Gegevensbeschermingsbeleid (Privacy beleid)

Colofon

Contactpersoon [redacted] privacy@nipv.nl

Datum 30 september 2024
Status Definitief
Versie 1.0

Het Nederlands Instituut Publieke Veiligheid is bij wet vastgelegd onder de naam Instituut Fysieke Veiligheid.

Bestuurlijke samenvatting

het NIPV hecht grote waarde aan het recht op eerbiediging van privé-, familie- en gezinsleven zoals opgenomen in het Europees Verdrag voor de Rechten van de Mens (EVRM) en in de Grondwet.
Hieruit volgend hecht het NIPV dan ook grote waarde aan de gegevensbescherming, zoals opgenomen in de Algemene Verordening Gegevensbescherming (AVG).

Visie op gegevensbescherming

De verwerking van persoonsgegevens is een essentieel onderdeel van de taakuitvoering van het NIPV. De verwerking van gegevens gaat gepaard met de verantwoordelijkheid om effectieve bescherming van gegevens te bieden. Het uitgangspunt hierbij is, dat we respect hebben voor de persoonlijke levenssfeer van alle betrokkenen. Daarbij houdt het NIPV zich aan de wettelijke regels op het gebied van de verwerking van de persoonsgegevens.

Het doel van dit gegevensbeschermingsbeleid is om formeel invulling te geven aan de manier waarop binnen het NIPV wordt omgegaan met privacy en gegevensbescherming en om bestuurlijk de randvoorwaarden vast te leggen voor verdere uitwerking van dit beleid.

Het hoger management (Directie en MT) is ambtelijk verantwoordelijk voor de juiste gegevensbescherming en informatiebeveiliging, waarbij de directeur ambtelijk eindverantwoordelijk is. Echter beperkt deze verantwoordelijkheid zich niet enkel tot het management. Zorgvuldige gegevensbescherming en -verwerking geldt voor iedereen die binnen het NIPV werkzaam is. Het NIPV draagt zorg voor- en investeert in- de beveiliging van de persoonsgegevens in technische, fysieke en organisatorische zin. Betrokkenen kunnen altijd gebruik maken van hun rechten.

Met dit beleid wordt het gegevensbeschermingsbeleid in lijn gebracht met de nieuwste inzichten ten aanzien van gegevensbescherming en informatiebeveiliging. Dit beleid is opgesteld met inachtneming van het verkennend onderzoek dat de Autoriteit Persoonsgegevens heeft gedaan naar gegevensbeschermingsbeleid. Het omgaan met persoonsgegevens wordt organisatie breed op uniforme wijze bepaald en formeel vastgesteld.

Waar eerder nog het voldoen aan de wet het uitgangspunt was, is dit beleid gestoeld op het beperken en voorkomen van de risico’s voor betrokkenen en de organisatie. Daarbij is er nog steeds alle ruimte om gegevens te verwerken, maar wordt aan de voorkant nagedacht over de risico’s die dat met zich meebrengt en de maatregelen die nodig zijn om die risico’s te mitigeren.

De toegenomen digitalisering van de samenleving brengt nieuwe risico’s met zich mee. De rechten van betrokken worden daarmee navenant belangrijker. In dit beleid is dan ook uitgebreid aandacht voor de rechten van betrokkenen en hoe ze die kunnen uitvoeren. Functies en verantwoordelijkheden op het gebied van gegevensbescherming worden in dit beleid vastgelegd. Van algemeen bestuur tot aan de medewerker.

Voorwoord

Binnen het Nederlands Instituut Publieke Veiligheid (NIPV) wordt gewerkt met persoonsgegevens van medewerkers, (keten)partners en burgers. Persoonsgegevens worden voornamelijk verzameld voor het uitvoeren van de wettelijke taken van het NIPV. De betrokken personen en instanties moeten erop kunnen vertrouwen dat het NIPV zorgvuldig en veilig met de persoonsgegevens omgaat. In deze tijd gaat ook het NIPV mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. Het NIPV is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy. Het NIPV geeft door middel van dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van het NIPV. Dit privacy-beleid van het NIPV is in lijn met de relevante nationale en Europese wet- en regelgeving.

In dit beleid staan kaders beschreven voor het verwerken en het beschermen van persoonsgegevens en de omgang met deze gegevens. In gevallen waarin dit beleid niet voorziet, beslist de centrummanager Staf of de Directie. Dit beleid geldt niet enkel ten aanzien van de medewerkers van het NIPV en derden die betrokken zijn bij de gegevensverwerking, maar ook ten aanzien van alle natuurlijke personen waarvan het NIPV over gegevens beschikt. Om het beschermen van persoonsgegevens te borgen is een adequate informatiebeveiliging beschikbaar. Hiervoor wordt verwezen naar het Integraal Beveiligingsbeleid zoals dit binnen het NIPV geformaliseerd is.

Dit gegevensbeschermingsbeleid treedt in werking na vaststelling door het algemeen bestuur van het NIPV. Het beleid wordt periodiek geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden aangekondigd via het intranet van het NIPV en in de interne communicatie.

Inhoudsopgave

1 Inleiding 5
1.1 Visie op gegevensbescherming 5
1.2 Reikwijdte 5
1.3 Juridisch kader 6
1.4 Begripsbepalingen 6

2 Organisatie 11
2.1 De wettelijke verantwoordelijkheden 11
2.2 Verantwoording 11
2.3 Organisatorische borging 11
2.4 Sturing en monitoring 11

3 Uitgangspunten zorgvuldige gegevensbescherming 13
3.1 Omgaan met persoonsgegevens 13
3.2 Categorieën persoonsgegevens en categorieën betrokkenen 13
3.3 Rechtmatige grondslag van de verwerking 14
3.4 Verkrijging van gegevens 15
3.5 Toegang tot en verstrekking van persoonsgegevens 15
3.6 Gebruik van gegevens voor onderzoek en statistische doelen 16
3.7 Doorgifte buiten de EU/ EER 16

4 Bescherming van gegevens 18
4.1 Data Protection Impact Assessment (DPIA) 18
4.2 Dataminimalisatie 18
4.3 Bewaren en vernietigen van gegevens 18
4.4 Dataclassificatie 19
4.5 Logging van gegevensgebruik 19
4.6 Verwerkersovereenkomst 19
4.7 Bewust omgaan met persoonsgegevens 19
4.8 Meldplicht voor inbreuken in verband met persoonsgegevens (datalekken) 20

5 Rechten van betrokkenen 21
5.1 Rechten van betrokkenen 21
5.2 Recht op informatie en toegang tot gegevens 21
5.3 Recht op inzage en afschrift van gegevens 21
5.4 Recht op rectificatie (correctie, aanvulling) van gegevens 22
5.5 Recht op gegevenswissing 22
5.6 Recht op beperking van de verwerking 23
5.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit) 23
5.8 Recht van bezwaar tegen verwerking 23
5.9 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming waaronder profilering 23
5.10 Klachten en vragen 24
5.11 Informeren van (keten)partners 24

6 Functies en verantwoordelijkheden 25

7 Formeel toezicht op de gegevensverwerking 29

1. Inleiding

Het NIPV hecht grote waarde aan het recht op eerbiediging van privé-, familie- en gezinsleven zoals opgenomen in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en in de grondrechten van Nederland, artikel 10 van de Grondwet:

Europees Verdrag voor de Rechten van de Mens, artikel 8

1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Grondwet, artikel 10

1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Hieruit volgend hecht het NIPV dan ook grote waarde aan de gegevensbescherming, zoals opgenomen in de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)

1.1 Visie op gegevensbescherming

De verwerking van persoonsgegevens is een essentieel onderdeel van de taakuitvoering van het NIPV. De verwerking van gegevens gaat gepaard met de verantwoordelijkheid om effectieve bescherming van gegevens te bieden. Hierbij is het uitgangspunt dat we respect hebben voor de persoonlijke levenssfeer van alle betrokkenen. Daarbij houdt NIPV zich aan de wettelijke regels op het gebied van de verwerking van de persoonsgegevens.

