Hoogheemraadschap van
Rijnland

Privacybeleid

hoogheemraadschap van Rijnland

Versie: 2.0
Datum: Juli 2020
Corsanr : 18.077531

Inhoudsopgave

Hoofdstuk 1: Inleiding

Bij het uitvoeren van zijn wettelijke taken verwerkt Rijnland persoonsgegevens.[1] Rijnland verwerkt persoonsgegevens van burgers, maar ook van medewerkers en (keten)partners. Gegevens van en over burgers, medewerkers en (keten)partners moeten bij Rijnland veilig zijn en hun privacy moet gewaarborgd zijn.

Sinds 25 mei 2018 is in de hele Europese Unie de Algemene Verordening Gegevensbescherming (AVG) van toepassing.[2] Daar waar de AVG ruimte laat om op nationaal niveau bepaalde vraagstukken (aanvullend) te regelen, is dit in Nederland gedaan door middel van de Uitvoeringswet Algemene Verordening Gegevensbescherming. [3]

De AVG legt organisaties meer verantwoordelijkheid op om aan te tonen dat zij voldoen aan de regels op het gebied van gegevensbescherming wanneer zij persoonsgegevens verwerken. Rijnland verwerkt persoonsgegevens, dus moet ook Rijnland voldoen aan deze verantwoordingsplicht (accountability). Dit betekent onder andere dat Rijnland moet kunnen aantonen dat:

a) een verwerking aan de belangrijkste beginselen van gegevensverwerking voldoet, zoals rechtmatigheid, transparantie, doelbinding en juistheid;
b) Rijnland ook moet kunnen laten zien dat de juiste technische en organisatorische maatregelen zijn genomen om de persoonsgegevens te beschermen.

Met het Privacy Beleidsstuk dat voor je ligt, geeft Rijnland duidelijke richting aan de wijze waarop de privacy binnen Rijnland wordt beschermd: het beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van Rijnland. Dit beleid laat zien hoe Rijnland op dagelijkse wijze omgaat met persoonsgegevens en privacy.

Bestuur en management spelen een cruciale rol bij het actief uitdragen van dit Privacybeleid. Het Privacybeleid van Rijnland is in lijn met de relevante nationale- en Europese wet- en regelgeving.

Dit Privacybeleid is ontwikkeld om structuur en een beleidskader te bieden bij het inrichten van de verplichtingen van de AVG en om daarover verantwoording te kunnen afleggen. Dit document maakt deel uit van het pakket aan maatregelen en documenten waarmee Rijnland voldoet aan zijn verantwoordingsplicht. Het doel van dit Privacybeleid is om de belangen van betrokkenen van wie Rijnland de persoonsgegevens verwerkt (burgers, ketenpartners en medewerkers) centraal te stellen. Daarnaast helpt dit beleid Rijnland zelf om te zien of er voldoende maatregelen zijn genomen om de bij Rijnland aanwezige persoonsgegevens te beschermen en vormt het tevens een

[1] De Algemene verordening gegevensbescherming (AVG) geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of organisaties zijn geen persoonsgegevens, maar er moet natuurlijk wel met gepast respect voor de overledene en diens nabestaanden omgegaan worden met diens persoonsgegevens.

[2] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

[3] Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van
27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en
betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming) (Stb. 2018, 144).

verantwoording dat Rijnland voldoet aan de AVG. Dit stuk is bestemd voor alle medewerkers van Rijnland en geeft aan waar Rijnland voor staat en wat Rijnland wil uitdragen.

Het beleid is vastgesteld en beoordeeld binnen de organisatie om te waarborgen dat gegevensverwerkingen op een rechtmatige wijze plaatsvinden. Het beleid bevat de visie en principes van de organisatie in het kader van de Privacy en wordt periodiek, of bij grote wijzigingen in de wetgeving beoordeeld om te controleren of het nog in voldoende mate aansluit op de realiteit.

Hoofdstuk 2 Algemeen

Wetgeving

Rijnland is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het Privacybeleid. Voor het Privacybeleid gelden onder andere de volgende wettelijke kaders:

- De Algemene Verordening Gegevensbescherming (AVG)
- De Uitvoeringswet Algemene Verordening Gegevensbescherming

Begrippenlijst

- Betrokkene:De betrokkene is degene van wie de gegevens worden verwerkt;;
- Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt (in opdracht van een andere persoon of organisatie);
- Persoonsgegevens: Alle gegevens waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een specifiek persoon (bijvoorbeeld: naam, adres, geboortedatum), maar ook het zorgvuldig omgaan met het BSN.
- Bijzondere Persoonsgegevens: Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, medische gegevens en politieke voorkeuren;
- Gegevensbeschermingseffectbeoordeling: Met een gegevensbeschermings-effectenbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een 'Data Protection Impact Assessment' (DPIA). Binnen Rijnland hanteren we het begrip DPIA;
- Verwerkingsverantwoordelijke: 'De persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt;
- Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander en vernietigen.

