Wet inburgering 2021;
- Wet gemeentelijke schuldhulpverlening (Wgs);
- Baseline Informatiebeveiliging Overheid (BIO): dit is het normenkader voor het niveau van informatiebeveiliging, geldend voor alle overheidsorganisaties.

1) In het Strategisch Informatieveiligheidsbeleid is de beveiliging uitgewerkt van alle informatie die wordt verwerkt binnen de RSD, waaronder de persoonsgegevens.

2.2 Uitgangspunten RSD

Vanuit bovengenoemde wet- en regelgeving vloeien een aantal verplichtingen voort voor het verwerken van persoonsgegevens, die hieronder zijn vertaald in uitgangspunten. Deze uitgangspunten waarborgen een zorgvuldige omgang met persoonsgegevens en de privacyrechten van betrokkenen. De invulling die is gegeven aan onderstaande uitgangspunten zijn verder uitgewerkt in de rest van het beleid en onderliggende procedures en richtlijnen.

- **Rechtmatigheid, behoorlijkheid, transparantie**
  Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. De RSD is transparant over de verwerkingen van persoonsgegevens die plaatsvinden binnen de RSD, op basis van welke grondslag deze gegevens worden verwerkt en op welke manier deze gegevens zijn beveiligd.
- **Grondslag en doelbinding**
  Persoonsgegevens worden alleen verwerkt als daar een rechtvaardige grondslag voor is en worden alleen gebruikt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen.
- **Dataminimalisatie**
  De RSD verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel van de verwerking. Dit vooraf bepaalde doel wordt zorgvuldig afgewogen en is altijd gebaseerd op een grondslag uit de AVG of de Wpg.
- **Bewaartermijnen**
  Onder het verwerken van persoonsgegevens valt ook het bewaren van deze persoonsgegevens. Het bewaren van persoonsgegevens is nodig om onze taken goed te kunnen uitoefenen en om wettelijke verplichtingen te kunnen naleven. De RSD bewaart persoonsgegevens niet langer dan strikt noodzakelijk is, waarbij onder andere uitgegaan wordt van de wettelijke termijnen zoals deze zijn vastgelegd in de Archiefwet en de Selectielijst gemeenten en intergemeentelijke organen 2020.
- **Integriteit en vertrouwelijkheid**
  De RSD gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Al onze medewerkers tekenen een geheimhoudingsverklaring. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de RSD voor een passende beveiliging van persoonsgegevens. Meer informatie over de beveiliging van onze gegevens is vastgelegd in het informatiebeveiligingsbeleid.
- **Delen met derden**
  In het geval van samenwerking met externe partijen, waarbij sprake is van de verwerking van persoonsgegevens, maakt de RSD afspraken over de eisen waar deze gegevensuitwisseling aan moet voldoen. Deze afspraken worden overeenkomstig relevante wet- en regelgeving uitgewerkt en vastgelegd in een verwerkersovereenkomst.
- **Rechten van betrokkenen**
  De RSD honoreert alle rechten van betrokkenen. Op onze website worden deze rechten toegelicht en is te vinden hoe een verzoek kan worden ingediend.
- **Subsidiariteit (noodzaak) en proportionaliteit (evenredigheid)**
  Het verwerken van persoonsgegevens is per definitie een inbreuk op de persoonlijke levenssfeer van de betrokken inwoner. Daarom wordt voorafgaand aan de verwerking zorgvuldig afgewogen of en welke persoonsgegevens noodzakelijk zijn voor het doel van de verwerking en wordt gekeken of de inbreuk op de belangen van de betrokkene niet onevenredig is in verhouding tot en met de verwerking.
- **Privacy by design**
  Privacy by design houdt in dat er voor de start van een verwerking of de aanschaf van een nieuw systeem is nagedacht over privacy. Door hier bij de inrichting al over na te denken, worden de verplichtingen uit de AVG en indien van toepassing de Wpg zo goed mogelijk geborgd in het nieuwe proces of systeem. Dit principe komt onder andere terug in het uitvoeren van DPIA's.
- **Privacy by default**
  Samenhangend met privacy by design is privacy by default. Dit principe houdt in dat de standaardinstellingen voor een gebruiker zo privacy-vriendelijk mogelijk zijn ingesteld. Heeft de medewerker het BSN-nummer niet nodig voor de verwerking, maar staat deze wel in het systeem? Dan wordt het systeem zo ingericht dat de medewerkers die deze gegevens niet nodig hebben, deze ook niet kunnen zien.

