PRIVACY BELEIDSKADER
NEDERLANDS REGISTER GERECHTELIJK DESKUNDIGEN

Datum 31 januari 2022
Status: versie 1.0

Privacy Officer	Els de Jong
Functionaris gegevens bescherming	Ella Schepel
Directeur	Michel Smithuis
Voorzitter College	Eric Bakker

VERSIEBEHEER

Versie	Datum	Auteur	Opmerkingen
1.0	10 februari 2022	Els de Jong	FG akkoord Vaststelling College

Voorwoord

“Bij het NRGD staat zicht op kwaliteit centraal. Dat geldt ook voor hoe het NRGD met persoonsgegevens omgaat.”

Het NRGD zorgt ervoor dat forensisch onderzoekers en hun rapportages voldoen aan (inter)nationaal geldende normen. Daardoor kunnen belanghebbenden vertrouwen hebben in de kwaliteit van forensisch deskundigenonderzoek.

Als onafhankelijke en transparante organisatie bevordert en waarborgt het NRGD de kwaliteit van de forensische expertise. Ook wordt de ontwikkeling van de kwaliteit van het forensisch veld als geheel gestimuleerd. Het NRGD concentreert zich op regulering, advisering en kennisuitwisseling.

Voor de uitvoering van zijn wettelijke taak verwerkt het NRGD persoonsgegevens van onder andere gerechtelijk deskundigen, leden van het College, leden van adviescommissies, medewerkers en de contactgegevens van ketenpartners. Het NRGD is verantwoordelijk voor een zorgvuldige omgang met deze persoonsgegevens.

Het NRGD verwerkt persoonsgegevens op rechtmatige, behoorlijke en transparante wijze en conform de geldende wet- en regelgeving. In dit privacy beleidskader wordt uitgelegd hoe het NRGD beleidsmatig omgaat met de verwerking van persoonsgegevens en wat de rol van de medewerker is bij de bescherming van die gegevens.

Utrecht, 10 februari 2022

w.g.

F.A.M. Bakker
Voorzitter College gerechtelijk deskundigen

INHOUD

Voorwoord	2
1. NRGD Privacy beleidsplan	5
1.1 Doel	5
1.2 Scope	5
1.3 Doelgroepen	6
1.4 Verantwoordelijk voor bijhouden privacy beleidsplan	6
1.5 Revisies	6
2. Uitgangspunten bij verwerking van persoonsgegevens	7
2.1 Algemeen kader voor verwerking van persoonsgegevens	7
2.1.1 Europese en Nederlandse wetgeving op het terrein van privacy	7
2.1.2 Specifieke context NRGD	8
2.1.3 Richtsnoeren Comité en AP	8
2.2 Uitgangspunten voor een verantwoorde omgang met persoonsgegevens	9
3. Privacy governance	17
3.1 Inleiding	17
3.2 Drie verdedigingslinies	17
3.3 Privacyverantwoordelijkheden rollen en taken	18
3.4 Privacy overlegstructuren	19
3.5 Sturing, regie en toezicht	20
3.6 Privacy trainingen en bewustwording	20
Bijlage 1: Terminologie en achtergrond	21
Bijlage 2: Instrumenten	23
Bijlage 3: PRIVACY FUNCTIONARISSEN NRGD	24

1 NRGD Privacy beleidsplan

Op het werk van het Nederlandse Register Gerechtelijk Deskundigen (NRGD) is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. In het Besluit register deskundige in strafzaken is vastgelegd welke gegevens het NRGD op grond van zijn wettelijke taak moet en mag verwerken.

1. Het NRGD verwerkt in de eerste plaats persoonsgegevens van gerechtelijk deskundigen die een aanvraag om (her)registratie doen. Zij verstrekken daartoe documenten die hun persoonsgegevens bevatten, zoals een aanvraagformulier met naam en contactgegevens. Het NRGD vermeldt conform de wettelijke taak de naam en contactgegevens van de geregistreerde deskundigen in het register. Het register is openbaar en toegankelijk via de website van het NRGD.
2. In het kader van de toetsing en registratie van gerechtelijk deskundigen heeft het NRGD verder te maken met persoonsgegevens van leden van het College, leden van adviescommissies en de medewerkers van het Bureau NRGD. De leden van de toetsings- en bezwaaradviescommissie beoordelen aanvragen om (her)registratie en maken daartoe een adviesbeoordelingsformulier op. De leden van het College nemen een besluit op basis van deze adviezen. De medewerkers van het Bureau begeleiden de toetsing, inclusief bezwaar, en bereiden de besluitvorming van het College voor.
3. Burgers kunnen een klacht of melding indienen over geregistreerde deskundigen. Het NRGD verwerkt de persoonsgegevens van de burgers die een melding doen.
4. Burgers kunnen een verzoek doen om informatie openbaar te maken. Het NRGD verwerkt de persoonsgegevens van de burgers die een verzoek om informatie doen.

Dit document schetst de kaders voor de bescherming van persoonsgegevens. Daarbij wordt verwezen naar praktische ondersteunende instrumenten die de medewerker kan inzetten voor het verwerken en beschermen van persoonsgegevens (checklists, stappenplan, procedures).

In dit document staan begrippen die in de context van de AVG dienen te worden gelezen. De belangrijkste begrippen worden in bijlage 1 kort toegelicht.

1.1 Doel

Doel van dit beleidsplan is een omgeving te creëren waarin elke medewerker van het NRGD:

- zijn of haar verantwoordelijkheid kent als het gaat om privacy en het verwerken van persoonsgegevens;
- in staat is om conform het beleid uitvoering te geven hieraan en de juiste procedures te volgen;
- contact kan opnemen met de juiste personen wanneer er vragen zijn.

1.2 Scope

Het privacy beleidsplan ziet op de bescherming van persoonsgegevens die het NRGD verwerkt in het kader van de uitvoering van de wettelijke taak. Het College is aan te merken als verwerkingsverantwoordelijke. Het Bureau NRGD ondersteunt, faciliteert en adviseert het College bij de uitvoering van zijn publieke taak, waaronder het in overeenstemming met de AVG verwerken van persoonsgegevens. De secretaris van het

College, eveneens directeur van het Bureau NRGD, is aangewezen als hoofd van dienst en als dusdanig verantwoordelijk voor de werkzaamheden die de medewerkers verrichten.