Reikwijdte

Het beleid is van toepassing op alle verwerkingen van persoonsgegevens die door of namens Rijnland als verwerkingsverantwoordelijke plaatsvinden.

Verantwoordelijke

Binnen de verantwoordelijkheids- en bevoegdheidsverdeling van Rijnland ligt de verwerkersverantwoordelijkheid bij het dagelijks bestuur. Het dagelijks bestuur stelt het Privacybeleid vast en de secretaris algemeen directeur (SAD) is als hoofd van de ambtelijke organisatie eindverantwoordelijk voor het uitvoeren van het Privacybeleid.

Hoofdstuk 3 Soorten verwerkingen

Verwerkingen **(artikel 4 AVG)**

De verwerking van persoonsgegevens is in elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In art. 4.2 van de AVG wordt de volgende definitie van 'verwerken' gegeven: *"een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens"*

Alhoewel dit artikel een tal van voorbeelden noemt, is deze lijst zeker niet limitatief. Kort gezegd komt het er op neer dat alles wat je kan doen met persoonsgegevens onder het begrip 'verwerken' valt. Het maakt daarbij niet uit of de handeling handmatig of automatisch wordt verricht.

Doeleinden **(artikel 5 AVG)**

Volgens de AVG mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Rijnland verwerkt alleen persoonsgegevens met een duidelijk en gerechtvaardigd omschreven doel. De gegevens worden niet voor andere doelen verwerkt. Deze doelen zijn gebaseerd op de (wettelijke) taken van Rijnland en de taken van Rijnland als werkgever.

Categorieën van persoonsgegevens

Rijnland verwerkt persoonsgegevens voor de uitoefening van de diverse waterschapstaken. Voorbeelden hiervan zijn contactgegevens van inwoners en van organisaties, zoals naam, adres, emailadres en telefoonnummer. Er worden voor deze taken geen bijzondere persoonsgegevens verwerkt.

Uit de verantwoordelijkheid van Rijnland als werkgever, vloeit voort dat van medewerkers van Rijnland naast de normale persoonsgegevens ook bijzondere persoonsgegevens kunnen worden verwerkt. Dit is gebaseerd op een wettelijke grondslag. Medewerkers worden hierover geïnformeerd via de Privacyverklaring voor medewerkers (Corsanr. 19.056271).

Rechtmatige grondslag **(artikel 6 AVG)**

De AVG vereist dat een verwerker een goede reden heeft om persoonsgegevens te verwerken. In de AVG staan 6 redenen genoemd. De juridische term voor die redenen is grondslagen. Rijnland verwerkt alleen persoonsgegevens met een rechtmatige grondslag, en dat zijn er voor Rijnland 5, omdat de 6e, 'vitaal belang' niet op het werk van Rijnland van toepassing is:

1. Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
2. Wanneer het noodzakelijk is om gegevens te verwerken voor de uitvoering van een overeenkomst;
3. Wanneer het noodzakelijk is om gegevens te verwerken om een wettelijke verplichting na te komen;
4. Wanneer het noodzakelijk is om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen;
5. Wanneer het verwerken van gegevens noodzakelijk is om een gerechtvaardigd belang te behartigen. Deze grondslag mag Rijnland niet gebruiken bij het uitvoeren van zijn publieke taak, maar alleen als zijn rol als werkgever of bijvoorbeeld als gebouweigenaar.

Wijze van verwerking

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de AVG én dat het op een zorgvuldige wijze gebeurt. Rijnland zorgt ervoor dat persoonsgegevens zoveel mogelijk bij betrokkenen zelf vandaan worden gehaald. Rijnland verwerkt alleen persoonsgegevens wanneer het doel niet op een andere manier kan worden bereikt.

In de AVG wordt ook gesproken over het vereiste van proportionaliteit. Rijnland verwerkt alleen persoonsgegevens als dat in verhouding staat tot het doel. Rijnland kiest altijd voor het gebruik van zo min mogelijk persoonsgegevens in relatie tot het te bereiken doel.

Rijnland hanteert een checklist voor het werken met persoonsgegevens, zie daarvoor BIJLAGE A bij dit beleidsstuk.

Hoofdstuk 4 Plichten van Rijnland

Informatieplicht **(Artikel 13 en 14 AVG)**

Rijnland informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan Rijnland geven, worden zij op de hoogte gesteld van de manier waarop Rijnland met hun persoonsgegevens om zal gaan, onder meer door te verwijzen naar de Privacy pagina op de website en de uitleg over de 'rechten van betrokkene' op dezelfde site.

Aanstellen van een Functionaris voor Gegevensbescherming (FG) **(artikel 37 t/m 39 AVG)**

Rijnland heeft een Functionaris voor Gegevensbescherming (verder: FG) aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren en optreden als contactpersoon van de Autoriteit Persoonsgegevens (AP). Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de organisatieclusters en teams binnen de organisatie overneemt. De teams hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een nieuwe verwerking van persoonsgegevens of een wijziging van een bestaande verwerking, wordt eerst aan de FG gemeld voordat de verwerking begint of de wijziging ingaat. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en richtlijnen op het gebied van privacy.