1.2 Reikwijdte

Dit beleid is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens binnen het NIPV. Daarnaast is het van toepassing op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen. De kaders die in dit beleid staan beschreven gelden voor iedereen (zowel interne als externe verwerkers) die namens het NIPV gegevens verwerken.
Wanneer in dit document gesproken wordt over het NIPV wordt bedoeld de gehele organisatie van het NIPV, waaronder in ieder geval begrepen:

- Bestuur en Directie
- Staf
- Bureau TEC
- Veiligheidsregio Diensten Centrum (VDC)
- Centrum Ondersteuning Landelijke Slagkracht (COLS)
- NL Academie voor Crisisbeheersing en Brandweerzorg (NACB)
- Centrum voor Opleiding en Vorming Brandweer (COVB)
- Individuele Programma’s en Projecten

1.3 Juridisch kader

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Er moet voorkomen worden dat er onnodig inbreuk wordt gemaakt. De Algemene Verordening Gegevensbescherming (AVG) welke sinds 25 mei 2018 van kracht is, biedt hiervoor het wettelijk kader. De AVG heeft als doel om de privacy van burgers in Europa beter te beschermen. In de Uitvoeringswet Algemene Verordening Gegevensbescherming is een nadere uitwerking vastgelegd.
Daarnaast is er specifieke wetgeving van kracht waarin ook een kader voor privacy is weggelegd, zoals in de zorg. Bij dit beleid wordt onder meer in aanmerking genomen:

- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG);
- Burgerlijk Wetboek (BW);
- Wet op de Veiligheidsregio's (WVr)
- Wet houdende regels inzake de telecommunicatie (Telecommunicatiewet)
- Belastingwet
- Aanbestedingswet
- De Europese e-Privacy verordening
- Wet open overheid (Woo)
- Archiefwet
- Nieuwe Europese regelgeving waaronder:
    - AI-Act
    - NIS2
    - CER

Het doel van dit gegevensbeschermingsbeleid is om invulling te geven aan de manier waarop binnen het NIPV wordt omgegaan met privacy en gegevensbescherming.
Als algemene regel geldt dat persoonsgegevens binnen NIPV op een zorgvuldige wijze moeten worden verwerkt. Persoonsgegevens moeten rechtmatig, op behoorlijke wijze en transparant zijn verkregen en mogen enkel en alleen voor een specifiek beschreven doel worden verwerkt. Het NIPV verwerkt niet meer persoonsgegevens dan nodig en bewaakt de juistheid, de integriteit en de vertrouwelijkheid. Daarbij geldt dat deze gegevens niet langer mogen worden bewaard dan noodzakelijk om het doel waarvoor ze zijn verzameld, te realiseren of om aan wettelijke verplichtingen te voldoen. Het NIPV draagt zorg voor beveiliging van de persoonsgegevens in technische, fysieke en organisatorische zin. De betrokkenen kunnen altijd gebruik maken van hun rechten op informatie, om in te zien, te wijzigen, vergeten te worden of gegevens over te dragen. Dit wordt in de volgende hoofdstukken nader uitgewerkt.

1.4 Begripsbepalingen

Anonimiseren
Persoonsgegevens die voor een taakuitvoering niet meer noodzakelijk zijn, worden verwijderd uit een dataset. De dataset bevat dan enkel geanonimiseerde gegevens, die wel worden bewaard voor bijvoorbeeld onderzoeksdoeleinden of om te gebruiken als open data. Geanonimiseerde gegevens zijn geen persoonsgegevens en vallen niet onder dit beleid. Het anonimiseren zelf is een verwerking en valt wel onder dit beleid.

Autoriteit Persoonsgegevens
De Nederlandse toezichthouder die tot taak heeft toe te zien op de verwerking van persoonsgegevens overeenkomstig de Algemene Verordening Gegevensbescherming.

AVG
Algemene Verordening Gegevensbescherming of in het Engels binnen de EU: General Data Protection Regulation (GDPR)

Beheerder
Degene die binnen de organisatie belast is met de inrichting en de beveiliging van een systeem, bestand of een verzameling van bestanden binnen een organisatieonderdeel.

Bestand
Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functionele of geografische wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op één of meer verschillende natuurlijke personen.

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft.

Bijzondere persoonsgegevens
Persoonsgegevens ten aanzien van:

- Ras of etnische afkomst
- Politieke opvattingen
- Religie of levensbeschouwing
- Lidmaatschap van vakvereniging of vakbond
- Gezondheid
- Seksueel gedrag of gerichtheid
- Genetische gegevens
- Biometrische gegevens ten aanzien van unieke identificatie

CIO Office
Een office, waarbinnen verschillende functionarissen samenwerken met als doel de integrale samenwerking op complexere vraagstukken, het wendbaar organiseren van de IV/ICT-faciliteiten en aan het bewaken van de complexe IV/ICT-infrastructuur vorm te geven

Datalek
Een situatie of gebeurtenis die onbevoegd of onopzettelijk leidt tot een inbreuk op de vertrouwelijkheid, op de integriteit of op de beschikbaarheid van persoonsgegevens.

- Inbreuk op de vertrouwelijkheid
  Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
- Inbreuk op de integriteit
  Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
- Inbreuk op de beschikbaarheid
  Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

Afhankelijk van de ernst van het datalek bestaat de verplichting om binnen 72 uur een melding daarvan te doen bij de Autoriteit Persoonsgegevens.

Dataminimalisatie
Bij het verzamelen en verwerken van persoonsgegevens mogen niet meer gegevens worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken.

Data Protection Impact Assessment (DPIA)
Een instrument om de privacy risico's in kaart te brengen wanneer er sprake is van een verwerking van persoonsgegevens. Ook wel genoemd Gegevensbeschermingseffectbeoordeling (GEB) of Privacy Impact Assessment (PIA). In gevallen met een hoog risico is een DPIA verplicht. Het NIPV gebruikt een DPIA-toets (pré-DPIA) om na te gaan of een DPIA nodig is.

Derde
Ieder ander dan de betrokkene, de verantwoordelijke, de verwerker, of degene(n) die onder gezag van de verantwoordelijke of de verwerker gemachtigd is (zijn) om persoonsgegevens te verwerken.

Directie
De Directeuren

Directie en MT (Hoger Management)
Directie, centrummanagers en afdelingshoofden

Eigenaar
De leidinggevende die binnen de organisatie de verantwoordelijkheid heeft voor de inrichting en de beveiliging van een systeem, bestand of een verzameling van bestanden binnen een organisatieonderdeel.

Gebruiker
Degene die geautoriseerd is gegevens in een persoonsregistratie in te voeren en/of te muteren, dan wel van enigerlei uitvoer van de persoonsregistratie kennis te nemen.

Gevoelige persoonsgegevens
Persoonsgegevens die in hun aard gevoelig zijn en extra voorzichtigheid behoeven. Daaronder in ieder geval alle bijzondere- en strafrechtelijke persoonsgegevens, maar ook gewone persoonsgegevens ten aanzien van minderjarigen, unieke identificatiegegevens, zoals BSN en DigiD, specifieke financiële gegevens etc.

Gewone persoonsgegevens
Alle persoonsgegevens niet zijnde Bijzondere of Strafrechtelijke persoonsgegevens

Gezondheidsgegevens
Alle gegevens die op enige wijze gaan over de fysieke of mentale gezondheid van een natuurlijk persoon of daarnaar te herleiden zijn. Gezondheidsgegevens vallen onder de bijzondere persoonsgegevens. Zie ook: Medische gegevens.

Least Privilege
Gebruikers hebben alleen toegang tot de informatie en middelen die nodig zijn voor de uitvoering van aan hun toebedeelde taken.

Medische gegevens
Onder-categorie van gezondheidsgegevens. Medische gegevens zijn gezondheidsgegevens die naar aard de van de gegevens voorbestemd zijn om door zorgverleners verwerkt te worden. Binnen het NIPV worden geen medische gegevens verwerkt, behoudens wettelijke verplichtingen daartoe en behoudens ten behoeve van de GHOR gebruikte gegevens die verwerkt worden door een daartoe bevoegde en geregistreerde medewerker in het kader van de wettelijke taken.

Ontvanger
Degene aan wie de persoonsgegevens worden verstrekt.