De directeur en medewerkers van het Bureau zijn in dienst van het ministerie van Justitie en Veiligheid. Het verwerken van personeelsgegevens van medewerkers valt buiten de reikwijdte van dit beleidsplan. Hiervoor heeft de minister van J&V een beleidsplan vastgesteld.

1.3 Doelgroepen

Dit beleidsplan is bedoeld voor alle medewerkers, ook de tijdelijke medewerkers, en alle andere personen die in opdracht van het NRGD werken.

De aard van de werkzaamheden bepaalt het type privacyvraagstukken en afwegingen die voor de voor de medewerker relevant zijn.

1.4 Verantwoordelijk voor bijhouden privacy beleidsplan

De privacy officer van het NRGD is verantwoordelijk voor het beheer van dit privacy beleidsplan.
In bijlage 2 is een overzicht van documenten en instrumenten die het NRGD gebruikt. Het beleidsplan is een dynamisch document dat de privacy officer periodiek zal actualiseren. Algemene vragen over dit beleid of suggesties tot wijziging of toevoeging aan het beleid, kunnen worden gericht aan de privacy officer van het NRGD.

1.5 Revisies

Dit beleid wordt periodiek herzien en bijgewerkt.

2 Uitgangspunten bij verwerking van persoonsgegevens

Dit hoofdstuk bevat de kern van het juridisch kader dat van toepassing is op de verwerking en bescherming van persoonsgegevens. De eerste paragraaf behandelt het wettelijk kader en de zogeheten soft law, onder vermelding van publicaties waarin de wetgeving begrijpelijk wordt toegelicht.

In paragraaf 2.2 staan de uitgangspunten voor de omgang met persoonsgegevens, wat dat voor de werkzaamheden van de medewerker betekent en welke instrumenten beschikbaar zijn om in overeenstemming met de AVG uitvoering te geven aan het privacy beleid van het NRGD.

2.1 Algemeen kader voor verwerking van persoonsgegevens

2.1.1 Europese en Nederlandse wetgeving op het terrein van privacy

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Vanaf dat moment geldt dezelfde privacywetgeving in de hele Europese Unie. De AVG vervangt de richtlijn 95/46 die was geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp).
De AVG is rechtstreeks van toepassing. Dit betekent dat de AVG direct voor iedereen geldt zonder dat daar eerst nationale wetgeving aan te pas is gekomen. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, is deze ingevuld in de Uitvoeringswet AVG (UAVG).

Op de verwerking van persoonsgegevens die in de basisregistratie personen (BRP) voorkomen is de (U)AVG niet van toepassing. Op de verwerking van die persoonsgegevens ziet de Wet BRP.

Publicaties/instrumenten:
- Handleiding AVG en UAVG, Den Haag 2018: Handleiding Algemene verordening gegevensbescherming (AVG) | Rapport | Rijksoverheid.nl
- Tekstuitgave privacyverordening & UAVG van Jan Berkvens en Cathérine Jakimowisc, 2018

Naast de AVG is sinds mei 2018 van toepassing de richtlijn 2016/680 ter vervanging van het kaderbesluit 2008/977. Deze richtlijn ziet op de verwerking van persoonsgegevens in het kader van het strafrecht en is geïmplementeerd in de Wpg en de Wjsg.[1] Dit is niet van toepassing op het NRGD, maar wel voor een aantal ketenpartners als het OM of de politie.

De ePrivacyverordening (EPV)[2] is een aanvulling op de AVG en ziet op bescherming van de belangen van gebruikers van communicatiediensten. Denk aan telecombedrijven en over-de-top-communicatiediensten (OTT's) zoals Skype en WhatsApp, Facebook en Google. De EPV ziet ook op cookieregels en het spamverbod. Dit is van belang in verband met de website van het NRGD. Wanneer de EPV in werking gaat treden, is op dit moment nog onduidelijk.

[1] De Wpg regelt de verwerking van politiegegevens door de Nationale Politie, de bijzondere opsporingsdiensten, de Koninklijke marechaussee en de Rijksrecherche.
De Wjsg regelt het verwerken van justitiële gegevens (in persoonsdossiers) en voor de VOG. De wet regelt ook de verwerking van strafvorderlijke gegevens.

[2] Verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG.

2.1.2 Specifieke context NRGD

De Wet deskundige in strafzaken (Wet dis), thans verankerd in het Wetboek van Strafvordering (WvSV), en het Besluit register deskundige in strafzaken (Brdis) zijn van toepassing op de werkzaamheden van het NRGD. In het Brdis zijn de bevoegdheden en taken van het NRGD uitgewerkt. Ook staat hierin voorgeschreven welke documenten de deskundige voor zijn aanvraag om (her)registratie moet toesturen. Voor de nadere invulling en implementatie van de kernprocessen heeft het NRGD beleid en werkwijzen ontwikkeld.

Enkele secundaire processen, zoals personeelsbeleid vallen onder verantwoordelijkheid van JenV en zijn in ondermandaat neergelegd bij de directeur van het Bureau NRGD. Voor het deel waarvoor het NRGD zelf aan de lat staat, zoals PIOFACH-processen, zoekt het NRGD afstemming met samenwerkingspartners en JenV, opdat voor alle betrokken partijen helder is onder wiens verantwoordelijkheid deze taken worden uitgevoerd.

2.1.3 Richtsnoeren Comité en Autoriteit Persoonsgegevens (AP)

Het Europees Comité voor gegevensbescherming (Comité)[3] is een onafhankelijk EU orgaan dat wordt gevormd door de voorzitters van de toezichthoudende autoriteiten en de Europese toezichthouder.[4] Doel van het Comité is de consequente toepassing van de AVG in de EU. De richtsnoeren, aanbevelingen en 'best practices' van het Comité zijn belangrijke bronnen voor de uniforme uitleg van de AVG. Denk bijvoorbeeld aan de vraag wanneer waarschijnlijk sprake is van een hoog risico bij datalekken.