3 Verwerkingen

Alle verwerkingen die plaatsvinden bij de RSD vloeien voort uit haar wettelijke taken en zijn opgenomen in het register van verwerkingen. In dit register is inzichtelijk gemaakt welke verwerkingsactiviteiten er onder de verantwoordelijkheid van de RSD plaatsvinden. In het register is (ten minste) de volgende informatie opgenomen:

- de herkomst van de persoonsgegevens;
- de verwerkingsdoeleinden;
- de grondslag van de verwerking;
- de categorieën van persoonsgegevens;
- de categorieën van betrokkenen;
- de categorieën van ontvangers;
- de beveiligingsmaatregelen;
- de bewaartermijn van de gegevens.

Het register van verwerkingen wordt beheerd door de privacy officer, onder toezicht van de functionaris gegevensbescherming. Meer informatie over de verwerkingen van de RSD is te vinden in het register, waarvan een publieke versie op de website van de RSD wordt geplaatst.

3.1 Aard en omvang persoonsgegevens
De RSD verwerkt tijdens de uitvoering van haar wettelijke taken alle mogelijke categorieën van persoonsgegevens, waaronder naam, adres, woonplaats, telefoonnummer, geboortedatum, e-mailadressen, financiële persoonsgegevens, bankrekeningnummers, paspoortkopieën, foto's, bijzondere persoonsgegevens zoals medische gegevens, strafrechtelijke persoonsgegevens en bij wet voorgeschreven identificatienummers (BSN). De RSD verwerkt alleen gegevens die noodzakelijk zijn voor het uitvoeren van haar wettelijke taken, zoals bijvoorbeeld het verlenen van (bijzondere) bijstand, financiële ondersteuning bij kinderopvang en re-integratie.

3.2 Grondslag en doelbinding
Persoonsgegevens worden alleen verwerkt als daar een rechtvaardige grondslag voor is. In de verschillende wetten die ten grondslag liggen aan de taakuitvoering van de RSD zijn bepalingen opgenomen welke persoonsgegevens voor welke taken mogen worden verwerkt. In de gevallen waar bijzondere categorieën persoonsgegevens worden verwerkt[2] is er sprake van een uitzonderingsgrond[3] en is in de uitvoering voorzien in zodanig waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. In het register van verwerkingen zijn de specifieke grondslagen per verwerking uitgewerkt.

Daarnaast worden persoonsgegevens alleen verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. Gegevens die door de RSD worden verwerkt hebben als doel het in behandeling nemen, beoordelen en afhandelen van de verschillende onderdelen van één van de (wettelijke) taken. Denk hierbij aan het verzamelen van financiële informatie om te bepalen of een inwoner recht heeft op schulddienstverlening of het uitvoeren van een fraudeonderzoek met betrekking tot een bijstandsuitkering. In het register van verwerkingen wordt per verwerking aangegeven met welk doel de persoonsgegevens worden verzameld en verwerkt.

3.3 Bewaartermijnen persoonsgegevens
Op grond van de Archiefwet moet de RSD bewaartermijnen hanteren voor specifieke gegevens. Hieronder is een overzicht weergegeven van de bewaartermijnen van de meest voorkomende processen.