Voor vragen over privacy of over deze toelichting kan contact worden opgenomen met de Functionaris Gegevensbescherming van Rijnland via: privacy@rijnland.net. In geval van vakantie of ziekte van de FG treden de privacy-juristen op als waarnemend FG.

Register van verwerkingen **(Artikel 30, AVG)**

Rijnland houdt een register bij van alle verwerkingen waarvan Rijnland de verwerkingsverantwoordelijke is (het verwerkingenregister). De meest actuele versie van het verwerkingsregister is te vinden op de kennisgroep Privacy op intranet of via de zoekfunctie op intranet. Dit register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, indien van toepassing, de gezamenlijke verwerkingsverantwoordelijke, inclusief de noodzaak voor een (verwerkers)overeenkomst voor uitwisseling persoonsgegevens;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;

- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarbinnen de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

Beveiliging **(Artikel 32, AVG)**

Rijnland is verantwoordelijk voor de bescherming van persoonsgegevens. Dit betekent dat Rijnland het proces en de organisatie zo moet inrichten dat alle persoonsgegevens passend beveiligd worden. Hiervoor wordt waar mogelijk aangesloten bij informatiebeveiliging zoals dat binnen Rijnland geregeld is: op basis van het Beleid Informatiebeveiliging (corsanr. 13.38344) en de Baseline Informatiebeveiliging Overheden (BIO). De medewerkers zijn al via de BIO verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen. De geheimhoudingsplicht is voor vaste werknemers van Rijnland verankerd in de ambtseed of –belofte. Tijdelijke krachten die toegang hebben tot persoonsgegevens moeten een integriteits- en geheimhoudingsverklaring ondertekenen.

Ten behoeve van de AVG is het dataclassificatiemodel uitgebreid met de classificatie 'Privacy'. In het kader van de BIO en de AVG worden de systemen (en bijbehorende gegevens) dus geclassificeerd op:

- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid
- Privacy

Privacy by design **(Artikel 24, AVG)**

Om al in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens af te dwingen bij de ontwikkeling van producten en diensten past Rijnland het principe toe van privacy by design en Privacy by Default. Hiervoor is het 'architectuurprincipe 22' toegevoegd aan de eerder vastgestelde architectuurprincipes (corsanr. 15.053242). Voor iedere nieuwe verwerking van persoonsgegevens (of grote wijziging) wordt een risico-inventarisatie uitgevoerd ten aanzien van de bescherming van de persoonsgegevens.

Gegevensbeschermingseffectbeoordeling **(Artikel 35, AVG)**

Met een gegevensbeschermingseffectbeoordeling ofwel een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Rijnland voert deze uit wanneer er sprake is van een grootschalige verwerking of wanneer een grootschalige monitoring van openbare ruimten plaatsvindt. Als er bijzondere persoonsgegevens worden verwerkt, kan dit een extra reden zijn om een DPIA uit te voeren. Een DPIA is in het bijzonder gewenst bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

Verwerkersovereenkomsten **(artikel 28 AVG)**

Soms schakelt Rijnland een externe partij in voor het verwerken van persoonsgegevens. Als die partij *hoofdzakelijk* is ingeschakeld voor het verwerken van persoonsgegevens, dan is die partij een verwerker in de zin van de AVG. In dat geval blijft Rijnland wel verantwoordelijk voor de verwerking van de persoonsgegevens. Daarom worden met partijen die namens Rijnland persoonsgegevens verwerken verwerkersovereenkomsten gesloten. Het sluiten van deze overeenkomsten is verplicht. In deze overeenkomsten is onder meer geregeld met welk doel en op welke wijze de persoonsgegevens mogen worden verwerkt; welke veiligheidsmaatregelen er getroffen moeten worden; waar de persoonsgegevens worden opgeslagen; de mogelijkheden om een audit uit te voeren en of de verwerker subverwerkers (andere partijen die namens hen weer persoonsgegevens verwerken) mag inschakelen. Verder is in de overeenkomst geregeld hoe partijen omgaan met datalekken en wie de schade die door een datalek ontstaat moet vergoeden, hoe de overeenkomst eindigt en wat er dan met de verwerkte persoonsgegevens gebeurt.

Een verwerkersovereenkomst bestaat altijd naast een contract voor een product en/of dienstverlening. Rijnland gebruikt hiervoor de 'Template Verwerkersovereenkomst' die in samenspraak met de Unie van Waterschappen is opgesteld. Deze wordt jaarlijks geëvalueerd en aangepast waar nodig op basis van eventuele nieuwe wetgeving en/of jurisprudentie. De juristen van het kernteam Privacy dragen zorg voor een correcte inhoud van de template. De leden van het kernteam kunnen ondersteuning bieden aan de procesmanager en/of contracteigenaar bij het opstellen van en onderhandelen over de verwerkersovereenkomst. Voor invulling van de technische en beveiligingsmaatregelen wordt aan een IT-medewerker om advies gevraagd.

