Veiligheidsregio Rotterdam-Rijnmond

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 884

14 april

2026

Officiële uitgave van de gemeenschappelijke regeling Veiligheidsregio Rotterdam-Rijnmond

Privacybeleid Veiligheidsregio Rotterdam-Rijnmond

Hoofdstuk 1 Inleiding

1.1 Introductie privacybeleid

De VRR verwerkt dagelijks en op grote schaal persoonsgegevens van medewerkers, zakelijke relaties en burgers. Alle informatie die direct of indirect te herleiden zijn naar personen zijn persoonsgegevens. De betrokken personen en instanties moeten erop kunnen vertrouwen dat de VRR zorgvuldig en veilig met deze gegevens omgaat: de VRR respecteert hierbij de privacy van alle betrokken personen. De VRR is van mening dat een goed privacybeleid belangrijk is, waarin wordt uitgelegd hoe de VRR met deze gegevens omgaat. De VRR zorgt ervoor dat dit volgens de Algemene Verordening Gegevensbescherming (AVG) verloopt. De wet AVG legt een verantwoordingsplicht op aan de VRR. Dit beleid past daarin.

1.2 Visie op persoonsgegevensverwerking en -bescherming

De verwerking van persoonsgegevens is een onderdeel van de taakuitvoering van de VRR. Verwerken van persoonsgegevens betekent elke bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens. Voorbeelden hiervan zijn: verzamelen, opslaan, bewaren maar ook delen en verwijderen van persoonsgegevens.

De VRR vindt dat de verwerking van persoonsgegevens hand in hand gaat met de verantwoordelijkheid om effectieve bescherming te bieden. De VRR draagt zorg voor de beveiliging van de persoonsgegevens in technische en organisatorische zin. Daarbij houdt de VRR zich aan de wettelijke regels op het gebied van de verwerking van persoonsgegevens. Er moet voorkomen worden dat er onnodig inbreuk wordt gemaakt op de rechten en vrijheden van personen met als gevolg dat deze personen schade of nadeel daardoor ondervinden. Dit houdt in dat persoonsgegevens rechtmatig, op behoorlijke wijze en transparant zijn verkregen en alleen voor een specifiek beschreven doel worden verwerkt.

De VRR verwerkt niet meer persoonsgegevens dan nodig en bewaakt de beschikbaarheid, de integriteit en de vertrouwelijkheid van de gegevens. Daarbij geldt dat deze gegevens niet langer mogen worden bewaard dan noodzakelijk is. De betrokkene, de persoon van wie de persoonsgegevens wordt verwerkt, kan altijd gebruik maken van zijn rechten op informatie, om in te zien, te wijzigen, vergeten te worden of gegevens over te dragen.

1.3 Reikwijdte

Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de VRR. De richtlijnen die in dit beleid staan beschreven gelden voor iedereen die namens de VRR gegevens verwerkt. Wanneer in dit document gesproken wordt over de VRR wordt bedoeld de gehele organisatie van de VRR.

Dit beleid vervangt het voorgaande privacybeleid en dient als paraplu beleidsstuk voor alle beleidsafspraken waar persoonsgegevens in voorkomen en geldt ten aanzien van alle natuurlijke personen waarvan de VRR gegevens over beschikt. Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens binnen de VRR. Daarnaast is het van toepassing op geheel of gedeeltelijk geautomatiseerde en niet geautomatiseerde verwerking van persoonsgegevens die in een (papieren of digitaal) bestand zijn opgenomen.

Het privacybeleid is onlosmakelijk verbonden met het Strategisch informatiebeveiligingsbeleid VRR.

1.4 Leeswijzer

De VRR geeft door middel van dit privacybeleid een duidelijke richting aan de zorgvuldige verwerking en bescherming van persoonsgegevens. Het beleid is opgedeeld in de volgende hoofdstukken:

- Hoofdstuk 2 beschrijft de verantwoordelijkheden en de borging van het privacybeleid.
- Hoofdstuk 3 beschrijft de richtlijnen voor een zorgvuldige omgang met deze persoonsgegevens.
- Hoofdstuk 4 beschrijft de richtlijnen voor de bescherming van persoonsgegevens.
- Hoofdstuk 5 beschrijft op hoofdlijnen de rechten van alle betrokkenen (medewerkers, zakelijke relaties en burgers).

In de bijlagen komen de volgende onderwerpen aan bod: het juridische kader, de categorieën persoonsgegevens die de VRR verwerkt en een uitgebreide beschrijving van de functies en verantwoordelijkheden.

Hoofdstuk 2 Organisatie

2.1 De organisatorische verantwoordelijkheden

De vaststelling van dit privacybeleid binnen de VRR vormt de basis van de privacyborging. De directie en de leidinggevenden zijn primair verantwoordelijk voor de algehele naleving van de AVG. Maar deze verantwoordelijkheid beperkt zich niet enkel tot de directie en de leidinggevenden. Zorgvuldige gegevensverwerking en -bescherming geldt voor iedereen die binnen de VRR werkzaam is.

