PRIVACY BELEID HOLLAND RIJNLAND

Status:	Door:	Datum:
Goedgekeurd:	Management Team	15 mei 2023
Goedgekeurd:	Dagelijks Bestuur	01 juni 2023
Vastgesteld:	Algemeen Bestuur	28 juni 2023

Inhoudsopgave

Visie privacy

De komende jaren zet de Gemeenschappelijke Regeling Holland Rijnland in op het verhogen van de privacy bewustwording en de verdere professionalisering van de privacy functie in de organisatie. Dit omvat een adequate privacy boekhouding en is de basis voor de bescherming van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Verantwoord en bewust gedrag van alle medewerkers is hierbij essentieel. Bij naleving van de privacy wetgeving staat de doelmatigheid van de bedrijfsprocessen op de eerste plaats.

Doel

Het privacy beleid biedt een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van personen waarvan de Gemeenschappelijke Regeling Holland Rijnland gegevens verwerkt of laat verwerken. De uitwerking van het privacy beleid is vastgelegd in procedures en werkinstructies. De taken en verantwoordelijkheden op het gebied van Gegevensbescherming binnen de organisatie worden beschreven en toebedeeld. De Gemeenschappelijke Regeling Holland Rijnland onderschrijft het strategisch regionaal gemeentelijk informatiebeveiligingsbeleid van de gemeente Leiden en heeft haar ICT aan uitbesteed. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens.

Iedere werknemer is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeenschappelijke regeling Holland Rijnland verlangt van al haar medewerkers dat de voorschriften van dit privacy beleid worden opgevolgd en actief worden uitgedragen. De gemeenschappelijke regeling Holland Rijnland verzamelt en gebruikt persoonsgegevens van inwoners, medewerkers en andere betrokkenen. Dit privacy beleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeenschappelijke regeling Holland Rijnland. Dit beleid is echter niet van toepassing op organisaties die onder mandaat van de gemeenschappelijke regeling Holland Rijnland persoonsgegevens verwerken.

Principes bij de verwerking van persoonsgegevens

Bij de verwerking van persoonsgegevens hanteert de gemeenschappelijke regeling Holland Rijnland zich op de wettelijke principes van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politie Gegevens (WPG) en verwerkt persoonsgegevens in overeenstemming met deze wetten.

Rechtmatige grondslag

Persoonsgegevens worden verwerkt op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat.

Welbepaald doel

Persoonsgegevens worden verwerkt voor uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeenschappelijke regeling Holland Rijnland alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeenschappelijke regeling

Holland Rijnland ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken ter bescherming van de persoonlijke levenssfeer.

Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeenschappelijke regeling Holland Rijnland voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeenschappelijke regeling Holland Rijnland bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan wordt bij voorkeur gekozen voor die mogelijkheid.

Juist en actueel

De gemeenschappelijke regeling Holland Rijnland zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. De gemeenschappelijke regeling Holland Rijnland neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Op tijd gegevens vernietigen

De gemeenschappelijke regeling Holland Rijnland stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Op grond van de Archiefwet 1995 worden zogenaamde selectielijsten opgesteld. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt het Dagelijks Bestuur van de gemeenschappelijke regeling Holland Rijnland de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. Holland Rijnland bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Integer en vertrouwelijk

De gemeenschappelijke regeling Holland Rijnland neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. Het informatiebeveiligingsbeleid beveiligt de informatie tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking conform het BIO-normenkader.

Privacy by Design/Default

De gemeenschappelijke regeling Holland Rijnland houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt Privacy by Design (PbD) genoemd. De gemeenschappelijke regeling Holland Rijnland draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij wordt Privacy by Default (Pbd) als uitgangspunt genomen: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Toegang

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid en het beleid vastgesteld door de afdelingsmanagers. Het beheer van bevoegdheden wordt periodiek gecontroleerd door de leidinggevende. De gemeenschappelijke regeling Holland Rijnland hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Inbreuk

Bij toegang tot en noodzakelijk zijn voor uitvoeren van de opgelegde taak, verlies of wijziging van persoonsgegevens, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De gemeenschappelijke regeling Holland Rijnland registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure meldplicht datalekken.

Samenwerking

Soms worden derden ingeschakeld om persoonsgegevens in opdracht van de gemeenschappelijke regeling Holland Rijnland te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan dit privacy beleid. De gemeenschappelijke regeling Holland Rijnland maakt hiervoor contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

Samenwerkingsverbanden

Het kan voorkomen dat de gemeenschappelijke regeling Holland Rijnland samenwerkt met andere (overheids-)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). Dan worden met deze organisaties afspraken gemaakt over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat minimaal gelijk is aan dat van de gemeenschappelijke regeling Holland Rijnland.

Doorgifte buiten de EER

Bij de werkzaamheden van de gemeenschappelijke regeling Holland Rijnland is er géén sprake van

doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie. Verzoeken hiertoe worden behandeld in overeenstemming met de toepasselijke wet- en regelgeving en dit privacybeleid.

Transparantie

De gemeenschappelijke regeling Holland Rijnland informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt Holland Rijnland van deze informatieplicht af.

Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeenschappelijke regeling Holland Rijnland over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid.

Geschillen

Indien de betrokkene van mening is dat de gemeenschappelijke regeling Holland Rijnland niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen bij het Dagelijks Bestuur van Holland Rijnland. Wij doen er alles aan om uw recht op privacy te beschermen. Heeft u een vraag of klacht over de wijze waarop Holland Rijnland omgaat met uw persoonsgegevens? Neem dan contact op met fg@hollandrijnland.nl
De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens. Zie: https:// www.autoriteitpersoonsgegevens.nl

Verantwoording

Onder de verantwoordelijkheid van het Algemeen Bestuur vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeenschappelijke regeling Holland Rijnland over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De organisatie stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

Verwerkingsregister

De gemeenschappelijke regeling Holland Rijnland beschikt over een actueel verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

Gegevenseffectbeoordeling

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de organisatie een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. In dat geval wordt een gegevenseffectbeoordeling (ook wel Data Processing Impact Assessment of DPIA genoemd) uitgevoerd. Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking,

moet de organisatie voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeenschappelijke regeling Holland Rijnland met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd.

Plannen en uitvoering

De organisatie verwerkt structureel en op grote schaal persoonsgegevens, waaronder bijzondere persoonsgegevens. De manager Bedrijfsvoering geeft ieder kwartaal sturing aan de verbetering van de privacy aspecten. Holland Rijnland heeft hierbij een functionaris gegevensbescherming (FG) aangesteld. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan het Dagelijks Bestuur en aan het Algemeen Bestuur van zijn werkzaamheden, bevindingen en aanbevelingen.

Privacy rollen en Verantwoordelijken

Met de onderstaande rollen en verantwoordelijkheden biedt de gemeenschappelijke regeling Holland Rijnland een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Om in de kleine organisatie serieus werk te maken van de het privacy onderwerp en de onafhankelijkheid, continuïteit te bewaken wordt externe deskundigheid aangetrokken voor de FG en PO taken. Deze worden niet als nevenfunctie bij een medewerker belegd.

R	Responsible / Feitelijk verantwoordelijk	- Secretaris – Directeur - Dagelijks Bestuur samenwerkingsorgaan Holland Rijnland - Manager Bedrijfsvoering, Manager Regionale Uitvoering, Manager Strategische Eenheid - Medewerkers (inclusief inhuur / externen) die persoonsgegevens verwerken
A	Accountable / Eindverantwoordelijk	- Algemeen Bestuur Samenwerkingsorgaan Holland Rijnland
C	Consulterend / Adviserend	- Privacy Officer (PO) - Functionaris Gegevensbescherming (FG) - CISO
I	Informerend / Geïnformeerd	- Algemeen Bestuur - Dagelijks bestuur Samenwerkingsorgaan Holland Rijnland - Functionaris Gegevensbescherming - Belanghebbende(n) - Betrokkene(n)

Het Algemeen Bestuur samenwerkingsorgaan Holland Rijnland is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeenschappelijke regeling Holland Rijnland. Het heeft de volgende rollen en verantwoordelijkheden:
- Eindverantwoordelijk voor de naleving van de privacywetgeving en vaststellen privacy beleid.

Het Dagelijks Bestuur samenwerkingsorgaan Holland Rijnland:
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de

FG;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacy-cultuur.
- Stelt de niet-wettelijke voorgeschreven bewaartermijnen vast.

De Secretaris-Directeur en de manager Bedrijfsvoering, manager Regionale Uitvoering en manager Strategische Eenheid zijn verantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid.

De manager Bedrijfsvoering, manager Regionale Uitvoering en manager Strategische Eenheid zijn:
- Verantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;
- Informeert de FG op welke manier de eigen afdeling compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen de eigen afdeling;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op de eigen afdeling;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Aansturen van de Privacy Officer, (door manager Bedrijfsvoering);
- Bevordert duurzame privacy-cultuur;
- Betrekt PO en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris Gegevensbescherming (FG)
De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie.
De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:
- Interne toezichthouder op de naleving van de AVG namens de Autoriteit Persoonsgegevens;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
- Draagt privacybeleid actief uit binnen Holland Rijnland en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacyklachten en verzoeken van betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beheert het centrale verwerkingenregister;
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert aan de directeur en het Dagelijks Bestuur en Algemeen Bestuur.

Privacy Officer
De Privacy Officer is het eerste aanspreekpunt rondom privacy gerelateerde vraagstukken, en heeft

een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid.
De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:
- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van gegevenseffectbeoordeling (GEB DPIA) en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
- Adviseert over de verwerkingsgrondslag (en adviseert over de informed consent);
- Ontwikkelt de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
- Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken.

CISO
De chief information security officer is verantwoordelijk voor:
- het implementeren van en toezicht houden op het informatiebeveiligingsbeleid;
- adviseert over technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens binnen de organisatie en voor aanvallen van buitenaf;
- beoordeelt de kwaliteit van de ICT dienstverlening;
- identificeert verbeteringsplannen aan de stand van de techniek en interne doelstellingen.