In bepaalde gevallen heeft Rijnland een partij ingeschakeld om bijvoorbeeld een waterschapsgerelateerd werk uit te voeren, maar is het in het kader van die uitvoering ook nodig dat die partij persoonsgegevens verwerkt. Het verwerken van de persoonsgegevens is in zo'n geval *bijkomstig* aan het hoofddoel van de overeenkomst met de externe partij. Het hoofddoel is namelijk het uitvoeren van het waterschapsgerelateerd werk en niet het verwerken van persoonsgegevens. In zo'n geval zijn er twee verwerkingsverantwoordelijken, zowel Rijnland als de ingeschakelde partij, en is het nuttig om een zogenaamde allonge (een verwerkers-verantwoordelijkenovereenkomst) af te sluiten. Hierin maak je gezamenlijk afspraken over hoe wordt omgegaan met de persoonsgegevens. Ook de allonge bestaat altijd naast een contract voor een product en/of dienstverlening. Rijnland gebruikt hiervoor de 'Template allonge'.

Zowel de verwerkersovereenkomst als de allonge worden altijd samen met het contract geregistreerd in MyCORSA. Tevens worden beide documenten opgevoerd in het contractenregister bij Inkoop, zodat altijd een goed overzicht bestaat van de geldende (en aflopende) afspraken met verwerkers. In het verwerkingenregister wordt de betreffende verwerking rechtstreeks gelinkt aan de afgesloten verwerkersovereenkomst of allonge.

Samenwerkingsverbanden

Rijnland werkt samen in diverse verbanden met andere overheden en organisaties. Indien er tussen deze organisaties doorgifte en/of verwerking van persoonsgegevens plaatsvindt als onderdeel van de overeengekomen samenwerking waarbij beide organisaties beide verwerkersverantwoordelijken zijn, worden er aanvullend op de samenwerkingsovereenkomst, afspraken gemaakt over de uitwisseling van persoonsgegevens. De Belastingsamenwerking Gouwe-Rijnland (BSGR) en Aquon (beiden zijn gemeenschappelijke regelingen waar Rijnland in deelneemt) zijn voorbeelden van samenwerkingsverbanden. Deze zelfstandige rechtspersonen hebben een eigen verantwoordelijkheid voor het verwerken van persoonsgegevens.

Melden en afhandelen datalekken **(Artikel 33, 34, AVG)**

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Rijnland heeft een Incident Response Plan (corsanr 18.039640) voor het melden van datalekken. In het plan staan de stappen, taken en verantwoordelijkheden beschreven bij het melden van een datalek. Voor meldingen met betrekking tot informatiebeveiliging en privacy is er een eenduidig loket via Topdesk Selfservicedesk dat open staat voor alle interne meldingen. Voor externe meldingen is er op de website van Rijnland een webformulier beschikbaar. Deze meldingen dienen door leden van het kernteam zelf in de Topdesk Selfservicedesk te worden geregistreerd. Datalekken moeten binnen 72 uur na ontdekking ervan worden gemeld aan de Autoriteit Persoonsgegevens (AP). Dat betekent dat elke werknemer van Rijnland de verantwoordelijkheid heeft om vermoedens van een datalek zo snel mogelijk te melden via de Topdesk Selfservicedesk. Of een gemeld lek moet worden gemeld bij de AP wordt beoordeeld door het Incident Response Team (IRT) en namens de lijnverantwoordelijke uitgevoerd door de FG. Van de gemelde (vermoedelijke) datalekken en van de meldingen aan de AP wordt periodiek gerapporteerd aan de portefeuillehouder en het Dagelijks Bestuur.

Doorgifte **(Artikel 44 t/m 50, AVG)**

Rijnland geeft geen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie.

Wet openbaarheid van Bestuur **(Wob)**

Via de Wob (en straks wellicht de Wet Open Overheid) bestaat de mogelijkheid om een verzoek om informatie in te dienen bij Rijnland. Bij het reageren op het verzoek zorgt Rijnland ervoor dat de over te leggen documenten waar nodig geanonimiseerd zijn.

Wet hergebruik van overheidsinformatie

De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt Rijnland of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen.

Actief verwijderen van persoonsgegevens

Rijnland bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van de taken, of zoals vastgelegd in diverse wetten zoals bijvoorbeeld de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren. Rijnland stelt hiervoor onder andere een bewaartermijnprocedure op.