Ook de uitleg van de AVG door de AP in de vorm van thematische beleidsregels zijn belangrijke bronnen voor de naleving van de AVG. Het gaat dan bijvoorbeeld om beleidsregels over cameratoezicht en de meldplicht datalekken. De AP gaat ervan uit dat verwerkingsverantwoordelijken als het NRGD de beleidsregels toepassen en adviezen opvolgen, dan wel gemotiveerd afwijken (comply or explain).

Instrumenten:
- Handreiking AVG en toelichting

Bronnen:
- https://edps.europa.eu/
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_avg.pdf

2.1.4 Naleving, toezicht en advies

De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de AVG. De AP is bevoegd om boetes op te leggen in het geval van overtredingen. Daarnaast is elke overheidsinstantie verplicht om een functionaris gegevensbescherming (FG) aan te stellen, zo ook het NRGD. De FG ziet toe op de naleving van de AVG en staat het NRGD bij met advies. Bij het NRGD zelf zijn de privacy officer en de chief information officer de functionarissen die erop toezien dat het NRGD in overeenstemming met de AVG persoonsgegevens

[3] European Data Protection Supervisor (EDPS).

[4] Het Comité volgt de Artikel 29-Groep op die op grond van richtlijn 95/46 als adviesgroep functioneerde.

verwerkt. Medewerkers kunnen in eerste instantie bij hen terecht. De medewerkers zelf vervullen ook een belangrijke rol in het beschermen van persoonsgegevens. De directeur van het Bureau NRGD is eindverantwoordelijk.

2.2 Uitgangspunten voor een verantwoorde omgang met persoonsgegevens

De uitgangspunten voor gegevensbescherming zijn van toepassing op *alle* verwerkingsactiviteiten met betrekking tot persoonsgegevens binnen het NRGD. Dit betekent dat alle verwerkingen van persoonsgegevens moeten voldoen aan onderstaande eisen. De medewerkers van het NRGD houden rekening hiermee bij het ontwikkelen, implementeren en uitvoeren van beleid.

1. **Het NRGD verwerkt alleen persoonsgegevens als voor de verwerking een rechtmatige grondslag aanwezig is en een duidelijk omschreven en gerechtvaardigd doel.**

Rechtmatige verwerking
Elke verwerking van persoonsgegevens moet behoorlijk en rechtmatig zijn. De verwerkingen hebben een wettelijke grondslag.

- Voor uitvoeringsorganisaties van de rijksoverheid als het NRGD geldt dat de verwerking van persoonsgegevens noodzakelijk moet zijn voor de vervulling van de publieke taak.[5] Dit betekent dat het NRGD alleen persoonsgegevens mag verwerken in het kader van de publieke taak ofwel in het kader van het beheer van het register, het bevorderen van deskundigheid en het delen van kennis hierover. De rechtsgrondslag van het NRGD is te vinden in artikel 51k van het Wetboek van het Strafvordering jo het Besluit register deskundige in strafzaken.
- De grondslag van een “gerechtvaardigd belang” uit de AVG kan niet worden gebruikt als er sprake is van verwerkingen door overheidsinstanties.[6] Deze grondslag kan wel in beeld komen bij een verwerking in het kader van de bedrijfsvoering (denk bijvoorbeeld aan cameratoezicht rond het gebouw). Hetzelfde geldt voor de grondslag “toestemming”. De ongelijke machtsverhouding tussen betrokkene en de overheid staat over het algemeen in de weg aan de eis dat betrokkene de toestemming vrijelijk moet kunnen verlenen. Een uitzondering daarop is de verhouding werkgever-werknemer. De toestemming van de werknemer om zijn foto te gebruiken in een smoelenboek vormt bijvoorbeeld wel voldoende grondslag.
- De verwerking dient voor betrokkenen duidelijk en transparant te zijn. Betrokkenen moeten weten wat het NRGD met de verzamelde persoonsgegevens doet en hoe lang het die bewaart. In de Privacyverklaring van het NRGD is dit terug te vinden.

Doelbinding
Persoonsgegevens mogen slechts worden verwerkt voor een voorafgaand aan de verwerking omschreven doel (of doeleinden).

[5] De zogenoemde e-grond van artikel 6 AVG: een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag.
[6] De zognoemde f-grond van artikel 6 AVG: noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerker of van de verwerkingsverantwoordelijke of van een derde.

Doelen die duidelijk zijn omschreven maken het voor betrokkene inzichtelijk wat met de gegevens wordt gedaan.

- Het NRGD verwerkt alleen persoonsgegevens waarvoor een wettelijke grondslag bestaat om ze te mogen verwerken. Het NRGD zorgt ervoor dat persoonsgegevens alleen verwerkt worden voor het specifieke doel waarvoor ze verzameld zijn of dat het nieuwe doel verenigbaar is met het oorspronkelijke doel.
- Het NRGD legt het doel van elke verwerking concreet vast. Als een bestand voor meer doelen wordt gebruikt dan wordt dat vermeld in de doelomschrijving.
- Bij verdere verwerking van persoonsgegevens voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verzameld, beoordeelt het NRGD of dit nieuwe doel verenigbaar is met het oorspronkelijke doel.

Register van verwerkingen
De verwerking dient te worden opgenomen in het register van verwerkingsactiviteiten. Dit register, dat een beschrijving van verwerkingsactiviteiten bevat en niet de persoonsgegevens zelf, moet de verwerkingsverantwoordelijke op verzoek van de AP direct kunnen laten zien. Het is niet toegestaan om dit achteraf te reconstrueren. Het is dus essentieel dat dit register actueel is. De privacy officer en chief information officer zijn hier samen verantwoordelijk voor.