Dossiers	**Bewaartermijn (in jaren)**	**Aanvullende informatie**
Levensonderhoud en bijzondere bijstand (toegekend)	10	Gegevens 10 jaar bewaren na stoppen uitkering
Levensonderhoud en bijzondere bijstand (afgewezen)	5	
Levensonderhoud en bijzondere bijstand (afgebroken)	1	
Levensonderhoud en bijzondere bijstand (buiten behandeling gesteld)	5	
Schuldhulpverlening (toegekend)	5	5 jaar na doorlopen proces SDV
Schuldhulpverlening	1	No show of éénmalig advies

2) Art. 9 lid 1 AVG
3) Art. 9 lid 2 AVG

Inburgering	5	Voor sommige gegevens geldt een bewaartermijn van 50 jaar (art. 9.9 Besluit inburgering 2021), namelijk: • BSN • naamgegevens • adresgegevens • woonplaats • geboortedatum • gegevens die betrekking hebben op gehele of gedeeltelijke vrijstelling van de inburgeringsplicht • gegevens die betrekking hebben op een ontheffing van de inburgeringsplicht • de datum en de wijze waarop aan de inburgeringsplicht is voldaan Alle andere gegevens worden 5 jaar na beëindiging inburgeringsplicht, of na overlijden van de inburgeringsplichtige, verwijderd.
Politiegegevens	Zie toelichting	De RSD verwerkt politiegegevens op grond van art. 9 Wpg (onderzoek in bepaald geval). De bewaartermijn van deze gegevens is als volgt op te delen: • bewaren tot niet meer nodig voor het doel van het onderzoek • daarna: een half jaar hergebruik van de gegevens voor andere doeleinden • daarna: 5 jaar opslaan voor audits en klachten • daarna vernietigen

3.4 Doorgifte[4]

De RSD maakt voor het verwerken van persoonsgegevens in applicaties en systemen afspraken[5] met leveranciers over deze verwerking(en) en eventuele doorgifte van persoonsgegevens aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie. Als er sprake is van doorgifte aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie, dan gebeurt dit alleen op grond van goedgekeurde afspraken door de Europese Commissie.

3.5 Datalekken

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt de RSD dit zonder onredelijke vertraging, uiterlijk binnen 72 uur nadat kennis van de inbreuk is vernomen, aan de Autoriteit Persoonsgegevens. Als de melding niet binnen 72 uur wordt gedaan, wordt een motivering voor de vertraging bijgevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dat geval meldt de RSD dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken periodiek geëvalueerd.

4 Governance en organisatie

Iedere medewerker van de RSD is zelf verantwoordelijk voor het juist verwerken van persoonsgegevens. De omgang met en beveiliging van persoonsgegevens wordt gevraagd en ongevraagd gecontroleerd door de functionaris gegevensbescherming.

4.1 Basisregels

De RSD hanteert onderstaande basisregels voor de omgang met en beveiliging van alle persoonsgegevens die worden verwerkt door en in opdracht van de RSD[6].

1. Verwerk alleen persoonsgegevens die nodig zijn voor het uitvoeren van de wettelijke taken van de RSD.

4) **Artikel 44 t/m 50 AVG en art. 6c Wpg**
5) Deze afspraken worden doorgaans vastgelegd in een verwerkersovereenkomst en/of contracten
6) Gebaseerd op de basisregels zoals beschreven in het privacybeleid van de AP, d.d. 8 oktober 2019

2. Gebruik alleen die persoonsgegevens die nodig zijn voor het doel/activiteit waarvoor ze zijn verzameld.
3. Zorg dat persoonsgegevens die worden verwerkt juist en actueel zijn.
4. Sla persoonsgegevens alleen op de daarvoor bestemde plekken op.
5. Deel persoonsgegevens alleen met collega's die direct betrokken zijn.
6. Laat persoonsgegevens niet onbeheerd achter.
7. Ga extra zorgvuldig om met bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens.
8. Verwijder persoonsgegevens na het verstrijken van de bewaartermijn.
9. Ga extra zorgvuldig om met het verstrekken van persoonsgegevens aan derden.
10. Raadpleeg de privacy officer bij bijzondere situaties of voor advies.
11. Maak een melding bij de functionaris gegevensbescherming als je persoonsgegevens hebt gelekt, of wanneer deze zijn gelekt door collega's (bijvoorbeeld stukken die zijn achtergebleven in de printer).