Informatie over de inzet van camera's

Bij de locaties van Rijnland worden camera's ingezet ter beveiliging van personen en goederen. Deze beelden mogen alleen voor dit doel worden gebruikt. Hiertoe worden alleen de openbaar toegankelijke ruimtes en de uitgangen gefilmd. Bij de ingang van een gebouw met cameratoezicht moet worden wordt er gewezen op het cameratoezicht. Op deze verwerking moet een DPIA worden uitgevoerd, zodat goed wordt vastgelegd of er beelden worden bewaard en zo ja, hoe lang en waar, en wie ze kan inzien. Als de beelden bij een derde staan, moet er een verwerkersovereenkomst zijn. (Bij het opmaken van dit beleidsstuk (juni 2020) is deze DPIA voor Rijnland nog niet uitgevoerd, waardoor nog niet helder is of aan alle voorwaarden wordt voldaan. De planning is om deze DPIA uit te voeren zodra het plan voor Fysieke Toegangsbeveiliging gereed is.)

Privacy bewuste organisatie

Medewerkers van Rijnland zijn zich bewust van de noodzaak om persoonsgegevens van medewerkers en burgers veilig en discreet te behandelen. Medewerkers zijn en worden getraind in het beschermen van persoonsgegevens en aspecten van informatiebeveiliging door middel van awarenessprogramma's. Rijnland evalueert de effectiviteit van de awarenesstrajecten.

Big Data

De essentie van Big Data is het verzamelen, combineren en analyseren van zoveel mogelijk data. Dit staat echter op gespannen voet met privacywetgeving die uitgaat van dataminimalisatie. In dit beleid benadrukken we dat ook voor Big Data analyse, net als voor alle overige verwerkingen de Privacy By design uitgangspunten onverminderd van toepassing zijn. Persoonsgegevens mogen dus niet worden verwerkt als onderdeel van Big Data analyse. Dit geldt ook voor gegevens die (direct of indirect) herleidbaar zijn tot een persoon. Om dit af te dwingen zullen Big Data alleen door geautoriseerde personen mogen worden verzameld.

Alleen in uitzonderlijke gevallen waar er toch een rechtmatige grondslag blijkt voor Big Data analyse op datasets waar persoonsgegevens in kunnen zitten]dan zullen deze eerst met uiterste zorg geanonimiseerd, of gepseudonimiseerd moeten worden.

Hoofdstuk 5 Rechten van betrokkenen

De AVG bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden de rechten van betrokkenen genoemd.

Op de website van Rijnland is via de privacypagina de mogelijkheid gegeven voor het uitoefenen van hun rechten van betrokkenen.

Per recht van betrokkenen geldt een aparte werkinstructie met vermelding van de daarbij behorende wettelijke termijnen uit de AVG. De rechten van betrokkenen zijn ook beschreven in de privacyverklaring die op de website van Rijnland staat. Het streven is om zo spoedig mogelijk en minimaal binnen de wettelijke termijn de privacy verzoeken te behandelen. De afhandeling van een privacy-vraag van een externe wordt ook in Topdesk geregistreerd (door een lid van het kernteam Privacy).

De rechten van betrokkenen bestaan uit de volgende rechten:

- *Recht op informatie (artikel 13 en 14 AVG)*
  Betrokkene moet op de hoogte worden gesteld van het feit dat verwerking van zijn persoonsgegevens plaatsvindt of zal plaatsvinden en wat de doeleinden hiervan zijn;

- *Recht van inzage (artikel 15 AVG)*
  Betrokkenen hebben het recht te weten of hun betreffende persoonsgegevens worden verwerkt door de verantwoordelijke;

- *Recht op rectificatie (artikel 16 AVG)*
  Betrokkene heeft recht op rectificatie van hem betreffende onjuiste persoonsgegevens dan wel het recht een aanvullende verklaring te verstrekken wanneer de verwerking plaatsvindt op basis van onvolledige gegevens;

- *Recht op gegevenswissing/vergetelheid (artikel 17 AVG)*
  De verwerkingsverantwoordelijke is verplicht persoonsgegevens van de betrokkene zonder onredelijke vertraging te wissen;

- *Recht op beperking van de verwerking (artikel 18 AVG)*
  Het recht op beperking houdt in dat de persoonsgegevens (tijdelijk) niet verwerkt mogen worden en niet gewijzigd mogen worden;

- *Recht op overdraagbaarheid/dataportibiliteit (artikel 20 AVG)*
  Dit recht houdt in dat een betrokkene de gegevens van een verwerkingsverantwoordelijke moet kunnen verkrijgen in gestructureerde, gangbare en machineleesbare vorm en het recht heeft deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen of rechtstreeks te laten overdragen, zonder daarbij te worden gehinderd tenzij dit afbreuk doet aan rechten en vrijheden van anderen;

- *Recht van bezwaar (artikel 21 AVG)*
  Een betrokkene kan vanwege redenen die verband houden met zijn specifieke situatie gebruik maken van dit recht van bezwaar tegen de verwerking van hem betreffende persoonsgegevens, als voldaan wordt aan de in de verordening genoemde eisen;

- *Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profiling (artikel 22 AVG)*
  Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen.