- Het NRGD legt verwerkingen van persoonsgegevens vast in een register van verwerkingen. Het NRGD maakt waar mogelijk gebruik van de door JenV aangeboden tooling.
- Het NRGD maakt waar mogelijk gebruik van generieke verwerkingen of vertaalt deze naar de situatie van het NRGD.

DPIA
Elke overheidsorganisatie is verplicht een Data Protection Impact Assessment, DPIA (ook wel genoemd GEB), uit te voeren bij de ontwikkeling van beleid en regelgeving waaruit op grote schaal of systematisch en stelselmatig verwerkingen van persoonsgegevens voortvloeien of de verwerking een hoog risico oplevert. De AP heeft een lijst van verwerkingen opgesteld waarvoor de DPIA verplicht is.[7] Voor het NRGD betekent dit dat het een DPIA moet doen wanneer het beleid ontwikkelt waar de verwerking van persoonsgegevens uit volgt.

De DPIA is bedoeld om de effecten van de beoogde gegevensverwerking(en) voor betrokkenen te inventariseren en te beoordelen. Op basis van de DPIA kunnen maatregelen worden genomen om de risico's aan te pakken. Het NRGD gebruikt hiervoor het Model gegevensbeschermingseffect-beoordeling Rijksdienst (PIA). De privacy officer en de FG kunnen helpen bij vragen over de opzet en uitvoering van de DPIA. Het NRGD legt Pre-DPIA's en DPIA's vast in een DPIA-register. De privacy officer beheert dit register.

[77] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667

- Het NRGD verricht voorafgaand aan een verwerking van persoonsgegevens een risico-analyse in de vorm van een Pre-DPIA.
- Indien uit de Pre-DPIA volgt dat de verwerking DPIA-plichtig is, voert het NRGD een DPIA uit.
- Het NRGD stelt per DPIA een risico- en maatregelen vast voor monitoring van de genomen en nog te nemen maatregelen, herijking en gronden voor herijking DPIA, zoals beschreven in het DPIA-proces.

Instrumenten:
- AVG-register van verwerkingen (via JenV) - Privacyverklaring NRGD - Rijksmodel GEB (PIA) - Pre-DPIA-model - DPIA proces - (Pre)DPIA-register - DPIA's risico- en maatregelenoverzicht

2 Het NRGD beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel.

Alleen voor het vooraf en precies omschreven doel mogen noodzakelijke gegevens worden verzameld. Gegevens mogen vervolgens niet verder worden verwerkt voor een met dat doel onverenigbare wijze. Persoonsgegevens die niet meer nodig zijn (moeten) worden verwijderd of waar mogelijk geanonimiseerd.[8] Er moet ook van te voren worden bedacht waarom gegevens voor die specifieke verwerking nodig zijn en of daadwerkelijk *alle* gegevens nodig zijn. Bij de ontwikkeling van nieuw (of wijziging van bestaand) beleid wordt met gegevensbescherming rekening gehouden.

- Het NRGD verwerkt niet meer gegevens dan die aantoonbaar noodzakelijk zijn voor het doel van de verwerking (*dataminimalisatie*).
- Het NRGD configureert nieuwe systemen op een wijze dat alleen de voor het specifieke verwerkingsdoel noodzakelijke gegevens worden verwerkt. Privacy wordt bij het ontwerp van een (nieuw) automatiseringssysteem al als uitgangspunt worden genomen (*privacy by design*).
- Het NRGD gaat bij het ontwikkelen van beleid, processen (en systemen) uit van de meest privacybeschermende instellingen *(privacy by default)*.

[8] De AVG is niet van toepassing op anonieme gegevens omdat deze gegevens niet terug te voeren zij op een geïdentificeerde of identificeerbare natuurlijke persoon. Anonimisering is versleuteling die onomkeerbaar is, het niet meer mogelijk om deze later weer met personen in verband te brengen. Bij pseudonimisering kunnen anonieme gegevens met de juiste sleutel inzichtelijk gemaakt worden, waardoor herleiding naar natuurlijke personen weer mogelijk is. De AVG is wel van toepassing op gepseudonimiseerde gegevens.

Instrumenten:
- Beleid Privacy by Design
- Handleiding Privacy by Design (versie 3.0 CIP) [9]

3 NRGD verwerkt persoonsgegevens die accuraat en actueel zijn.

Dit betekent onder meer dat er sprake is van zorgvuldig beheer van gegevens (*betrouwbaarheid en integriteit*) en dat het voor betrokkenen mogelijk is om verzoeken met betrekking tot rectificatie van onjuiste persoonsgegevens in te dienen (*rechten van betrokkenen*).

- Het NRGD zorgt dat het de juistheid en actualiteit van de persoonsgegevens zoveel mogelijk waarborgt. Bijvoorbeeld door periodieke controles en/of controle op de input.
- Het NRGD zorgt dat het mogelijk is om gegevens aan te passen die onjuist, onvolledig of verouderd zijn.
- Het NRGD geeft invulling aan de rechten van betrokkenen conform het Protocol rechten van betrokkenen bij het verwerken van een (wijzigings)verzoek van een betrokkene.

Instrumenten:
- Protocol Rechten van betrokkenen
- Modellen voor de beantwoording van inzageverzoeken

Bronnen:
- Wijzigen of afmelden (nrgd.nl) op website NRGD

4 Het NRGD bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel.

Persoonsgegevens worden slechts bewaard zolang dit nodig is om de beschreven doelen te bereiken, of zolang als bepaald door een specifieke wet.

Elke overheidsorganisatie is verplicht om in een selectielijst maximale bewaartermijnen te bepalen, ook voor alle persoonsgegevens waarover het beschikt. Nadat de bewaartermijn is verstreken, is de organisatie verplicht om de persoonsgegevens te verwijderen of te anonimiseren. Persoonsgegevens kunnen meerdere doelen dienen. Hiermee moet rekening worden gehouden bij het vernietigen en het opstellen van de bewaartermijnen.

- Het NRGD bewaart persoonsgegevens niet langer dan noodzakelijk voor de doelen van de verwerking.
- Het NRGD stelt bewaartermijnen vast conform de selectielijst van het NRGD.
- Het NRGD wist gegevens wanneer deze niet langer noodzakelijk zijn voor het verwerkingsdoel.