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is

Pseudonimiseren
Pseudonimiseren is een procedure waarmee identificerende gegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem). Het algoritme kan voor een persoon altijd hetzelfde pseudoniem berekenen, waardoor informatie over de persoon, ook uit verschillende bronnen, kan worden gecombineerd. Daarin onderscheidt pseudonimiseren zich van anonimiseren, waarbij het koppelen op persoon van informatie uit verschillende bronnen niet mogelijk is. Pseudonieme gegevens vallen onder de werking van dit beleid.

Strafrechtelijke persoonsgegevens
Persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. Of met veiligheidsmaatregelen die daarmee verband houden.

Taakverantwoordelijke
Diegene die verantwoordelijk is voor of belast is met de uitvoering van een bepaalde taak.

Team Privacy
De samenwerking van functionaris gegevensbescherming en privacy officer.

Toestemming van betrokkene
Elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat zijn persoonsgegevens worden verwerkt. Deze toestemming moet vrij en ondubbelzinnig zijn. Dat betekent dat betrokkenen in vrijheid hun wil moeten kunnen uiten. Ook mag er geen twijfel zijn of betrokkenen hun toestemming hebben gegeven en voor welke specifieke verwerking zij dit hebben gedaan. Er zijn geen vormvereisten voor de toestemming, maar omdat er geen twijfel mag bestaan is het aan te bevelen om geen mondeling toestemming te gebruiken als deze niet wordt opgenomen.

Nederlands Instituut Publieke Veiligheid (NIPV)
Het rechtspersoonlijkheid bezittend openbaar lichaam met die naam, ingesteld op grond van de Wet gemeenschappelijke regelingen en de Wet veiligheidsregio's. De Algemene Verordening Gegevensbescherming is van toepassing op alle gegevensverwerkingen binnen het NIPV.

Verstrekken van persoonsgegevens
Het bekend maken of ter beschikking stellen van persoonsgegevens.

Verwerker
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt" (artikel 4, lid 8 AVG)

Verwerkingsregister
Een overzicht van alle verwerkingen van persoonsgegevens die plaatsvinden binnen het NIPV. Het register dient actueel te zijn en wordt dus aangepast zodra verwerkingen worden aangepast of wanneer sprake is van nieuwe verwerkingen. Ten minste jaarlijks vindt een review plaats.

Verwerkingsverantwoordelijke
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van- en de middelen voor de verwerking van persoonsgegevens vaststelt'' (artikel 4, lid 7 AVG).
Binnen het NIPV is het dagelijks bestuur van het NIPV bestuurlijk verantwoordelijk.

Verwerking van persoonsgegevens
Elke handeling of geheel van handelingen met betrekking tot persoonsgegevens al dan niet handmatig dan wel geautomatiseerd uitgevoerd, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, anonimiseren, pseudonimiseren, uitwissen of vernietigen van gegevens.

2. Organisatie

2.1 De wettelijke verantwoordelijkheden

De manier waarop dit beleid binnen het NIPV wordt verankerd, vormt het fundament van de privacy borging. Het hoger management (Directie en MT) is ambtelijk verantwoordelijk voor juiste gegevensbescherming en informatiebeveiliging. Echter beperkt deze verantwoordelijkheid zich niet enkel tot het management. Zorgvuldige gegevensbescherming en -verwerking geldt voor iedereen die binnen NIPV werkzaam is. Het niet in acht nemen van privacyregels of ernstige schending daarvan kan leiden tot sancties.

Het NIPV is verplicht een gegevensbeschermingsbeleid op te stellen als dat in verhouding staat tot de verwerkingsactiviteiten. Dat is afhankelijk van de aard, de omvang, de context en het doel van de gegevensverwerking. Het NIPV is van mening dat een goed gegevensbeschermingsbeleid belangrijk is. De wet legt een verantwoordingsplicht op aan het NIPV. Dit beleid past daarin.

2.2 Verantwoording

Het hoger management is verantwoordelijk voor de juiste naleving van de AVG en het beleid op het gebied van de gegevensbescherming. Naast het jaarlijkse verantwoorden hebben zowel het management als de Functionaris Gegevensbescherming de plicht om het dagelijks bestuur te informeren over bijzonderheden en ernstige incidenten ten aanzien van gegevensbescherming.

2.3 Organisatorische borging

De centrummanagers en afdelingshoofden zijn verantwoordelijk voor de borging van de uitganspunten van dit beleid binnen hun werkprocessen. Het borgen van de privacy is hierbij onlosmakelijk verbonden met het integraal beveiligingsbeleid NIPV. Het NIPV beschikt over een Functionaris Gegevensbescherming (FG) en over een Privacy Officer (PO). De taken en positie van functionarissen is verder uitgewerkt in hoofdstuk 6. Beide functionarissen worden in de gelegenheid gesteld om in het kader van hun functie opleidingen, cursussen en certificering te volgen om zich te bekwamen, bekwaam te blijven en ontwikkelingen op het gebied van privacy en gegevensbescherming bij te houden.

2.4 Sturing en monitoring

Met een reeks maatregelen wordt geborgd dat er continu gewerkt wordt aan het optimaliseren en borgen van de kwaliteit van de werkprocessen waarbij privacy een rol speelt. Elke centrummanager en elk afdelingshoofd is zelfstandig verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar werkprocessen plaatsvindt. Het is daarom ook hun verantwoordelijkheid om te monitoren of persoonsgegevens zorgvuldig verwerkt worden en dit zo nodig bij te sturen. Daarnaast zijn zij verplicht om incidenten te melden bij team Privacy. De FG heeft de verantwoordelijkheid om structureel te toetsen of de wettelijke eisen en richtlijnen op het gebied van gegevensbescherming zijn geïmplementeerd, worden uitgevoerd, en te adviseren omtrent privacy en gegevensbescherming. De PO adviseert en ondersteunt de organisatie bij de uitvoering van de wettelijke eisen en richtlijnen.
Juist omdat gegevensbescherming voor een belangrijk deel mensenwerk is, moet op alle niveaus binnen NIPV over gegevensbescherming worden nagedacht. Door dit onderwerp vast op de diverse agenda's te plaatsen, ontstaat een continu proces van veranderen en verbeteren. Door vanuit verschillende niveaus en rollen binnen NIPV naar de kwaliteit van de

uitvoering van privacy te kijken, ontstaat een evenwichtig systeem. De belangrijkste elementen van deze borging zijn:

- Vaststellen van dit beleid
- Uitvoering van dit beleid
- Gegevensbescherming als onderwerp in werkoverleggen
- Toezicht op gegevensbescherming
- Gegevensbescherming in het plan- en control proces (PDCA)
- Interne (en externe) audit

3. Uitgangspunten voor een zorgvuldige gegevens-bescherming

3.1 Omgaan met persoonsgegevens

Persoonsgegevens worden bij het NIPV in overeenstemming met de wet en op zorgvuldige wijze verwerkt. Dit houdt in dat persoonsgegevens alleen voor specifieke, uitdrukkelijke en legitieme doeleinden worden verzameld en dat er niet meer persoonsgegevens worden verwerkt dan voor dat doel noodzakelijk zijn. Daarbij wordt tenminste rekening gehouden met de wettelijke grondslag, de aard van de gegevens, de gevolgen van de verdere verwerking voor de betrokkene, de wijze waarop de gegevens zijn verkregen en de gestelde waarborgen ter bescherming van de persoonlijke levenssfeer.
De doeleinden van de verwerking worden binnen het NIPV organisatie breed op uniforme wijze bepaald en formeel vastgesteld.

3.2 Categorieën persoonsgegevens en categorieën betrokkenen

Het NIPV verwerkt persoonsgegevens van verschillende categorieën betrokkenen. In hoofdzaak zijn er drie categorieën betrokken te onderscheiden:

- Medewerkers van het NIPV, waaronder ook inhuur, stagiaires en gedetacheerd personeel
- Medewerkers van derden (in dienst van overheden/bedrijven/ instellingen waar wij mee samen werken).
- Burgers

Het NIPV verwerkt gewone persoonsgegevens, maar in specifieke gevallen ook bijzondere persoonsgegevens.