Hoofdstuk 6 Privacy governance

Om te borgen dat privacybeleid niet een dode letter wordt en de uitvoering ervan stelselmatig wordt geëvalueerd voor verbeteringen zal Rijnland de zogenaamde Plan Do Check Act cyclus (PDCA-cyclus) gaan hanteren:

- Plan: planvorming, beleidsvorming, risicoanalyse
- Do: implementatie
- Check: monitoring, evaluatie en controle
- Act: nemen van maatregelen ter verbetering

- **P**lan: de cyclus start met Privacybeleid, gebaseerd op wet- en regelgeving (AVG), landelijke normen zoals de BIO en best practices. Dit beleid wordt uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving (privacyplan). Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. Vaktechnische- dan wel teamspecifieke activiteiten worden bij voorkeur opgenomen in plannen van vakafdelingen of teamspecifieke plannen .
- **D**o: het beleidskader is de basis voor risicomanagement, uitvoering van (technische en organisatorische) maatregelen en bevordering van privacybewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.
- **C**heck: control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van privacy processen, informatie en ICT en compliance aan wet- en regelgeving. Externe controle betreft de controle (buiten het primaire proces) door een auditor. Dit heeft het karakter van een steekproef. Jaarlijks worden meerdere van dergelijke onderzoeken uitgevoerd. Bevindingen worden opgenomen in de rapportage door de FG. Indien nodig wordt het privacybeleid hierop tussentijds bijgesteld.
- **A**ct: de cyclus is rond met de uitvoering van verbeteracties o.b.v. check en (eventueel) externe controle. De cyclus is een continu proces, waarbij de bevindingen van controles input vormen voor het privacybeleid, de jaarplanning en privacyplannen. De bevindingen worden in beginsel gerapporteerd aan de directie; voor ingrijpende verbeteracties wordt een verbetervoorstel gedaan.

Bij de uitvoering van de PDCA-cyclus zal worden aangesloten op de bestaande risicomanagement- en Planning & Control-cyclus van Rijnland. Het streven is om de PDCA-cyclus uiterlijk in 2022 te sluiten, zodat we kunnen voldoen aan het CBCF besluit van 15 mei 2020 om dan op volwassenheidsniveau 4 te functioneren als Rijnland. Om dit op een controleerbare wijze te doen is het noodzakelijk dat Rijnland de beschikking heeft over een zogenaamd 'ISMS-tooling' (ISMS is een Information Security Management System, die ook geschikt is voor Privacy. Op het moment van vaststelling van dit beleid (16 juli 2020) is een dergelijk tool nog niet aangeschaft, maar wordt gewerkt aan de aanbesteding. De planning (juni 2020) is, dat in het 3^{e} kwartaal van 2020 een dergelijk tool geïmplementeerd kan gaan worden.

Hoofdstuk 7 Organisatie van privacy

Rijnland is sinds enige tijd vóór de invoering van de AVG gestart met opzetten van een privacy-organisatie. In de eerste periode was de FG daarin vooral spin-in-het-web en aanjager/schrijver van alle voorgeschreven stukken en overzichten
Het uiteindelijke doel is een privacy-organisatie die in control is, met de FG in de zogeheten derde lijn.

4 lines of defense-model

Privacy is binnen Rijnland ingericht volgens het '4 lines of defense'-model. Dit houdt in dat privacy-gerelateerde taken op vier verschillende niveaus binnen of buiten de organisatie belegd zijn.

Het model bestaat uit de volgende vier lagen:

1st line – uitvoering: leidinggevenden en proceseigenaren (beheersmaatregelen en interne controls)
2nd line – Kernteam Privacy (monitoring en advies)
3rd line – intern toezicht : Functionaris Gegevensbescherming
4th line – extern toezicht: Autoriteit Persoonsgegevens en externe audits

1st line – teamleiders en proceseigenaren
Het uitgangspunt van dit model is dat iedere leidinggevende/proceseigenaar als eigenaar van de informatie verantwoordelijk is voor de bescherming van persoonsgegevens in het eigen proces. Die verantwoordelijkheid bestaat onder andere uit het correct toepassen van de principes van de AVG in het proces en het bekend zijn met bijbehorende beleid en protocollen zoals bijvoorbeeld het protocol 'meldplicht datalekken'. Ook is de leidinggevende verantwoordelijk voor het correct en volledig (laten) invullen van de verwerkingen in het verwerkingenregister. Hierdoor is ten allen tijden een actueel beeld van alle verwerkingen van persoonsgegevens beschikbaar voor Rijnland en voor de toezichthouder. De leidinggevenden van ieder cluster wijzen gezamenlijk contactpersonen Privacy aan (minimaal 2 per cluster) die de verbinding vormen tussen eerste en tweede lijn en structureel overleg hebben met de FG en waar nodig met andere leden van het kernteam. Ook de leidinggevenden van de stafafdelingen wijzen gezamenlijk een contactpersoon Privacy aan.