De VRR streeft naar een cultuur waarbij iedereen elkaar in alle openheid aanspreekt op het gedrag rondom privacy en daarmee van elkaar leert. Communicatie, openheid en toezicht zijn belangrijke randvoorwaarden om een optimaal privacybeleid te realiseren.

Alle binnen de VRR werkzame personen behandelen alle informatie over individuele personen vertrouwelijk en dragen er zorg voor dat deze informatie niet aan onbevoegde derden bekend wordt.

Om bewustwording te realiseren is kennisdeling over het onderwerp noodzakelijk. De VRR zorgt ervoor dat de informatie over privacy herhaaldelijk onder de aandacht wordt gebracht bij medewerkers van de VRR.

De VRR verwacht van al haar medewerkers dat zij deze richtlijnen naleven en bijdragen aan een zorgvuldige omgang met persoonsgegevens. Het niet in acht nemen van de richtlijnen die in dit privacybeleid zijn opgenomen of een ernstige schending daarvan kan leiden tot sancties.

2.2 Organisatorische borging

De leidinggevenden zijn binnen hun werkprocessen verantwoordelijk voor de uitvoering van de richtlijnen van dit beleid.

De VRR beschikt over een Functionaris Gegevensbescherming en over een Privacy Officer. De Functionaris Gegevensbescherming heeft de verantwoordelijkheid om structureel te toetsen of de wettelijke eisen en richtlijnen op het gebied van gegevensbescherming zijn geïmplementeerd en worden uitgevoerd. De Privacy Officer adviseert en ondersteunt de organisatie bij de uitvoering van de wettelijke eisen en de richtlijnen die in dit beleid staan beschreven. Zie bijlage 3 voor meer informatie over functies en verantwoordelijkheden.

2.3 Verantwoording

Door middel van periodieke rapportages legt de VRR aantoonbaar verantwoording af over de naleving van de AVG binnen de VRR. Naast de periodieke rapportages hebben zowel de directie als de Functionaris Gegevensbescherming de plicht om het dagelijks bestuur te informeren over bijzonderheden en ernstige incidenten met betrekking tot persoonsgegevens.

2.4 Sturing en monitoring

Iedere leidinggevende is zelfstandig verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar werkprocessen plaatsvindt. Het is daarom ook haar verantwoordelijkheid om te monitoren of persoonsgegevens zorgvuldig verwerkt worden en dit zo nodig bij te sturen. Ook draagt zij zorg voor het continu optimaliseren en borgen van de kwaliteit van de werkprocessen waarbij privacy een rol speelt. Daarnaast is zij verplicht om incidenten te melden bij het Servicedesk.

Juist omdat zorgvuldig omgaan met persoonsgegevens voor een belangrijk deel mensenwerk is en dit op elke afdeling anders ingericht kan zijn, moet op alle niveaus binnen de VRR over privacy worden nagedacht. De belangrijkste elementen van deze borging zijn:

- Uitvoering van de richtlijnen van dit beleid. Zie hoofdstuk 3 en 4.
- Privacy als onderwerp in werkoverleggen
- Toezicht op gegevensbescherming
- Privacy opnemen in het planning- en control proces (PDCA)
- Interne en externe audit.

Hoofdstuk 3 Richtlijnen voor een zorgvuldige omgang met persoonsgegevens

3.1 Transparantie

Transparantie is een basisprincipe van de AVG. Het houdt in dat de VRR duidelijk, toegankelijk en open is over de omgang van persoonsgegevens binnen de VRR. Ook is de VRR transparant over wat, waarom en welke persoonsgegevens er verwerkt worden. De VRR informeert de medewerkers, relaties en burgers

tijdig over de verwerking. Voor alle betrokkenen is het duidelijk hoe en waarom de VRR hun persoonsgegevens verwerkt.

De VRR heeft een privacyverklaring die goed vindbaar is voor alle betrokkenen.

3.2 Rechtmatige grondslag van de verwerking

De verwerking van persoonsgegevens mag alleen gebeuren wanneer er sprake is van een of meerdere rechtmatige grondslagen voor de verwerkingen zoals vastgelegd in artikel 6 van de AVG:

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

Vanuit de VRR zijn er verschillende grondslagen aan te reiken om gegevens te verwerken. Bij de VRR gaat het in veel gevallen om het voldoen aan een wettelijke verplichting en voor het uitvoeren van een publieke taak. Denk hierbij aan het leveren van ambulancezorg of brandweerzorg.

Maar ook de overige grondslagen zijn op specifieke verwerkingen van toepassing. Bijvoorbeeld voor het gebruik van camerabewaking geldt -in sommige specifieke gevallen- de grondslag gerechtvaardigd belang en voor het verwerken van foto's in een smoelenboek is toestemming vereist.