Medewerkers
Met betrekking tot medewerkers worden zowel gewone persoonsgegevens verwerkt als ook bijzondere persoonsgegevens. Veelal met als doel verplichtingen die samenhangen met werkgeverschap. Onder de categorie medewerkers vallen in ieder geval gegevens zoals:

- Naam en achternaam
- Contactgegevens, adres, telefoon, email
- Nummer van paspoort of de identiteitskaart
- Burgerservicenummer
- Locatiegegevens van mobiele apparatuur
- IP-adres
- Herleidbare gegevens, zoals de locatie van een dienstvoertuig
- Opleiding en oefen gegevens
- Keuringen, assessments
- Functioneren en beoordelen

- Financiële en fiscale gegevens
- Lidmaatschap van een vakbond of vakvereniging
- Gezondheidsgegevens
- Biometrische gegevens ten behoeve van identificatie
- Verklaring omtrent gedrag

Burgers
Met betrekking tot burgers worden in beperkte mate gegevens verwerkt. Het NIPV heeft richting burgers taken op het gebied van voorlichting, kennisdeling, onderzoek, het versterken van veiligheidsbewustzijn en ondersteunende taken op het gebied van hulpverlening, incident- en crisisbeheersing. Gegevens worden meestal verwerkt met als doel het uitvoeren van wettelijke taken of het algemeen belang. In andere gevallen wordt specifiek om toestemming gevraagd. Onder de categorie burgers vallen in ieder geval gegevens zoals:

- Naam en achternaam
- Contactgegevens, adres, telefoon, email
- Gezondheidsgegevens (bij slachtoffers tijdens incidenten)
- Meldingsgegevens
- Gegevens over de aard van de woning
- Kennis en kunde rond veiligheidsbewustzijn

Medewerkers van derden
Hieronder vallen medewerkers zoals contactpersonen van bedrijven, maar ook functionarissen van ketenpartners, zoals veiligheidsregio's, ministeries, politie, defensie, waterschappen, Rijks Kennis Instituten, hogescholen en universiteiten etc. Gegevens worden meestal verwerkt met als doel het uitvoeren van wettelijke taken of het algemeen belang of vanuit afgeleid werkgeverschap. In andere gevallen wordt specifiek om toestemming gevraagd Onder de categorie medewerkers van derden vallen gegevens zoals:

- Naam en achternaam
- Contactgegevens, adres, telefoon, email
- Locatiegegevens van mobiele apparatuur
- IP-adres
- Herleidbare gegevens, zoals de locatie van een dienstvoertuig
- Opleidings- en oefengegevens
- Keuringen, assessments
- Functioneren en beoordelen
- Biometrische gegevens ten behoeve van identificatie
- Verklaring omtrent gedrag

3.3 Rechtmatige grondslag van de verwerking
De verwerking van persoonsgegevens mag alleen gebeuren wanneer er sprake is van een rechtmatige grondslag voor de verwerkingen zoals vastgelegd in artikel 6 AVG:

- De toestemming van de betrokken persoon.
- De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
- De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.
- De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.
- De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Vanuit het NIPV zijn er verschillende grondslagen aan te reiken om gegevens te verwerken. Bij het NIPV gaat het in veel gevallen om het voldoen aan een wettelijke verplichting of worden gegevens verwerkt om een taak van algemeen belang goed te vervullen. Maar ook alle andere grondslagen zijn op specifieke verwerkingen van toepassing. De grondslag voor de verwerking wordt in het verwerkingsregister vastgelegd. De rechtvaardigingsgronden van de verwerking worden binnen het NIPV organisatie breed op uniforme wijze bepaald en formeel vastgesteld

3.4 Verkrijging van gegevens

De persoonsgegevens worden door de betrokkene zelf verstrekt, vanuit een (landelijke) administratie ontsloten of door derden verstrekt. Wat er precies met de verzamelde gegevens gebeurt, is afhankelijk van het doel waarvoor ze verzameld worden. Meestal worden ze in een informatiesysteem opgenomen waar ze alleen toegankelijk zijn voor de medewerkers en ketenpartners die belast zijn met het uitvoeren van een specifieke taak. Gegevens worden niet zonder toestemming van de betrokkene of wettelijke grondslag gedeeld. Informatiesystemen moeten voldoen aan de gestelde eisen. De herkomst van de gegevens wordt vastgelegd in het verwerkingsregister.

3.5 Toegang tot en verstrekking van persoonsgegevens

Alle medewerkers, intern en extern zijn verplicht tot geheimhouding van de persoonsgegevens, waarvan zij kennisnemen. Uitsluitend de proces- of taakverantwoordelijke heeft ten behoeve van een juiste verwerking rechtstreekse toegang tot de daarvoor benodigde persoonsgegevens. Het NIPV hanteert hiertoe het “Least Privilege principe”. Gegevens uit de gegevensverwerking en uit de bestanden die gebruikt worden voor het verwerken van gegevens kunnen worden verstrekt aan binnen het NIPV werkzame personen, voor zover dit voor hun taakuitoefening noodzakelijk is. Indien de werkzame persoon niet direct toegang zou hoeven hebben voor het uitvoeren van zijn/haar taak, wordt ook geen toegang verleend.

In afwijking van voorstaande hebben de FG en PO, voor zover dit voor hun taakuitvoering nodig is, toegang tot alle gegevens binnen het NIPV[1]. Waar mogelijk zullen zij hierbij een beroep doen op de betreffende proces- of taakverantwoordelijke.

Het NIPV mag niet zomaar persoonsgegevens doorgeven aan personen buiten het NIPV of aan andere organisaties. De algemene regel is dat verstrekken van persoonsgegevens alleen mag als dat verenigbaar is met het doel waarvoor de gegevens zijn verzameld. Of dit het geval is, hangt af van de concrete omstandigheden. Dat kan dus per situatie verschillen.

Aan derden worden de gegevens enkel verstrekt indien:

1. Dit verenigbaar is met het doel waarvoor de gegevens oorspronkelijk verzameld waren;
2. Een wettelijk voorschrift ertoe verplicht de gegevens te verstrekken;

[1] Dit betekent niet dat FG en PO standaard toegang hebben tot alle gegevens. In principe hebben zij als normale medewerkers toegangsrechten. Voor de uitvoering van hun taken (toezicht, onderzoek, beoordelen, adviseren e.d.) mogen zij toegang tot gegevens hebben. Dat verloopt bij voorkeur via de voor die gegevens verantwoordelijke leidinggevende.

3. De betrokkene toestemming heeft verleend tot gegevensverstrekking voor een kenbaar specifiek doel;
4. Daarnaast worden de gegevens verstrekt aan verwerkers, voor zover dit voor de uitoefening van hun taken voor het NIPV als verwerkingsverantwoordelijke noodzakelijk is.

Derden, die op vastgestelde wijze bepaalde persoonsgegevens verwerken, worden door het NIPV ingelicht over de daaraan gestelde voorwaarden en beperkingen. De afspraken hierover worden vastgelegd in een verwerkersovereenkomst, een gegevensuitwisselingsovereenkomst of een overeenkomst gezamenlijke verwerkingsverantwoordelijke. Het NIPV beschikt organisatie breed over modellen voor deze overeenkomsten.

Extra aandacht is er voor de processen rondom in- door en uitstroom (IDU proces) van personeel. Toegang tot gegevens wordt verschaft wanneer dit voor het uitvoeren van de functie noodzakelijk is. Bij door- en uitstroom is de direct leidinggevende verantwoordelijk dat accounts tijdig worden geblokkeerd. Door functioneel beheerders dient er actief gecontroleerd te worden op de toegang en autorisaties en dienen deze vastgelegd te zijn.

3.6 Gebruik van gegevens voor (wetenschappelijk) onderzoek en statistische doelen

Het gebruik van persoonsgegevens voor wetenschappelijk of historisch onderzoek of statistische doeleinden is toegestaan mits het geen geanonimiseerde gegevens betreft en betrokkene(n) van wie de data voor het onderzoek wordt gebruikt hierover is/zijn geïnformeerd en passende waarborgen zijn genomen. Binnen het NIPV wordt de data zo mogelijk tenminste gepseudonimiseerd voor gebruik.

Wanneer persoonsgegevens worden gedeeld met derde partijen voor (wetenschappelijk) onderzoek of statische doeleinden moet toestemming aan betrokkenen worden gevraagd. Het kan ook zijn dat het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en het NIPV zorg heeft gedragen dat de gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen. In dat geval kunnen gegevens zonder toestemming worden gedeeld.