2nd line – kernteam Privacy
De tweede lijn is ingericht om de organisatie te helpen bij het inrichten en beheersen van privacy. Zij ondersteunen de eerstelijns/procesmanagers door het beantwoorden van vragen, het geven van advies en het opzetten en monitoren van kaders zoals beleid en protocollen. De tweede lijn bestaat uit het kernteam Privacy. Dit team heeft naast een adviesfunctie ook uitvoerende taken op het gebied van meldplicht datalekken. Deze zijn vermeld in het Incident Respons Protocol t.b.v. datalekken.

Het beheersen bestaat voor een groot deel uit het begeleiden, coördineren en monitoren van gemaakte afspraken met de eerste lijn en of zij daadwerkelijk hun verantwoordelijkheden ten opzichte van het Privacybeleid nemen en de principes op de juiste wijze toepassen. Hierbij wordt gevraagd en ongevraagd advies gegeven. Het kernteam Privacy bestaat uit functionarissen vanuit verschillende vakgebieden: juridische zaken, ICT en communicatie. De FG zit de kernteam Privacy voor. De spil van het kernteam Privacy is de juridisch adviseur omdat de meeste meldingen een verzoek om juridisch advies betreffen.

Het kernteam Privacy van Rijnland werkt samen met het kernteam Privacy van het hoogheemraadschap van Schieland en de Krimpenerwaard. Door het gezamenlijk aanpakken van privacy en informatiebeveiliging ontstaat er synergie die het mogelijk maakt om middelen en capaciteit efficiënter en effectiever in te zetten en kennis optimaal te delen.

3rd line – Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (verder FG genoemd) is een derdelijns-functie die niet betrokken is met de operationele uitvoering, maar juist toezicht houdt en toetst hoe de bescherming van persoonsgegevens binnen Rijnland opgepakt wordt.

De derde lijn toetst in hoeverre het samenspel tussen de '1st line' en '2nd line' naar behoren functioneert en de beoogde doelstellingen behaald worden, zoals aangegeven in dit beleidsstuk en in jaarplannen. Daar wordt een objectief en onafhankelijk oordeel over uitgebracht met bevindingen en mogelijkheden tot verbetering. De beoogde ISMS tool moet waarborgen dat in de opvolging van deze bevindingen, verbeteringen kunnen worden belegd binnen het proces planning & control (PDCA cyclus).

De FG is volledig onafhankelijk van de uitvoering op gebied van privacy en heeft directe escalatiemogelijkheden op directieniveau en dagelijks bestuur.

De FG is het Rijnland-aanspreekpunt voor de AP. Communicatie tussen de AP en de Rijnland geschiedt altijd en enkel met medeweten van de FG. Rijnland deelt de contactgegevens van de FG mee aan de AP. Medewerkers van Rijnland kunnen contact opnemen via het kernteam Privacy of direct met de FG. Burgers kunnen contact opnemen via de reeds bestaande kanalen (deze staan op de website). In geval van de afhandeling van een datalek worden de kanalen situationeel vastgesteld en naar de betrokken doelgroepen gecommuniceerd.

De FG heeft geen formele sanctiebevoegdheden. Maar Rijnland ondersteunt de FG met de volgende maatregelen:

- De FG is bevoegd om ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen om zijn wettelijke taken uit te voeren. Hiertoe maakt de FG eigen keuzes, zonder instructie omtrent de uitvoering van zijn taak;
- De FG heeft voor de uitvoering van zijn taken dezelfde ontslagbescherming als de leden van de OR;
- De FG is met betrekking tot de uitvoering van zijn taken tot geheimhouding en vertrouwelijkheid gehouden;
- De FG brengt rechtstreeks verslag, met medeweten van het DT, uit aan het Dagelijks Bestuur.

Scheiding 2nd en 3rd line

De onafhankelijkheid van de FG is essentieel voor een zuivere werking van het '4 lines of Defense'-model. Zodoende worden de taken van de FG niet vermengd met uitvoerende taken van het kernteam Privacy. Het kernteam Privacy heeft namelijk een beperkte mate van onafhankelijkheid in verband met het inrichten van privacy en de adviezen die hij/zij geeft aan de organisatie.

Voor de duidelijkheid is hieronder een overzicht gemaakt van de verdeling van taken tussen de lijnorganisatie, het kernteam Privacy en de FG.