[9] https://www.rijksoverheid.nl/documenten/rapporten/2018/02/19/handleiding-privacy-by-design

Instrumenten:
- Selectielijst van het NRGD
- Memo bewaartermijn Persoonsgegevens in de AVG
- Handreiking Bewaren van e-mail Rijksoverheid

Bronnen:
- https://www.tuxx.nl/bewaartermijnen/documenten/#

5 **Het NRGD is voor zover mogelijk open en transparant over de verwerking van persoonsgegevens aan de betrokkene, de samenleving en ketenpartners.**

Betrokkenen dienen te weten wat er met hun persoonsgegevens gebeurt, willen zij hun rechten kunnen uitoefenen. De informatie over de verwerking en de omgang met de gegevens en over de rechten van betrokkene dient eenvoudig toegankelijk en begrijpelijk te worden aangeboden. Dit gebeurt in een privacyverklaring.

- Het NRGD verstrekt de vereiste informatie over onze verwerkingsactiviteiten via de privacyverklaring op *www.nrgd.nl.*
- De privacy officer controleert de privacyverklaring periodiek op haar actualiteit.

Instrumenten:
- Privacyverklaring extern NRGD op www.nrgd.nl
- Privacyverklaring intern NRGD

Bronnen:
- (voor medewerkers NRGD: Privacy | Rijksportaal en P-Direkt (p-direkt.nl))

6 **Het NRGD zorgt dat persoonsgegevens veilig en vertrouwelijk worden verwerkt.**

Informatiebeveiliging
Het NRGD moet voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Het NRGD volgt de Gedragscode Integriteit Rijk en de Gedragsregeling voor de digitale werkomgeving. Het NRGD neemt passende organisatorische (bijvoorbeeld autorisatiebeleid) en technische maatregelen (bijvoorbeeld versleuteling) ter beveiliging van de persoonsgegevens.

Het NRGD maakt gebruik van de digitale weg om informatie met deskundigen, het College en leden van adviescommissies uit te wisselen. Daarbij kan het ook gaan om persoonsgegevens. Het is belangrijk om een passend beschermingsniveau toe te passen bij het ontvangen en versturen van dergelijke gegevens. Het NRGD werkt aan digitalisering van de aanvraag waardoor niet langer via de post en e-mail gegevens behoeven te worden verzonden.

Vanwege de aard van de stukken die aan leden van de adviescommissies en het College worden verstuurd heeft het NRGD aanvullende maatregelen getroffen. Deze worden verstuurd via de tool OurMeeting. Het is niet mogelijk deze stukken te downloaden en uit te printen. Als het nodig is om gegevens op een andere manier en versleuteld te versturen naar de ontvanger, verstuurt het NRGD deze bijvoorbeeld door middel van de Bestandenpostbus.

- Het NRGD verstrekt toegang tot persoonsgegevens alleen aan die medewerkers die toegang tot de gegevens nodig hebben en die toestemming hebben om gegevens verder te verwerken.
- Het NRGD volgt voor wat betreft de beveiliging van persoonsgegevens de BIO.
- Het NRGD verstuurt persoonsgegevens per e-mail versleuteld.

Datalekken
Een datalek is een inbreuk op de beveiliging van de persoonsgegevens die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking of toegang tot persoonsgegevens. Een datalek dient binnen 72 uur aan de AP worden gemeld en soms ook aan betrokkene.

- Een medewerker dient een datalek of het vermoeden ervan onverwijld te melden aan de privacy officer of chief information officer.
- Het NRGD volgt het Protocol datalekken voor de afhandeling van datalekken. De privacy officer en chief information officer handelen een datalek conform dit protocol af.

Instrumenten:
- Gedragscode Integriteit Rijk
- Gedragsregeling voor de digitale werkomgeving
- BIO (meest recente versie)
- Informatiebeveiligingsbeleid NRGD
- Autorisatiematrix NRGD
- Register datalekken NRGD
- Protocol datalekken NRGD
- Formulier datalekken NRGD
- Circulaire Datalekken JenV
- EHBI NRGD

7 Het NRGD kan verantwoording afleggen over de zorgvuldige verwerking van persoonsgegevens.

Accountability
Een overheidsorganisatie moet passende maatregelen nemen en die evalueren om de bescherming van persoonsgegevens te waarborgen. Aan de hand van documentatie moet de organisatie kunnen aantonen dat de privacyregels worden nageleefd. Deze verantwoordingsplicht (*accountability*) staat centraal in het nieuwe wettelijk privacy kader. Hieronder valt ook de controle en monitoring door de FG.

- Het NRGD neemt de nodige technische en organisatorische maatregelen om naleving van bovengenoemde uitgangspunten te kunnen waarborgen.

Register van verwerkingen
Elke verwerkingsverantwoordelijke dient een register van verwerkingsactiviteiten bij te houden. In dat register staat informatie over de gegevens die worden verwerkt. De persoonsgegevens zelf staan niet in het register.

- Het NRGD houdt een registratie van de verwerkingen bij .
- De privacy officer is verantwoordelijk voor het beheer van dit verwerkingenregister. Medewerkers van het Bureau NRGD moeten wijzigingen in de verwerkingen aan de privacy officer doorgeven. De Directeur Bureau NRGD heeft de verantwoordelijkheid om bij nieuwe verwerkingen (activiteiten/andere ICT systemen) de privacy officer en de FG op de hoogte te stellen. De FG houdt toezicht op het op juiste wijze verwerken van de verwerkingen in het register van verwerkingsactiviteiten (verwerkingenregister).
- Het NRGD volgt het DPIA-proces bij het starten van een nieuw project of bij wijziging van beleid en procedures zodat elke verwerking deugdelijk geregistreerd kan worden.