3.7 Doorgifte buiten de EU/EER

De AVG (GDPR) geldt voor alle lidstaten van de Europese Unie en daarom is het mogelijk om persoonsgegevens door te sturen naar een andere EU-lidstaat, zonder daarvoor extra maatregelen te nemen. Binnen de EU gelden dankzij de AVG in alle landen dezelfde regels voor het beschermen van persoonsgegevens. De Europese Commissie heeft daarnaast ook beoordeeld dat Liechtenstein, Noorwegen en IJsland voldoen aan een adequaat beschermingsniveau. Dit zijn geen EU-lidstaten maar deze drie landen vormen samen met de Europese lidstaten de Europese Economische Ruimte (EER)[2]. Binnen deze ruimte mogen persoonsgegevens doorgegeven en verwerkt worden.

[2] https://www.rijksoverheid.nl/onderwerpen/europese-unie/vraag-en-antwoord/welke-landen-horen-bij-de-europese-economische-ruimte-eer

Soms geeft een organisatie persoonsgegevens door naar een ander land. Bijvoorbeeld bij gebruik van een clouddienst met de servers in een ander land. Doorgeven van persoonsgegevens is volgens de Algemene Verordening Gegevensbescherming (AVG) alleen toegestaan binnen de EER of naar landen die een passend beschermingsniveau bieden[3].

Het NIPV geeft in principe geen persoonsgegevens door buiten de EER. Als dit toch onvermijdelijk of noodzakelijk is, dan is een passend beschermingsniveau vereist.

[3] Zie adequaatheidsbesluiten https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en en info over data doorsturen naar de VS https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/doorgifte-binnen-en-buiten-de-eer/doorgifte-persoonsgegevens-naar-de-vs

4. Bescherming van gegevens

Het NIPV treft passende technische en organisatorische maatregelen ter bescherming, bevordering van de juistheid en volledigheid van de persoonsgegevens en ter voorkoming van inbreuk, verlies en onrechtmatige verwerking van de persoonsgegevens. De AVG bevat geen verplichtingen over de manier waarop de gegevensbescherming geborgd moeten worden. De maatregelen dienen een passend niveau van beveiliging, met inbegrip van vertrouwelijkheid, te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. Er zijn verschillende instrumenten beschikbaar om gegevensbescherming te waarborgen.

4.1 Data Protection Impact Assessment (DPIA)

Eén van de instrumenten om de gegevensbescherming te borgen is de uitvoering van een Data Protection Impact Assessment (DPIA). De DPIA wordt ook wel de gegevensbeschermingseffectbeoordeling (GEB) of de Privacy Impact Assessment (PIA) genoemd. Bij het aanpassen van een bestaande verwerking of het starten van een nieuwe verwerking moet een DPIA worden uitgevoerd indien de verwerking een hoog risico voor de gegevensbescherming bevat. De DPIA wordt gebruikt om risico’s in kaart te brengen en om de maatregelen te nemen om deze risico’s in de gegevensverwerking te minimaliseren.

4.2 Dataminimalisatie

Met de komst van de AVG worden de beginselen “Privacy by design” en “Privacy by default” geïntroduceerd. Om te waarborgen dat binnen het NIPV wordt gehandeld in overeenstemming met Privacy by design en Privacy by default, moet met name dataminimalisatie voldoende gewaarborgd zijn.
Dataminimalisatie houdt in dat bij het verzamelen en verwerken van persoonsgegevens niet meer gegevens mogen worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken. Om dataminimalisatie goed toe te passen is het belangrijk om goed vast te leggen op welke manier de gegevens zijn verkregen en voor welk doel de gegevens worden gebruikt, waarbij ook de duur van het gebruik van de gegevens een bepalende factor is.

4.3 Bewaren en vernietigen van gegevens

Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is dient NIPV termijnen vast te stellen voor het wissen van gegevens of voor een periodieke toetsing ervan.
De bewaartermijnen van persoonsgegevens lopen uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Zo zijn er papieren en elektronische documenten welke onder de Archiefwet vallen en waarvoor andere wettelijke bewaartermijnen gelden dan in de AVG beschreven.
Gegevens moeten aan het einde van hun bewaartermijn opgeschoond worden. Indien gegevens daarna nog gebruikt worden voor statistische- of onderzoeksdoeleinden, dan dienen de gegevens geanonimiseerd te worden. Het tijdig en gecontroleerd vernietigen van persoonsgegevens wordt meegenomen in het ontwerp van de verwerking.

4.4 Dataclassificatie

De maatregelen die getroffen moeten worden om de gegevensbescherming te kunnen borgen, is niet voor elk proces en informatiesysteem hetzelfde. Daarom is het nodig dat alle processen en informatiesystemen die gegevens verwerken een dataclassificatie krijgen. Dataclassificatie heeft als doel om de beschikbaarheid, integriteit en vertrouwelijkheid van het proces en het informatiesysteem te benoemen. Zo wordt inzichtelijk welke maatregelen genomen moeten worden om de gegevens die verwerkt worden passend te beschermen.

4.5 Logging van gegevensgebruik

Elk geautomatiseerd systeem dat persoonsgegevens verwerkt, moet logging bijhouden van de verwerkingen. In deze logging staat minimaal vermeld welke gebruiker, op welk moment, welke gegevens heeft verwerkt.
Logging:

- Chronologische registratie van gegevens over van belang zijnde gebeurtenissen, die zich gedurende een periode in een verwerking voordoen;
- Het vastleggen in een logfile, bijvoorbeeld een systeem log of een security log, van feitelijk uitgevoerde bewerkingen en/of pogingen daartoe.

4.6 Verwerkersovereenkomst

In specifieke situaties schakelt het NIPV derden in om gegevens namens het NIPV te verwerken. Het uitbesteden van werkzaamheden aan derden brengt risico's met zich mee op het gebied van gegevensverwerking en informatiebeveiliging. Directie en MT blijven ambtelijk verantwoordelijk voor de verwerking van de gegevens. Zij moeten er daarom op toezien dat gegevens juist verwerkt en beveiligd worden. Met het oog op de omgang met privacy door alle partijen waar het NIPV mee samenwerkt en waarbij persoonsgegevens worden verwerkt worden verwerkersovereenkomsten afgesloten.
Het NIPV beschikt organisatie breed over modellen voor verwerkersovereenkomsten, overeenkomsten gezamenlijk verwerkingsverantwoordelijken en gegevensuitwisseling overeenkomsten.

4.7 Bewust omgaan met persoonsgegevens

Het NIPV streeft naar een cultuur waarbij iedereen elkaar in alle openheid aanspreekt op het gedrag rondom privacy en daarmee van elkaar leert. Communicatie, openheid en toezicht zijn belangrijke randvoorwaarden om een optimaal gegevensbeschermingsbeleid te realiseren.
Het management en alle binnen het NIPV werkzame personen behandelen alle informatie over individuele personen vertrouwelijk en dragen er zorg voor dat deze informatie niet aan onbevoegde derden bekend wordt.

Een medewerker van het NIPV moet zich bij de uitoefening van zijn/haar taken voortdurend bewust zijn van het belang van het waarborgen van de rechten van betrokkenen. Hij/Zij moet persoonsgegevens op een zorgvuldige manier verwerken, zoals omschreven in dit beleid.

Om bewustwording te realiseren is kennisdeling over het onderwerp noodzakelijk. De Functionaris Gegevensbescherming en de Privacy Officer zorgen er samen met andere functionarissen voor dat de informatie over informatiebeveiliging en gegevensbescherming herhaaldelijk onder de aandacht wordt gebracht bij medewerkers van het NIPV.

In bepaalde gevallen kunnen gegevens vallen onder het medisch beroepsgeheim. Deze gegevens dienen met uiterste zorg behandeld te worden. Dit betekent dat gegevens niet zomaar gebruikt mogen worden voor andere doeleinden. Het verwerken van de gegevens is

voorbehouden aan daartoe bevoegde personen. Inzage voor anderen dient afgeschermd te worden en daar waar dit (technisch of organisatorisch) niet mogelijk is, maakt het management helder afspraken over het verwerken. In alle gevallen is inzage in het dossier pas mogelijk na toestemming van de behandelaar of betrokkene zelf.