4.2 Verantwoordelijkheidsniveaus
Binnen de RSD worden vier verantwoordelijkheidsniveaus met betrekking tot privacy en informatieveiligheid onderscheiden. Deze niveaus zijn hieronder beschreven.

- **Het dagelijks bestuur**
  Het dagelijks bestuur, als eigenaar van de verwerkingen en (informatie)systemen van de RSD, draagt de bestuurlijke verantwoordelijkheid voor een passend niveau van informatieveiligheid en privacy. Zij stelt – onder andere middels het privacybeleid - de kaders ten aanzien van informatieveiligheid en privacy op basis van relevante wet- en regelgeving en normenkaders. Zij is verantwoordelijk voor een duidelijk te volgen informatieveiligheidsbeleid en privacybeleid en stimuleert de directeur en het managementteam deze beleidsstukken na te leven.
- **De directeur en het managementteam**
  Gemandateerde verantwoordelijkheid voor informatieveiligheid en privacy ligt bij de directeur. Deze stelt met het managementteam het gewenste niveau van informatieveiligheid en privacy vast. De directeur is verantwoordelijk voor een correcte omgang met en juiste beveiliging van persoonsgegevens, bedrijfsprocessen en in- en externe informatiesystemen. De directeur wijst voor ieder (informatie)systeem een proceseigenaar aan[7]. De ambtelijke eindverantwoordelijkheid ligt bij de directeur.
- **Unitmanagers**
  De unitmanagers zijn verantwoordelijk voor de persoonsgegevens en integrale beveiliging van de processen en systemen die draaien onder hun verantwoordelijkheid. De unitmanagers zijn verantwoordelijk voor een juiste en veilige omgang met persoonsgegevens en de implementatie en het uitdragen van de maatregelen die voortvloeien uit het informatieveiligheidsbeleid en het privacybeleid.
- **Medewerkers**
  Iedere medewerker is verantwoordelijk voor een juiste omgang met en beveiliging van persoonsgegevens die worden verwerkt binnen de eigen functie en taken. Medewerkers zijn zich bewust van de eisen ten aanzien van de omgang met persoonsgegevens en de vertrouwelijkheid, integriteit en beschikbaarheid van de informatieprocessen binnen de eigen functie en taken. Door de Unitmanager worden ze geïnformeerd over procedures en werkwijzen en passen de regels en uitgangspunten hieruit toe in de uitvoering van de werkzaamheden.

4.3 Functies IV&P
Binnen de RSD zijn de rollen en functies met betrekking tot privacy en informatieveiligheid geclusterd in het team informatieveiligheid en privacy, het IV&P-team. Iedere rol en/of functie komt met eigen verantwoordelijkheden en taken afkomstig uit wettelijke bepalingen, welke zijn afgestemd op de dagelijkse praktijk.

- **Functionaris gegevensbescherming**
  De functionaris gegevensbescherming is verantwoordelijk voor het toezicht op de naleving van de AVG, de UAVG, de Wpg en andere relevante privacywetgeving relevante privacywetten en -regels. De functionaris gegevensbescherming informeert de verwerkingsverantwoordelijke en haar medewerkers over hun verplichtingen die voortvloeien uit deze wet- en regelgeving en geeft gevraagd en ongevraagd advies in de gehele organisatie. De functionaris gegevensbescherming legt verslag af over de stand van zaken ten aanzien van privacy bij de organisatie (zie paragraaf 4.4). Eindverantwoordelijkheid voor een veilige omgang met en beveiliging van persoonsgegevens ligt nimmer bij de functionaris gegevensbescherming, maar ligt altijd in de lijn (integrale verantwoordelijkheid).