Gegevensdelingen met derde partijen
Bij het delen van persoonsgegevens al dan niet in het kader van contracteren met derden neemt het NRGD de verplichtingen van de AVG in acht. Het NRGD wil zich ervan vergewissen dat derde partijen behoorlijk en zorgvuldig met persoonsgegevens omgaan. Dit hoeft niet noodzakelijkerwijs te gaan over partijen waarmee een verwerkersovereenkomst mee afgesloten dient te worden. Denk hierbij aan partijen die een eigen verantwoordelijkheid hebben, zoals de accountant. Waar nodig wordt een verwerkersovereenkomst gesloten.

Instrumenten:
- BIO
- Werkprocessen Privacy NRGD (waaronder DPIA)
- AVG-register van verwerkingen (via JenV)
- Verwerkersregister
- Model verwerkersovereenkomst NRGD
- Verwerkersovereenkomst checklist

8 Het NRGD respecteert de rechten van de betrokkenen.

Het NRGD respecteert de rechten van betrokkenen. Dat betekent dat systemen, processen en de interne organisatie zodanig worden ingericht dat op de juiste manier gehoor kan worden gegeven aan verzoeken om inzage in persoonsgegevens. Bekend moet zijn wanneer en hoe, indien van toepassing, verzoeken van betrokkenen tot inzage in hun gegevens worden gehonoreerd. Het NRGD heeft een document Protocol rechten van betrokkenen opgesteld, waarin staat hoe het met verzoeken van betrokkenen omgaat. Tevens zijn er modellen voor de beantwoording van deze verzoeken.

Het Protocol rechten van betrokkenen biedt vuistregels, een stappenplan en een model voor de afhandeling van verzoeken om inzage in persoonsgegevens en bezwaar. Ook op de website van de AP is meer informatie over dit onderwerp te vinden.[10]

[10] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/voorbeeldoverzicht_bij_inzageverzoek_def.pdf

Het NRGD wijst betrokkenen in een privacyverklaring op hun rechten. Zij kunnen bij de AP een klacht indienen over de manier waarop NRGD met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

Instrumenten:
- Protocol rechten van betrokkenen
  Modellen voor de beantwoording van inzageverzoeken
- Privacyverklaring extern (incl. sollicitanten)
- Privacyverklaring intern

3 Privacy governance

3.1 Inleiding

Doel van dit hoofdstuk over de privacy governance is de verantwoordelijkheden op het gebied van de privacybescherming binnen het NRGD te waarborgen. De governancestructuur helpt het NRGD om zorgvuldig met persoonsgegevens om te gaan en verantwoording af te kunnen leggen over genomen beslissingen. Een robuuste beheersorganisatie is van belang voor de implementatie en handhaving van de principes en doelstellingen uit het privacy beleid.

Omgevingsveld
Het College is een zelfstandig bestuursorgaan en valt onder de politieke verantwoordelijkheid van JenV. Hoewel het NRGD een *zelfstandig* bestuursorgaan is, blijft de minister van JenV politiek verantwoordelijk voor compliance met wet- en regelgeving en dus ook de AVG. JenV faciliteert het NRGD in het compliance worden en blijven met de eisen van de AVG en zal het NRGD vragen om periodiek te rapporteren over compliance met betrekking tot de AVG.

Bronnen: https://www.rijksoverheid.nl/onderwerpen/rijksoverheid/zelfstandige-bestuursorganen Kaderwet zelfstandige bestuursorganen

De AP is de Nederlandse toezichthouder met betrekking tot het voldoen aan de vereisten van de AVG. Wanneer betrokkenen klachten hebben over hoe het NRGD omgaat met persoonsgegevens, kunnen zij terecht bij de AP. De Nationale Ombudsman kan eventueel ook nog een bemiddelende rol spelen tussen het NRGD en personen waarvan het NRGD gegevens verwerkt.

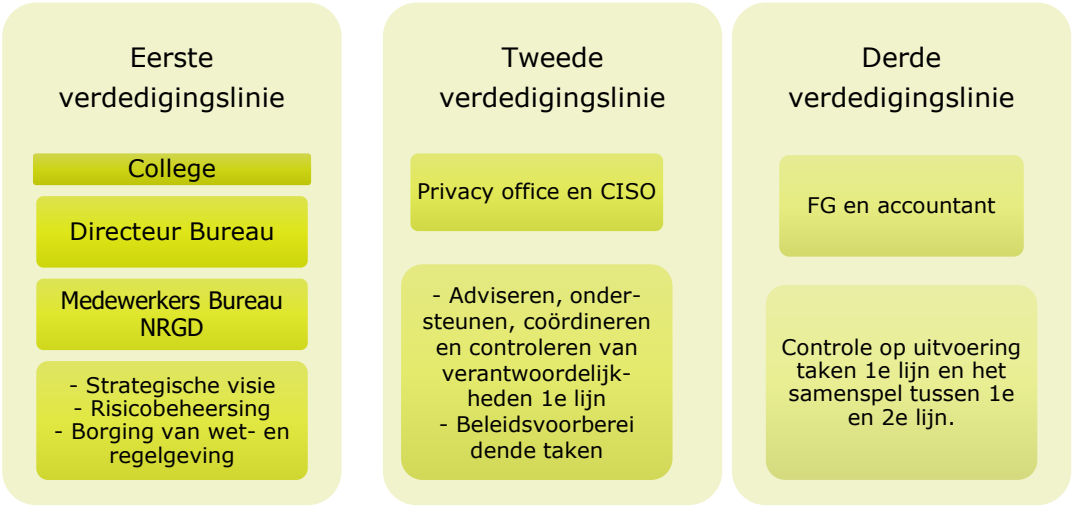
3.2 Drie verdedigingslinies

Het NRGD heeft drie linies waarin de verantwoordelijkheid voor de privacy valt. Het College is verwerkingsverantwoordelijke en als dusdanig verantwoordelijk voor een aantoonbare naleving van de wet- en regelgeving op het terrein van privacybescherming. De secretaris van het College, Directeur Bureau NRGD, is voor wat betreft de uitvoering als eerste verantwoordelijk voor het ontwikkelen van de strategische visie, de risicobeheersing en voor het borgen van de wet- en regelgeving op het terrein van privacybescherming binnen het NRGD. Iedere medewerker van het Bureau NRGD is verantwoordelijk voor een zorgvuldige omgang met persoonsgegevens. Daarom zijn ook zij een belangrijk onderdeel van de eerste verdedigingslinie.