4.8 Meldplicht voor inbreuken in verband met persoonsgegevens (datalekken)

Indien zich een Datalek voordoet, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, handelt het NIPV in overeenstemming met het vastgestelde proces voor Meldplicht en Afhandeling van (vermoedelijke) datalekken. Dit is een proces van te doorlopen stappen om de eventuele schade of de kans hierop, bij een ‘datalek’ te beperken en de getroffen perso(o)n(en) te beschermen.

De AVG kent in bepaalde gevallen een verplichting om datalekken te melden aan de Autoriteit Persoonsgegevens (AP). Dit is het geval als er sprake is van een hoog risico op nadelige gevolgen voor betrokkene, dan wel nadelige gevolgen voor de bescherming van persoonsgegevens. Het gaat dan om omstandigheden waarbij het NIPV de verantwoordelijkheid draagt.

Wanneer er een dergelijk datalek heeft plaatsgevonden, wordt dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Indien de inbreuk een hoog risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt, wordt de inbreuk in begrijpelijke taal aan de betrokkenen gemeld.

Meldingen van datalekken lopen intern altijd via team Privacy (aanmelden via Synergie). Meldingen aan de Autoriteit Persoonsgegevens is voorbehouden aan de FG of bij diens afwezigheid aan de PO of Jurist.

Team Privacy maakt de afweging of het informeren van de betrokkene in diens belang is of dat dit beter achterwege kan blijven om de betrokkene zelf of anderen te beschermen. Indien van informeren wordt afgezien zal Team Privacy dit besluit registreren en duidelijk motiveren. Team Privacy houdt namens het NIPV een datalekregister bij waarin alle datalekken zijn opgenomen. Het NIPV maakt haar register van datalekken niet openbaar. Jaarlijks legt het MT in haar bestuur rapportage verantwoording af over naleving van de AVG. In betreffende verantwoording zijn ten minste de volgende onderdelen opgenomen:

- Het aantal geregistreerde datalekken en de opvolging hiervan, incl. resultaat;
- Het aantal beroepen op rechten van betrokkenen en de uitvoering hiervan;
- Het aantal DPIA’s en de resultaten daarvan;
- Het aantal medewerkers dat heeft deelgenomen aan het bewustwordingstraject;
- Status certificering(en) op het gebied van informatiebeveiliging (bijv. ISO27001);
- Gesignaleerde knelpunten en geplande/ voorgestelde aanpak inclusief tijdspad van implementatie.

5. Rechten van betrokkenen

5.1 Rechten van betrokkenen

De AVG brengt betrokkenen sterkere privacyrechten dan in voorgaande privacywetgeving. Organisaties die persoonsgegevens verwerken hebben juist meer verplichtingen dan voorheen. De nadruk ligt op de verantwoordelijkheid van het NIPV om te kunnen aantonen dat de organisatie zich aan de wet houdt. De rechten van de betrokkene zijn binnen het NIPV op transparante wijze ingericht. Betrokkenen hebben recht op:

- Informatie en toegang tot gegevens (artikel 13 AVG en 14 AVG);
- Inzage van gegevens (artikel 15 AVG);
- Rectificatie van gegevens (artikel 16 AVG);
- Gegevenswissing, oftewel recht op "vergetelheid" (artikel 17 AVG);
- Beperking van de verwerking (artikel 18 AVG);
- Kennisgevingplicht inzake rectificatie, wissing of beperking (artikel 19 AVG);
- Overdraagbaarheid van gegevens, dataportabiliteit (artikel 20 AVG);
- Bezwaar (artikel 21 AVG);
- Het niet onderworpen worden aan geautomatiseerde besluitvorming (artikel 22 AVG).

Het NIPV geeft hier onder andere uitvoering aan door betrokkenen op haar website(s) helder te informeren over hoe van deze rechten gebruik gemaakt kan worden.
Om gebruik te maken van hun rechten kunnen betrokkenen een verzoek indienen. Alvorens het verzoek te kunnen behandelen moet de identiteit van de verzoeker op deugdelijke wijze worden vastgesteld.

5.2 Recht op informatie en toegang tot gegevens

Tijdens het eerste contact informeert het NIPV betrokkene(n) over de wijze waarop de persoonsgegevens worden verwerkt. Als het niet mogelijk is om de betrokkene tijdens het eerste contact te informeren, dan zorgt het NIPV dat de betrokkene zo spoedig als de situatie toe laat, alsnog over de gegevensverwerking wordt geïnformeerd. Van het uitstellen of niet informeren van de betrokkene kan een aantekening worden gemaakt in het verwerkingsregister.
Het NIPV verzamelt gegevens om haar taken te kunnen uitvoeren. Indien het persoonsgegevens betreft en de betrokkene is hiervan niet op de hoogte, dan informeert het NIPV de betrokkene actief over de verwerking van zijn/haar persoonsgegevens. Hierbij dient in ieder geval gecommuniceerd te worden wat het doel is, welke persoonsgegevens worden verwerkt, wie daarvoor verantwoordelijk is en of de gegevens aan derden worden verstrekt. Het NIPV informeert betrokkene uiterlijk binnen vier weken na de verzameling van persoonsgegevens indien de persoonsgegevens van derden afkomstig zijn.

5.3 Recht op inzage en afschrift van gegevens

Medewerkers en andere betrokkenen kunnen altijd hun persoonsgegevens inzien wanneer zij hier om vragen en kunnen erop vertrouwen dat deze gegevens correct zijn dan wel worden aangepast wanneer noodzakelijk of door de betrokkene is aangegeven dat deze aangepast dienen te worden, voor zover een (wettelijke) verplichting dit niet onmogelijk maakt en zover de aanpassing niet in strijd is met de juistheid en integriteit van de gegevens.
Betrokkene heeft de mogelijkheid om te controleren of en op welke manier zijn/haar gegevens worden verzameld en verwerkt. Ook heeft betrokkene het recht op inzage en een afschrift van zijn/haar dossier. Uitzondering op deze regel is als de persoonlijke levenssfeer, de privacy of veiligheid van een ander/anderen daardoor wordt geschaad. Bijvoorbeeld

informatie die door een betrokken derde is verstrekt in het vertrouwen dat betrokkene deze informatie niet te zien krijgt.
Het NIPV verstrekt de betrokkene, binnen 1 maand na ontvangst van het verzoek, kosteloos een kopie van de persoonsgegevens die worden verwerkt. Indien de termijn van 1 maand onhaalbaar blijkt, verlengt het NIPV de termijn met twee maanden en brengt de betrokkene hiervan op de hoogte. Indien de betrokkene om bijkomende kopieën vraagt, kan het NIPV een vergoeding rekenen niet hoger dan de kostprijs.

In een aantal in de wet (UAVG, artikel 41) opgenomen gevallen mag het NIPV deels of geheel het inzageverzoek weigeren of hier aanvullende vergoeding voor in rekening brengen:

- Indien het persoonsgegevens betreft die niet zijn van betrokkene zelf of van het kind jonger dan 16 jaar over wie aanvrager het wettelijk gezag heeft;
- Indien betrokkene eerder om dezelfde gegevens vroeg;
- Indien betrokkene veel verzoeken doet;
- Indien het inzageverzoek tot een extreme administratieve last leidt;
- Als dat noodzakelijk is voor de openbare veiligheid;
- Als dat noodzakelijk is om strafbare feiten te voorkomen of op te sporen;
- Om de rechten en vrijheden van anderen te beschermen;
- Om informatie af te schermen die over anderen gaat;
- Om iemand anders de kans te geven bezwaar te maken.

Het NIPV mag een inzageverzoek niet zomaar afwijzen. Het NIPV moet argumenten geven voor de weigering van het verzoek en moet kunnen laten zien dat de organisatie een zorgvuldige afweging heeft gemaakt tussen de belangen van alle betrokken partijen.