7) Dit is geregistreerd in het register van verwerkingen

- **Privacy officer**
  De privacy officer is verantwoordelijk voor het vormgeven en bewaken van het privacybeleid en onderliggende plannen, procedures en richtlijnen en draagt zorg voor het waarborgen van de privacy binnen de organisatie. De privacy officer is het aanspreekpunt van de organisatie op het gebied van privacy en ondersteunt onder andere bij het uitwerken van afdelingsspecifieke werkinstructies, het behandelen en melden van datalekken, het inrichten van werkprocessen, het uitvoeren van DPIA's, het afhandelen van verzoeken van rechten van betrokkenen.
- **Chief information security officer**
  De chief information security officer is verantwoordelijk voor het vormgeven, bewaken, implementeren en naleven van het informatieveiligheidsbeleid en onderliggende plannen, procedures en richtlijnen. De chief information security officer is het aanspreekpunt in de organisatie op het gebied van informatiebeveiliging en ondersteunt onder andere bij de aanschaf van nieuwe (informatie)systemen, het in kaart brengen van risico's bij (nieuwe) verwerkingen en de implementatie van maatregelen die dergelijke risico's beperken.
- **Informatieambassadeurs**
  In elke unit zijn twee informatieambassadeurs aangewezen. De informatieambassadeur fungeert als eerste aanspreekpunt binnen diens unit als het gaat om informatieveiligheid- en privacyvraagstukken en is de schakel tussen de unit en de functionaris gegevensbescherming/privacy officer. De informatieambassadeur signaleert incidenten, datalekken en wijzigingen in processen en geeft dit door aan de functionaris gegevensbescherming, de privacy officer en/of de chief information security officer.

4.4 Toezicht op de naleving

De functionaris gegevensbescherming is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de richtlijnen op het gebied van privacy. Er zijn verschillende momenten waarop de functionaris gegevensbescherming rapporteert over de werkzaamheden en resultaten van de organisatie rondom privacy en informatiebeveiliging.

- **Jaarplan**
  In het privacybeleid worden de uitgangspunten en verantwoordelijkheden rondom privacy en informatiebeveiliging uiteengezet. In het jaarplan worden de acties en doelen voor een specifiek jaar uitgewerkt. Dit plan is afgestemd op het jaarverslag van de functionaris gegevensbescherming en relevante ontwikkelingen en dreigingen in het werkveld.
- **Periodieke rapportages**
  Periodiek worden rapportages voorgelegd aan de directeur en het managementteam met betrekking tot de implementatie van privacy in de organisatie. Door te rapporteren via de bestaande P&C-cyclus wordt het managementteam op de hoogte gehouden van de ontwikkelingen op gebied van privacy en informatiebeveiliging.
- **Jaarverslag functionaris gegevensbescherming**
  In het jaarverslag van de functionaris gegevensbescherming wordt verantwoording afgelegd over de naleving van de privacywetgeving door de organisatie. Dit verslag wordt jaarlijks voorgelegd aan het dagelijks bestuur.

Met behulp van bovenstaande controlemomenten wordt gestuurd op het zorgvuldig en rechtmatig omgaan met persoonsgegevens. Vanuit het IV&P team wordt dit gecontroleerd, onder toezicht van de functionaris gegevensbescherming.

5 Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG en de Wpg verschillende rechten. Met deze rechten kunnen zij controle uitoefenen op de verwerking van hun persoonsgegevens door de RSD. De werkwijze voor het afhandelen van een verzoek is vastgelegd in de procedure 'Rechten van betrokkenen'. Hieronder zijn de uitgangspunten aangaande deze rechten beschreven.