In de tweede linie opereren de privacy officer en de chief information officer die de eerste lijn adviseren, ondersteunen en controleren bij zijn verantwoordelijkheden. Ook beleidsvoorbereidende taken en het organiseren van interne risicoanalyses zijn taken van de tweede lijn.

De derde linie wordt ingevuld door de Functionaris Gegevensbescherming (FG) en vaak ook de accountant vanwege hun specifieke rollen en wettelijke taken.

Externe toezichthouders, zoals AP maken geen onderdeel uit van deze ‘drie verdedigingslinies’. Het is de eigen verantwoordelijkheid van het NRGD om intern toezicht te houden op de waarborging van privacybescherming, los van eventuele externe audits en evaluaties.



Instrumenten:
- Mandaat- en ondermandaatregeling NRGD
- Jaarplan en jaarverslag Privacy Office
- Privacymanagement KPI's NRGD
- Jaarverslag FG

3.3 Privacy verantwoordelijkheden rollen en taken

Iedere medewerker is verantwoordelijk voor de naleving van dit privacybeleid. De verantwoordelijkheid voor de uitvoering van en de verantwoording ligt bij de directeur van het Bureau. Het College is accountable voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens.

Hieronder zijn de privacy functionarissen genoemd en vervolgens kort toegelicht.

Functionaris Gegevensbescherming (FG)
Het NRGD heeft een FG aangesteld overeenkomstig artikel 37 e.v. van de AVG. De FG rapporteert aan het College. In de AVG is de rol van de FG als volgt beschreven:
- informeren en adviseren van het NRGD over de verplichtingen uit hoofde van privacy wet- en regelgeving;
- toezien op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie;
- advies leveren bij een DPIA, zowel de inhoudelijke beoordeling als de naleving van de voorgenomen beheermaatregelen;
- samenwerken met de AP, de centrale toezichthouder, in het geval van onderzoek;
- aanspreekpunt voor betrokkenen (burgers en medewerkers) voor alle aangelegenheden bij de verwerking van hun persoonsgegevens.

Jaarlijks stelt de FG een Jaarverslag op in het kader van de toezichthoudende werkzaamheden.

Privacy officer
Het NRGD heeft een privacy officer die de volgende taken verricht. De privacy officer:

- ondersteunt en adviseert het NRGD in het naleven van de eisen uit dit privacy beleid en de privacy wetgeving;
- beheert het privacy beleid en kan op verzoek van het College en de directeur of uit eigen beweging een voorstel tot aanpassing van het beleid doen;
- adviseert de eerste lijn bij de analyse van mogelijke risico's die samenhangen met de verwerking van persoonsgegevens;
- fungeert als vraagbaak voor het College en de directeur ten aanzien van het verzamelen, registreren en leveren van persoonsgegevens. Hij of zij raadpleegt indien nodig de Functionaris Gegevensbescherming of externe adviseurs over complexere verwerkingen en relaties met verwerkers;
- zorgt voor de dagelijkse afhandeling van privacy aangelegenheden voor het NRGD;
- beheert de relevante privacy registers, waaronder het register van verwerkingsactiviteiten, (pre)DPIA register, verwerkersregister;
- coördineert de voorbereiding en begeleiding van DPIA's;
- monitoring van maatregelen en herijking van DPIA's;
- stelt de jaarplanning op.

CISO
Het onderwerp privacy en gegevensbescherming heeft een multidisciplinair karakter. Het vraagt om een zorgvuldige afstemming met de experts op het gebied van juridische zaken, ICT, beveiliging, communicatie, de privacy officer en de FG. De CISO is in eerste instantie verantwoordelijk voor de informationele privacy. De CISO ondersteunt en adviseert op verzoek het NRGD bij privacyvraagstukken. De CISO helpt onder meer door het geven van (zo mogelijk) advies op maat, is betrokken bij het uitvoeren van een DPIA, het opbouwen van de noodzakelijke kennis over privacy wet- en regelgeving, het toepassen hiervan en het (mede-)ontwikkelen van producten zoals informatiebeveiligingsbeleid waaronder autorisatiebeleid.

3.4 Privacy overlegstructuren

Overlegstructuren binnen NRGD
Op regelmatige basis vinden overleggen over privacy plaats. Er is een tweejaarlijks overleg van de privacy officer, de CISO, Directeur Bureau NRGD en de FG. Er is verder een vast tweemaandelijks overleg van de privacy officer en CISO met de FG.

Extern Privacynetwerk
Het NRGD participeert actief in overleggen van zowel Klein Lef organisaties (AVG-werkgroep) als JenV overleggen (Privacy- en CIO Board, Privacy Werkgroep) op het gebied van privacy om de kennis omtrent privacy te delen en elkaar te helpen om beleid omtrent privacy te ontwikkelen. Vanuit het samenwerkingsverband KleinLef is ook de FG betrokken.

3.5 Sturing, regie en toezicht

De privacy officer NRGD past het format beleidsplan van JenV aan, zorgt dat het passend is voor het NRGD en zorgt voor de bekendheid van het beleidsplan binnen het NRGD.

Periodiek, aan de hand van de KPI's JenV voert het NRGD self-assessments uit, waaruit blijkt wat de stand van zaken is met betrekking tot privacy. Het NRGD neemt periodiek deel aan de uitvraag van JenV conform de intentieverklaring NRGD.

De FG ziet toe op de naleving van de relevante wetgeving, het privacy beleid en de inrichting van de interne privacy organisatie.

Instrumenten:
- Relatiestatuut
- Intentieverklaring NRGD JenV
- JenV Privacymanagement KPI's

3.6 Privacy trainingen en bewustwording

Alle medewerkers van het Bureau NRGD zijn in dienst van JenV en vallen rechtspositioneel onder het Bestuursdepartement. Zij leggen de eed of gelofte af als rijksambtenaar. Vanuit J&V zijn er diverse bewustwordingsacties en trainingen over de AVG en privacy, zoals de modules Brons en Zilver van Weerbaar JenV.