5.4 Recht op rectificatie (correctie, aanvulling) van gegevens

Als het NIPV persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij het NIPV om feitelijke onjuistheden in het dossier te corrigeren. Het gaat dan bijvoorbeeld om onjuiste adresgegevens. Niet wordt bedoeld dat bijvoorbeeld beoordelingen, meningen, opinies of resultaten mogen worden gewijzigd.
Er kan ook een verklaring aan het dossier worden toegevoegd, bijvoorbeeld wanneer het gaat om de eigen visie van de betrokkene. Ook als het NIPV het niet eens is met de verklaring moet deze worden opgenomen.

5.5 Recht op gegevenswissing

Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien het NIPV niet langer een goede grond heeft voor het gebruik hiervan, bijvoorbeeld indien betrokkene een eerder gegeven toestemming intrekt, indien de gegevens onjuist zijn of wanneer de gegevens niet langer nodig zijn. Het NIPV voert een beleid ten aanzien van bewaartermijnen en vernietiging dat bij de beoordeling van het verzoek gebruikt kan worden.
Het geldt niet voor (persoons)gegevens, zoals financiële gegevens die het NIPV op andere gronden moet bewaren.

Het NIPV hanteert zes uitzonderingen op het recht op vernietiging:

1. Een andere wet schrijft een afwijkende bewaartermijn voor waarbinnen de gegevens niet vernietigd mogen worden;
2. Een ander dan de betrokkene heeft een aanmerkelijk belang bij het bewaren van de gegevens;
3. Verwijdering zou het NIPV in ernstige mate schaden. Bijvoorbeeld als daardoor de validatie van wetenschappelijk onderzoek in het gedrang komt, terwijl eerder wel toestemming is gegeven.

4. De gegevens zijn nodig in het kader van een strafrechtelijk onderzoek of bij een rechtsgang;
5. Vernietiging is in strijd met de wet, met het algemeen belang, met de veiligheid van betrokkene of met het gerechtvaardigd belang van het NIPV. Hierbij mag het NIPV het gerechtvaardigd belang wel inzetten in haar rol van werkgever, maar niet in haar rol als overheid;
6. ‘Goed hulpverlenerschap’ staat vernietiging in de weg.

Het NIPV mag een verzoek tot gegevenswissing niet zomaar afwijzen. Het NIPV moet argumenten geven voor de weigering van het verzoek en moet kunnen laten zien dat de organisatie een zorgvuldige afweging heeft gemaakt tussen de belangen van alle betrokken partijen.

5.6 Recht op beperking van de verwerking

Het recht op beperking van de verwerking van persoonsgegevens houdt in dat de gegevens wel beschikbaar blijven, maar dat ze tijdelijk niet gebruikt mogen worden. De persoonsgegevens mogen dan alleen nog worden gebruikt met toestemming van de betrokkene, of als dat nodig is voor het instellen, uitoefenen of onderbouwen van een rechtsvordering of ter bescherming van de rechten van andere natuurlijke personen of rechtspersonen. Voorbeeld: als de juistheid van de persoonsgegevens worden betwist en voor een periode die de verwerkingsverantwoordelijke in staat stelt om de juistheid van die persoonsgegevens te controleren.

5.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

Het NIPV is vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens voor zover het werkzaamheden betreft in het kader van algemeen belang of op basis van een wettelijke verplichting.
Het recht om gegevens te mogen meenemen geldt voor persoonsgegevens die de betrokkene zelf actief en bewust heeft verstrekt (eigen data). Deze vallen onder het recht op dataportabiliteit. Dit geldt ook voor de gegevens die de betrokkene indirect heeft verstrekt door het gebruik van een dienst of een apparaat. Gegevens die niet (in)direct door de betrokkene zijn verstrekt vallen hier niet onder.

5.8 Recht van bezwaar tegen verwerking

De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens.
Het NIPV staakt de verwerking van de persoonsgegevens tenzij het NIPV dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

5.9 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming waaronder profilering

Bij geautomatiseerde individuele besluitvorming is geen sprake van (noemenswaardige) menselijke tussenkomst zodat eventuele uitkomsten kunnen worden gecorrigeerd. Het is uitsluitend gebaseerd op geautomatiseerde verwerking van persoonsgegevens.
Het NIPV past geen geautomatiseerde individuele besluitvorming, waaronder profilering, toe als daaraan rechtsgevolgen voor de betrokkene zijn verbonden of als het besluit betrokkene in aanmerkelijke mate kan treffen.

5.10 Klachten en verzoeken

Onverminderd de rechten die de betrokkenen in de wet worden toegekend, kan iedere betrokkene schriftelijk een verzoek conform AVG indienen bij het NIPV indien hij meent dat door of namens het NIPV persoonsgegevens worden verwerkt op een wijze die in strijd is met de wet of met dit beleid.
Binnen 1 maand beoordeelt het NIPV of de het verzoek ontvankelijk is. Het NIPV laat binnen die termijn weten wat er met de het verzoek gaat gebeuren, waaronder of het NIPV de behandeling met twee maanden verlengt.

Als het verzoek niet (tijdig) kan worden opgevolgd, deelt het NIPV uiterlijk binnen 1 maand of binnen de verlengde termijn mee waarom de het verzoek zonder gevolg is gebleven. De betrokkene heeft dan de mogelijkheid om bezwaar te maken bij het NIPV, een klacht in te dienen bij de Autoriteit Persoonsgegevens of het bezwaar aan een bevoegd rechter voor te leggen.

Daarnaast kan elke betrokkene een klacht indienen. Het NIPV behandelt klachten volgens de daarvoor door haar vastgestelde en bekendgemaakte klachtenregeling.

5.11 Informeren van (keten)partners

Het NIPV informeert relevante (keten)partners indien een klacht of verzoek wordt ingewilligd. Dit betreft o.a. organisaties met wie een verwerkersovereenkomst, een overeenkomst gezamenlijk verwerkersverantwoordelijken dan wel een gezamenlijke uitwisselingsovereenkomst is afgesloten. Indien relevant vraagt het NIPV actief om bevestiging van de betreffende (keten)partners dat aan het verzoek is voldaan.

6. Functies en verantwoordelijkheden

Het NIPV heeft gegevensbescherming ingebed in de organisatie. Voor alle medewerkers, op ieder niveau, is duidelijk welke rollen er zijn op het gebied van gegevensbescherming. Medewerkers kennen hun rol en verantwoordelijkheid op het gebied van gegevensbescherming zoals hierna uiteengezet.
Het betreft hier alleen de rol en verantwoordelijkheid voor zover die verband houden met privacy en gegevensbescherming.

Algemeen bestuur

- Bestuurlijk eindverantwoordelijke in de zin van AVG
- Kaders stellen ten aanzien van privacy beleid.

Dagelijks bestuur

- Bestuurlijk verantwoordelijk;
- Eindverantwoordelijk voor toezicht en controle op naleving van het beleid;

De algemeen directeur/Directie

- Gemandateerd door het DB;
- Aanstellen van een Functionaris Gegevensbescherming om namens het bestuur toezicht te houden en te adviseren
- Ambtelijk eindverantwoordelijk;
- Vaststellen van gewenste niveau van informatiebeveiliging en privacy, implementatie, en aanwijzing van procesverantwoordelijke/systeemeigenaar per informatiesysteem;
- Bevordert de beschikbaarheid van voldoende middelen om gegevensbescherming passend te waarborgen.

Centrummanagers en afdelingshoofden

- Ambtelijk verantwoordelijk binnen het eigen centrum en gezamenlijk binnen de gehele organisatie;
- Bevorderen van het bewustzijn rond gegevensbescherming in de organisatie;
- Verantwoordelijk voor de borging van de beschikbaarheid, integriteit en vertrouwelijkheid van de door het centrum of de afdeling verwerkte persoonsgegevens;
- In voorkomend geval verantwoordelijk voor de uitvoering van een DPIA en borging van de hieruit voortvloeiende mitigerende maatregelen;
- Verantwoordelijk voor de principes van Privacy by Design en Privacy by Default bij nieuwe verwerkingen en bij grote wijzigingen in de verwerking;
- Verantwoordelijk voor aanmelden van nieuwe (of veranderde) verwerkingen van persoonsgegevens;
- Het afsluiten van verwerkersovereenkomsten en andere regelingen;
- Ervoor zorgdragen dat ondersteunende systemen en processen voldoen aan wet- en regelgeving.