5.1 De rechten van betrokkenen AVG[8]

Betrokkenen hebben onder de AVG de volgende rechten:

1. recht op inzage;
2. recht op rectificatie (wijzigen en aanvullen);
3. recht op vergetelheid (verwijderen);
4. recht op beperking van de verwerking;
5. recht op dataportabiliteit (overdragen);
6. recht op bezwaar tegen de verwerking;

8) Art. 15 t/m 18 en 20 t/m 22 AVG

7. recht om niet te worden onderworpen aan geautomatiseerde besluitvorming en profilering.

Naast deze rechten hebben betrokkenen recht op duidelijke informatie over de verwerking van hun persoonsgegevens, mogen zij eerder gegeven toestemming voor het verwerken van bepaalde persoonsgegevens intrekken en hebben ze het recht op het indienen van een klacht bij de Autoriteit Persoonsgegevens als de verwerking een inbreuk maakt op de AVG.

5.2 De rechten van betrokkenen Wpg[9]
Indien persoonsgegevens van een betrokkene zijn gebruikt in het kader van een strafrechtelijk onderzoek, dan heeft de betrokkene in ieder geval het recht op inzage in deze gegevens. In bepaalde gevallen heeft de betrokkene tevens recht op rectificatie, het aanvullen of het wissen van de gegevens.

5.3 Indienen verzoek
Een verzoek in het kader van de rechten van betrokkenen kan op verschillende manieren worden ingediend. De werkwijze met betrekking tot het indienen van een verzoek is toegelicht op de website. Uitgangspunt bij het indienen van een verzoek is dat deze schriftelijk wordt ingediend.

- **Formulier website**
  De eerste manier voor het indienen van een verzoek is via een DigiD-formulier op de website. Betrokkene kan hier de gegevens betreffende het verzoek invullen en kan door middel van DigiD direct ondertekenen. In het geval van deze stap kan de stap tot het identificeren van de betrokkene worden overgeslagen.
- **E-mail/post**
  Verzoeken kunnen tevens worden ingediend bij de functionaris gegevensbescherming, via de e-mail of per post.
- **In persoon**
  Tot slot kunnen verzoeken persoonlijk afgeleverd worden op het kantoor van de RSD.

5.4 Inhoudelijke beoordeling verzoek
Na ontvangst van het verzoek vindt een inhoudelijke beoordeling van het verzoek plaats. Allereerst wordt gekeken of de RSD aan het verzoek van betrokkene kan voldoen, of dat het verzoek op grond van de AVG of andere relevante wet- en regelgeving afgewezen moet worden. Dit laatste is het geval wanneer het verzoek in strijd is met de wettelijke plicht om gegevens te verwerken, bijvoorbeeld het bewaren van persoonsgegevens op basis van de Archiefwet. Bij een verzoek op basis van de Wpg kan een verzoek tot inzage bijvoorbeeld worden afgewezen als dit nadelige gevolgen heeft voor de openbare veiligheid.

5.5 Afhandeling verzoek AVG
De RSD reageert binnen een maand na binnenkomst op het verzoek van de betrokkenen. In uitzonderlijke gevallen zal de RSD binnen drie maanden reageren op het verzoek. Indien dit het geval is, wordt de betrokkene in ieder geval binnen een maand van deze keuze schriftelijk op de hoogte gebracht. Er zijn verschillende routes voor het afhandelen van een verzoek mogelijk:

- **Er wordt voldaan aan het verzoek tot inzage**
  Als de functionaris gegevensbescherming tot het oordeel komt dat een verzoek om inzage moet worden toegewezen, wordt een kopie gemaakt van de persoonsgegevens die worden verwerkt en wordt de informatie op een veilige manier verstrekt aan de betrokkene[10]. Voor het verzamelen van de juiste informatie schakelt de functionaris gegevensbescherming de betreffende units/medewerkers in die toegang hebben tot de benodigde informatie. De unitmanager is verantwoordelijk voor het beschikbaar stellen van de informatie door de medewerkers en de tijd die met de verzameling van deze informatie gemoeid gaat.
- **Er wordt voldaan aan overige verzoeken**
  Indien wordt voldaan aan het verzoek gegevenswissing, dataportabiliteit, wijziging of aanvulling van gegevens, beperking van de verwerking of bezwaar zijn specifieke handelingen en medewerkers nodig per proces. Per verzoek wordt bepaald hoe aan dergelijke verzoeken kan worden voldaan.
- **Er wordt niet voldaan aan het verzoek van de betrokkene**
  Indien de functionaris gegevensbescherming na beoordeling tot de conclusie komt dat het verzoek moet worden afgewezen, deelt zij dit schriftelijk gemotiveerd met de betrokkene. De privacy officer ontvangt hiervan een afschrift.