Iedere nieuwe medewerker krijgt bij aanstelling een korte introductie AVG van de privacy officer van het NRGD. Medewerkers die in het kader van hun werkzaamheden meer verdieping nodig hebben, kunnen zich in overleg met de Directeur van het Bureau inschrijven voor een cursus op dat gebied. Daarnaast worden medewerkers ook geïnformeerd over de AVG en privacy door dit onderwerp met enige regelmaat te bespreken in de Bureau-overleggen (bewustwordingsacties).

Bijlage 1: Terminologie en achtergrond

Wat zijn persoonsgegevens?
Niet alle data of gegevens zijn per definitie persoonsgegevens. Persoonsgegevens betreft alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon (de “betrokkene”).

De betrokkene hoeft geen direct geïdentificeerd individu te zijn, maar zodra een individu uit een groep kan worden onderscheiden, zijn de gegevens persoonsgegevens. Het is dus niet altijd nodig om de naam te weten van de persoon in kwestie om te spreken van persoonsgegevens.

Alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare persoon moeten als persoonsgegevens worden beschouwd. Enkel transactiegegevens zijn bijvoorbeeld op zichzelf geen direct identificeerbare gegevens, maar worden persoonsgegevens wanneer deze verband houden met een geïdentificeerde of identificeerbare persoon, bijvoorbeeld omdat deze is gekoppeld aan een naam, een e-mailadres of een telefoonnummer.

De AVG heeft een speciaal regime voor bijzondere categorieën persoonsgegevens. Dit betreffen persoonsgegevens waaruit de raciale of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen blijken, lidmaatschap van een vakvereniging, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie, gezondheids- of medische gegevens, gegevens over iemands seksleven of seksuele geaardheid.

Strafrechtelijke persoonsgegevens zijn persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Hieronder vallen zowel veroordelingen als mogelijk gegronde verdenkingen. Dit wil zeggen dat er concrete aanwijzingen zijn dat iemand een strafbaar feit heeft gepleegd. Een voorbeeld hiervan is een opgestelde zwarte lijst van frauderende klanten bij een financiële instelling. Onder de AVG gelden speciale regels voor het verwerken van strafrechtelijke gegevens.

De verwerking, het verzamelen of gebruiken, van gevoelige persoonsgegevens, is verboden, tenzij een uitzondering op het algemene verbod van toepassing is. Het verzamelen en gebruiken van dergelijke gegevens zal daarom zoveel mogelijk worden vermeden. Vermijd ook het verzamelen en gebruik van gegevens van gevoelige groepen, zoals kinderen / minderjarigen, gehandicapten en ouderen, tenzij hiervoor duidelijk toestemming is gegeven door de bevoegde persoon.

Hieronder volgen voorbeelden van gegevens die over het algemeen als persoonsgegevens worden beschouwd:

Voornaam en / of initialen en achternaam	Financiële gegevens
E-mailadres	Betaling of transactiegegevens
Telefoonnummer	Rijbewijs
Foto	Strafrecht ketennummer

Geboortedatum / geboorteplaats	Identificatienummer werknemer
IP-adres	Werknemers informatie
Uitkomsten functioneringsgesprekken	Medische informatie
Burgerservicenummer	Biometrische gegevens
Unique Device Identifiers	MAC-adressen

Wat is een betrokkene?
De betrokkene is de persoon van wie persoonsgegevens worden verwerkt.

Wat is een verwerking?
Het 'verwerken van persoonsgegevens' of een 'verwerking van persoonsgegevens' betreft alle handelingen die men met persoonsgegevens kan verrichten. Denk hierbij aan het verzamelen, vastleggen, raadplegen, opvragen, ordenen, structureren, opslaan, bewerken of wijzigen, verstrekken en combineren. Zelfs het wissen of vernietigen van gegevens is een verwerking van persoonsgegevens.

Wat is een verwerkingsverantwoordelijke?
De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon die (alleen of tezamen met anderen) bepaalt welke persoonsgegevens worden verzameld, waarom persoonsgegevens worden verwerkt (doel) en hoe persoonsgegevens worden verwerkt (middelen). Wanneer partijen gezamenlijk het doel en de middelen vaststellen voor de verwerking van persoonsgegevens dan spreken we van een gezamenlijke verantwoordelijkheid.

Wat is een verwerker?
Een verwerker is de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Het gaat om derde partijen die voor de verwerkingsverantwoordelijke werken. Een verwerker handelt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies, maar er is geen hiërarchische relatie (medewerkers zijn geen verwerkers). Daarnaast heeft de verwerker geen zeggenschap over de verwerkingen en mag de gegevens niet voor eigen doelen gebruiken.

Bijlage 2: Instrumenten

Dit document wordt jaarlijks geüpdatet.

De meest recente versie van het document is

Bijlage 2 – Instrumenten Beleidsplan 2021

Bijlage 3: Privacy functionarissen NRGD

Soort functionaris	naam	e-mailadres
FG	Ella Schepel	e.t.schepel@nrgd.nl; e.schepel@rvr.org
Privacy Officer	Els de Jong	e.a.a.de.jong@nrgd.nl
CISO	Stephanie Pompies	s.pompies@nrgd.nl
contractbeheer	Cathy van Bekkum	c.p.m.van.bekkum@nrgd.nl
Van belang zijnde externe functionarissen (samenwerkende partijen)		
FG JenV	Pieter de Groot	p.j.de.groot@minvenj.nl
BVA/BVC	Hans Driessen	h.j.w.a.driessen@minjenv.nl
Privacy Officer JenV (CPO)	Pauline Verhaak	p.m.verhaak@minjenv.nl
Secretaris JenV Privacy Board	Céline Janssen	c.c.janssen@minjenv.nl
Secretaris Klein Lef	Anna Demoed	info@kleinlef.nl