Teammanagers

- Ambtelijk verantwoordelijk binnen het eigen team en gezamenlijk binnen het centrum of de afdeling;
- Bevorderen van het bewustzijn rond gegevensbescherming in het team;
- Verantwoordelijk voor de borging van de beschikbaarheid, integriteit en vertrouwelijkheid van de door het team verwerkte persoonsgegevens;
- In voorkomend geval verantwoordelijk voor de uitvoering van een DPIA en borging van de hieruit voortvloeiende mitigerende maatregelen;
- Verantwoordelijk voor de principes van Privacy by Design en Privacy by Default bij nieuwe verwerkingen en bij grote wijzigingen in de verwerking;
- Verantwoordelijk voor aanmelden van nieuwe (of veranderde) verwerkingen van persoonsgegevens;
- Het afsluiten van verwerkersovereenkomsten en andere regelingen;
- Ervoor zorgdragen dat ondersteunende systemen en processen voldoen aan wet- en regelgeving.

Programmamanagers

- Ambtelijk verantwoordelijk binnen het eigen programma;
- Bevorderen van het bewustzijn rond gegevensbescherming binnen het eigen programma;
- Verantwoordelijk voor de borging van de beschikbaarheid, integriteit en vertrouwelijkheid van de binnen het programma verwerkte persoonsgegevens;
- In voorkomend geval verantwoordelijk voor de uitvoering van een DPIA en borging van de hieruit voortvloeiende mitigerende maatregelen;
- Verantwoordelijk voor de principes van Privacy by Design en Privacy by Default bij nieuwe verwerkingen en bij grote wijzigingen in de verwerking;
- Verantwoordelijk voor aanmelden van nieuwe (of veranderde) verwerkingen van persoonsgegevens;
- Ervoor zorgdragen dat ondersteunende systemen en processen voldoen aan wet- en regelgeving.

Functionaris voor de gegevensbescherming (FG)

De FG heeft een wettelijke positie. De FG is onafhankelijk, wordt rechtstreeks door het bestuur benoemd en is verantwoording verschuldigd aan het bestuur en afgeleid daarvan aan de directie. De FG mag geen aanwijzingen krijgen ten aanzien van zijn werkzaamheden. De FG kent ontslagbescherming en kan niet verantwoordelijk worden gehouden voor het door de organisatie voldoen aan de AVG en andere privacywetgeving.

De FG heeft een controlerende en toezichthoudende taak en daarnaast een adviserende taak richting bestuur, directie, management, organisatie en in crisisomstandigheden:

- Toezicht houden op een juiste en zorgvuldige omgang met persoonsgegevens en het naleven van de AVG en andere privacywetgeving;
- Gevraagd en ongevraagd adviseren en informeren van bestuur, directie en organisatie ten aanzien van privacy, de omgang met persoonsgegevens, de inrichting van de privacy organisatie klachten en verzoeken;
- Het geven van aanwijzingen aan de organisatie ten aanzien van privacy en de omgang met persoonsgegevens. (Adviezen en aanwijzingen zijn niet vrijblijvend);
- Formeel aanspreekpunt voor de Autoriteit Persoonsgegevens;
- Rapporteert tenminste jaarlijks aan het bestuur, directie en MT over de manier waarop het NIPV de afgelopen periode met gegevensbescherming is omgegaan;

- Actueel houden- en coördineren van de uitvoering van dit gegevensbeschermingsbeleid;
- Het afhandelen van klachten ten aanzien van de omgang met gegevensbescherming;
- Het creëren van bewustzijn en kennisontwikkeling binnen de organisatie ten aanzien van privacy en informatieveiligheid;
- Het verzorgen van trainingen om de interne kennis te vergroten en borgen;
- Beoordelen van meldingen van datalekken;
- Het vertegenwoordigen van de organisatie in landelijke overleggen en gremia;
- Lid van de CIO office;
- Coördineren van privacy werkzaamheden;
- Samenwerken met- en zo nodig vervangen van de Privacy Officer;
- Samen met de CISO adviseren ten aanzien van informatieveiligheid;
- Beheert het overzicht van datalekken (datalekregister).

Privacy Officer (PO)
De PO vervangt de FG bij afwezigheid, met uitzondering van de toezichthoudende taak.

De Privacy Officer heeft een adviserende taak richting de organisatie. Daarnaast verzorgt en coördineert de PO de uitvoerende taken die uit het gegevensbeschermingsbeleid volgen:

- Mede opstellen van beleid, procedures en richtlijnen ten uitvoering van het gegevensbeschermingsbeleid;
- Advisering over en ondersteunen bij privacy en gegevensbescherming gerichte zaken en de uitvoering en naleving van privacywetgeving;
- Het creëren van bewustzijn en kennisontwikkeling binnen de organisatie ten aanzien van privacy en informatieveiligheid;
- Het verzorgen van trainingen om de interne kennis te vergroten en borgen;
- Beoordelen van- en adviseren over de verwerking van persoonsgegevens;
- Het verzorgen van de formele afhandeling ten aanzien van rechten en plichten van (externe) betrokkenen;
- Verzorgen van overige privacy werkzaamheden zoals inzage- en correctie verzoeken;
- Het vertegenwoordigen van de organisatie in landelijke overleggen en gremia;
- Mede beoordelen van meldingen van datalekken;
- Advisering en ondersteuning bij het afsluiten van verwerkersovereenkomsten;
- Beheer van het register van de verwerkingsactiviteiten (verwerkingsregister);
- Bevorderen van privacy- en informatiebeveiligingsbewustzijn;
- Samenwerken met- en zo nodig vervangen van de FG;
- Samen met de ISO adviseren ten aanzien van informatieveiligheid.

Chief Information Security Officer (CISO)
- Actueel houden- en coördineren van de uitvoering van het integraal beveiligingsbeleid;
- Aanspreekpunt voor informatiebeveiliging;
- Bevorderen van informatiebeveiligingsbewustzijn;
- Verantwoordelijk voor de afhandelen van informatiebeveiligingsincidenten;
- (Pro) actief adviseren over informatiebeveiliging en het informatiebeveiligingsbeleid;
- Uitvoeren van analyses en advies over BIO (minimaal benodigde aanpassingen);
- Ondersteunen bij het uitvoeren van risicoanalyses en DPIA;

- Adviseren en ondersteunen van de organisatie om het benodigde niveau van informatiebeveiliging te bereiken dat minimaal voldoet aan de wet- en regelgeving;
- Samen met de FG en PO adviseren ten aanzien van gegevensbescherming.

Information Security Officer (ISO)

- Verzorgt de uitvoering van het informatiebeveiligingsbeleid;
- Aanspreekpunt voor informatiebeveiliging;
- Bevorderen van informatiebeveiligingsbewustzijn;
- Mede verantwoordelijk voor de afhandelen van informatiebeveiligingsincidenten;
- Adviseren over informatiebeveiliging en het informatiebeveiligingsbeleid;
- Ondersteunen bij het uitvoeren van risicoanalyses en DPIA;
- Adviseren en ondersteunen van de organisatie om het benodigde niveau van informatiebeveiliging te bereiken dat minimaal voldoet aan de wet- en regelgeving;
- Samen met de FG en PO adviseren ten aanzien van gegevensbescherming.

Functioneel beheerders informatiesystemen

- Uitvoering geven aan het gegevensbescherming- en integraal beveiligingsbeleid voor de betreffende applicaties.

CIO office

- Toezien op- en adviseren over risico's ten aanzien van gegevensbescherming en informatiebeveiliging.

Medewerker

- Is zich bewust van de eigen verantwoordelijkheid en de risico's van het eigen handelen ten aanzien van privacy en gegevensbescherming;
- Gaat binnen de eigen taakuitvoering op juiste wijze om met persoonsgegevens;
- Meldt geconstateerde risico's en incidenten.

7. Formeel toezicht op de gegevensverwerking

Het bestuur van het NIPV heeft een Functionaris voor de Gegevensverwerking aangesteld. Deze functionaris heeft als taak binnen de organisatie toezicht te houden op de privacy, de verwerking van persoonsgegevens en daarmee op de toepassing en naleving van de AVG.
De FG is geregistreerd bij de Autoriteit Persoonsgegevens onder nummer **FG006385**.
De FG is bereikbaar via privacy@nipv.nl