9) **Art. 24a, 24b, 25 en 28 Wpg**
10) artikel 15 lid 1 AVG

5.6 Afhandeling verzoek Wpg

- De RSD reageert uiterlijk binnen zes weken na binnenkomst op inzageverzoeken op basis van de Wpg. Een inzageverzoek wordt toegekend onder de voorwaarde dat er geen uitzonderingen van toepassing zijn en het verzoek niet ongegrond of buitensporig is.
- De RSD reageert uiterlijk binnen vier weken op rectificatie-/vernietigingsverzoek. Dergelijke verzoeken worden toegekend onder de voorwaarde dat de gegevens onjuist of onvolledig zijn, onrechtmatig worden verwerkt, er geen uitzonderingen van toepassing zijn en het verzoek niet ongegrond of buitensporig is.

Bijlage 1 Verwerking van politiegegevens

In aanvulling op het algemene beleid, vraagt de omgang met politiegegevens extra zorgvuldigheid van ons als organisatie. Politiegegevens zijn persoonsgegevens die worden verwerkt door de daarvoor aangewezen Buitengewoon opsporingsambtenaar (Boa) in het kader van een strafrechtelijk onderzoek. Om ervoor te zorgen dat we zo zorgvuldig mogelijk omgaan met deze politiegegevens en deze zo goed mogelijk beschermen, leggen we onderstaande uitgangspunten vast ter aanvulling op het huidige privacybeleid.

Algemene uitgangspunten

1. Als raamwerk voor beheersmaatregelen wordt het door Wpg-auditoren gehanteerde raamwerk gehanteerd, zoals dat is opgenomen in bijlage 3 en 4 van de NOREA Handreiking Privacy audit Wet politiegegevens voor boa's.
2. Bij gebruik van een informatiesysteem dat wordt beheerd door een leverancier (bijvoorbeeld SaaS) wordt een verwerkersovereenkomst afgesloten en levert de leverancier een Third Party Memorandum (TPM) aan.
3. Voor elke verwerking van politiegegevens wordt een DPIA uitgevoerd en deze wordt elke drie jaar herzien. Daarin worden de volgende principes getoetst en geborgd:
   - gegevensbescherming door beveiliging en ontwerp;
   - gegevensbescherming door standaard-instellingen.

4. De RSD verwerkt politiegegevens op basis van:
   - artikel 9 Wpg (onderzoek in een bepaald geval) en verleent de boa medewerking aan onderzoeken onder verantwoordelijkheid van de politie of andere opsporingsdiensten;
   - art. 15-21 en 23-24 Wpg (ter beschikking stellen en verstrekking van politiegegevens).

5. De RSD verwerkt geen politiegegevens op basis van:
   - art. 8 Wpg (uitvoering van de dagelijkse politietaak);
   - art. 11 Wpg (geautomatiseerd vergelijken en in combinatie zoeken t.b.v. een art. 9 onderzoek);
   - art. 13 Wpg (ondersteunende taken, zoals bijvoorbeeld het landelijke register bijtincidenten);
   - art. 17a Wpg (doorgifte aan derde landen, d.w.z. landen buiten de Europese Economische Ruimte);
   - art 7a Wpg (geautomatiseerde besluitvorming, waaronder profilering).