Onderwerp	Leidinggevenden en proceseigenaren	Kernteam Privacy	Functionaris Gegevensbescherming
Welke 'line of defense'	1st line of defense	2nd line of defense: Leden kernteam Privacy	3rd line of defense: Intern toezichthouder Privacy
Relatie met de Autoriteit Persoonsgegevens (AP)	-	Mogelijk advies vragend, incident meldend.	Formeel aanspraakpunt
Invulling rol op hoofdlijnen	Uitvoerend	Adviserend, monitorend en uitvoerend.	Toezichthoudend en controlerend.
Kerntaak	Toepassen van de principes van de AVG in het proces.	Adviseren en ondersteunen van eerste lijn voor verbeteren implementatie Privacy in de organisatie.	Toezicht houden en controleren van functioneren kernteam Privacy.
Taken			
Privacy kader	Correct toepassen van de principes van de AVG in het proces uitvoering geven aan beleid en protocollen.	• Opstellen en/of adviseren over interne regelingen, beleidsregels en procedures.	• Toetsen interne regelingen, beleidsregels en procedures.
Verwerkingen in beeld hebben/houden	(Laten) invullen van de verwerkingen in het verwerkingenregister.	• Inventarisatie maken Verwerkingsregister Beheren; • Afspraken maken over eventuele verbeteringen met procesmanagers, OSO's en contract-eigenaren van verwerkingsovereenkomst; • Meldingen van gegevensverwerking bijhouden.	• Toezicht houden op kwaliteit en actualiteit verwerkingenregister; • Toezicht houden op de meldingen van verwerkingen; • Eigenaar van het verwerkingsregister.
Meldingen over verwerkingen	Invullen van de verwerkingen in het verwerkingenregister.	Meldingen van gegevensverwerkingen bijhouden.	Overzicht van meldingen van gegevensverwerkingen beoordelen.
Meldplicht datalekken	Signaleren en melden datalekken	• Opstellen protocol/plan; • Oppakken (potentiele) datalekken; • Bijhouden register datalekken.	• Toetsen werking van protocol/plan; • Controleren register datalekken.
Vragen en klachten van binnen en buiten de organisatie	Signaleren en melden.	Oppakken/behandelen.	Toetsen van procedure en afhandeling.
Privacy enhancing technologies	Toepassen van PET.	Adviseren over en ondersteunen van toepassing PET.	Toezicht houden op de toepassing van PET.

(PET)			
Gedragscodes	Opstellen van en naleven van gedragscodes.	Input leveren bij het opstellen of aanpassen van een gedragscode.	Beoordelen gedragscode.
Rapporteren	Input leveren voor rapportage.	Opstellen management rapportage Privacy.	Onafhankelijk oordeel geven over management rapportage privacy.
Audit	Input leveren voor Audit.	Meewerken aan en inplannen van een audit.	Opdrachtgeven voor en oordeel vormen over audit (rapport).

4th line – Autoriteit Persoonsgegevens en de externe audit

De vierde lijn staat buiten de organisatie en is uitsluitend voor toezicht houden en toetsen. Uiteraard gaat het hier over de extern toezichthouder: de Autoriteit Persoonsgegevens (AP). Daarnaast bestaat de mogelijkheid om periodiek extern te laten auditen op gebied van privacy. Dit zal jaarlijks plaatsvinden op basis van de 'CIP privacy baseline' van het Centrum informatiebeveiliging en privacybescherming. Externe partijen die op enige wijze betrokken zijn bij het tot stand komen en/of implementatie van de privacy en/of informatiebeveiliging binnen Rijnland, worden uitgesloten van het uitvoeren van deze externe audits op gebied van privacy en informatiebeveiliging. De FG regelt de periodieke externe privacy-audits en betrekt hierbij de Privacy Desk voor wat betreft het kader en specifieke aandachtsgebieden.

Bijlage A: Checklist voor het werken met persoonsgegevens

Uitgangspunten bij het werken met persoonsgegevens	
1	**Doel** Heb ik vooraf een doel voor de verwerking van persoonsgegevens vastgesteld?
2	**Doelbinding** Worden de persoonsgegevens alleen gebruikt voor het doel dat ik heb vastgelegd?
3	**Grondslag** Is er minimaal een wettelijke grondslag voor de verwerking? • Ik heb aantoonbare toestemming van de burger of werknemers • De gegevens zijn nodig voor de uitvoering van een overeenkomst • Het verwerken van deze gegevens is wettelijk verplicht • De verwerking van gegevens is nodig voor het uitvoeren van onze publiekrechtelijke taak • Er is een gerechtvaardigd belang dat ik kan uitleggen aan de burgers of werknemers
4	**Kwaliteit** Zijn de te gebruiken gegevens: • Actueel • Nauwkeurig • Juist
5	**Dataminimalisatie** • Gebruik ik alleen die gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? • Bewaar ik deze gegevens niet langer dan nodig?
6	**Transparantie** • Heb ik de burgers of werknemers vooraf geïnformeerd over het doel van de gegevensverwerking? • Heb ik uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld?
7	**Geheimhoudingsplicht** • Ik ben mij ervan bewust dat ik bij het gebruik van persoonsgegevens een geheimhoudingsplicht heb van de gegevens en de afleidbare informatie • Heb ik een verwerkersovereenkomst gesloten met degene die de persoonsgegevens voor mij verwerkt (indien van toepassing)?
8	**Meldplicht Beveiligingsincidenten** Bij verlies of diefstal van persoonsgegevens of als ik een vermoeden heb van een datalek weet ik dat ik dit moet melden in Topdesk.