6. Toegangsbeveiliging is zodanig ingericht dat alleen boa's en geautoriseerden toegang hebben tot politiegegevens.
7. Bij de verzending van politiegegevens worden deze altijd versleuteld verstuurd via Zivver.
8. Betrokkenen worden geïnformeerd over de verwerking van politiegegevens via de website en, indien van toepassing, bij de eerste brief die zij ontvangen over strafrechtelijke handhaving.

Rollen, taken en bevoegdheden

1. De **privacy officer** inventariseert jaarlijks of het bereik van de verwerkingen met politiegegevens is gewijzigd. Op basis daarvan worden het privacybeleid, de procedures voor het melden van datalekken en de rechten van betrokkenen en het register van verwerkingen indien nodig aangepast.
2. De **unitmanager I&S** is verantwoordelijk voor de implementatie en uitvoering van de Wpg en heeft in dat kader onder andere de volgende taken en bevoegdheden:
   - onder de aandacht brengen van de handreiking/gedragsregels voor boa's bij de medewerkers en het toezien op naleving van deze gedragsregels;
   - nemen van autorisatiebesluiten in de zin van art. 6 lid 3, 4 en 5 Wpg, met behulp van het formulier 'autorisatie verwerking politiegegevens';
   - besluiten over toegang tot informatiesystemen met politiegegevens, waaronder het vaststellen van de autorisatiematrix en de controle hierop door de ICT-Regisseur.

3. De **security officer** is verantwoordelijk voor de controle op de toegang tot politiegegevens en heeft hierin onder andere de volgende taken:
   - controleert autorisatiebesluiten en aanvragen voor toegang tot informatiesystemen met politiegegevens, door deze te verifiëren bij de bevoegd functionaris;
   - analyseert de log-bestanden en documenteert de bevindingen.

4. De **functioneel beheerder** kent de aangevraagde autorisaties voor politiegegevens toe op aanwijzing van de security officer.
5. De **ICT-Regisseur** heeft in het kader van de Wpg de volgende taken:
   - bewaakt de beveiliging van de applicatie en de afspraken die hierover zijn gemaakt met leverancier(s);
   - coördineert de interne en externe Wpg-audits;

- houdt een overzicht bij met geautoriseerden en controleert deze op juistheid en volledigheid.

6. De rol van **bevoegd functionaris** is toegewezen aan de Boa die het langst in dienst is. Deze heeft de volgende taken:
   - zorgen dat de extra eisen aan art. 9 Wpg verwerkingen worden nageleefd, zoals documentatie van doel, noodzakelijkheid, herkomst van gegevens en correcte vastlegging van gegevens;
   - overleg met de OvJ;
   - bijhouden van een lijst met veelvoorkomende verstrekkingen met daarbij de onderbouwing van de grondslag voor de verstrekking;
   - waarborgen van de bewaartermijnen voor art. 9 Wpg gegevens:
     - binnen ½ jaar na de veroordeling van de dader of de verjaring van het delict de gegevens verwijderen, dat wil zeggen alleen beschikbaar zijn voor audits en klachtenprocedures;
     - vijf jaar daarna de gegevens vernietigen;
   - goedkeuring van de autorisatie van personen;
   - toezien op rechtmatige verkrijging van gegevens, doelbinding etc.;
   - instemmen met terbeschikkingstellingen (gebruik voor een ander onderzoek) en verstrekkingen van art. 9 Wpg gegevens;
   - hergebruik van informatie inregelen.

7. De **functionarisgegevensbescherming**:
   - adviseert en informeert over de Wpg, onder andere over DPIA's;
   - is contactpersoon voor en werkt samen met de AP;
   - houdt toezicht op de uitvoering van de Wpg en voert daartoe jaarlijks controles uit volgens het vastgestelde controleplan Wpg;
   - stelt op basis van bovengenoemd controleplan Wpg jaarlijks een verslag op met bevindingen.