De grondslag voor de verwerking wordt in een zogenaamd verwerkingsregister vastgelegd.

3.3 Verwerkingsregister

De VRR is verplicht om een verwerkingsregister bij te houden. Dit is een overzicht van alle verwerkingen van persoonsgegevens die plaatsvinden binnen de VRR. In dit register houdt de VRR bij welke verwerkingen de VRR uitvoert, waarom dit gebeurt en op basis van welke grondslag. Het register dient actueel te zijn en wordt dus aangepast, zodra verwerkingen worden gewijzigd of wanneer er sprake is van een nieuwe verwerking.

Ten minste jaarlijks vindt een review plaats. De leidinggevende van elk organisatieonderdeel heeft de verantwoordelijkheid om het verwerkingsregister actueel te houden. De Privacy officer of de Security & Privacy Supporter (SPS'er) van de desbetreffende afdeling biedt de leidinggevende ondersteuning.

3.4 Verkrijging van gegevens

Persoonsgegevens worden door de betrokkene zelf verstrekt of door derden (burgers of organisaties) verstrekt. Wat er precies met de verzamelde gegevens gebeurt, is afhankelijk van het doel waarvoor ze verzameld worden. Meestal worden ze in een informatiesysteem opgenomen waar ze alleen toegankelijk zijn voor de medewerkers (en/of eventuele ketenpartners) die belast zijn met het uitvoeren van een specifieke taak. In bijlage 2 is beschreven welke persoonsgegevens de VRR verwerkt.

3.5 Toegang tot en verstrekking van persoonsgegevens

Alle medewerkers zijn verplicht tot geheimhouding van de persoonsgegevens, waarvan zij kennisnemen. Dit houdt in dat deze medewerkers de gegevens niet openbaar maken. Uitsluitend de proces- of taakverantwoordelijke heeft ten behoeve van een verwerking rechtstreekse toegang tot de daarvoor benodigde persoonsgegevens. De VRR hanteert hiertoe het "Least Privilege principe":

- Gegevens kunnen ingezien en verwerkt worden door binnen de VRR werkzame personen, voor zover dit voor hun taakuitoefening noodzakelijk is.
- Indien de werkzame persoon voor het uitvoeren van zijn/haar taak niet direct toegang nodig heeft tot de persoonsgegevens, wordt ook geen toegang verleend.

De Functionaris Gegevensbescherming en Privacy officer hebben voor zover dit voor hun taakuitvoering (toezicht, onderzoek, beoordelen, adviseren e.d.) nodig is, toegang tot alle persoonsgegevens binnen de VRR. Dit betekent niet dat zij standaard toegang hebben tot alle gegevens. Ook voor hen geldt het Least Privilege principe. Het verkrijgen van toegang tot de persoonsgegevens verloopt via de voor die gegevens verantwoordelijke leidinggevende.

De plicht tot geheimhouding van persoonsgegevens vervalt voor de medewerker wanneer persoonsgegevens doorgegeven moeten worden aan personen buiten de VRR of aan andere organisaties omdat het verenigbaar is met het doel waarvoor de gegevens zijn verzameld. Of dit het geval is, hangt af van de concrete omstandigheden. Dat kan dus per situatie verschillen.

Aan personen buiten de VRR of aan andere organisaties worden de gegevens enkel verstrekt indien:
- Een wet die voorschrijft om de gegevens te verstrekken of voor het vervullen van een publieke taak;
- De betrokkene toestemming heeft verleend tot gegevensverstrekking voor een kenbaar specifiek doel;
- Daarnaast worden de gegevens verstrekt aan verwerkers, voor zover dit voor de uitoefening voor hun taken voor de VRR als verwerkingsverantwoordelijke noodzakelijk is.

3.6 Verwerkersovereenkomst
In specifieke situaties schakelt de VRR derden in om gegevens namens en voor de VRR te verwerken. Het uitbesteden van werkzaamheden aan derden brengt risico's met zich mee op het gebied van gegevensverwerking en - bescherming. Met het oog op de omgang met persoonsgegevens, door alle partijen waar de VRR mee samenwerkt en waarbij persoonsgegevens worden verwerkt, worden verwerkersovereenkomsten afgesloten.

3.7 Gezondheidsgegevens
Gegevens die door de Meldkamer Ambulancezorg en door Ambulancezorg Rotterdam Rijnmond worden verwerkt over burgers kunnen onder het medische beroepsgeheim vallen. Gegevens die onder het medische beroepsgeheim vallen, dienen met uiterste zorg behandeld te worden. Dit betekent dat gezondheidsgegevens niet zomaar gebruikt mogen worden voor andere doeleinden. Het verwerken van deze gegevens is voorbehouden aan daartoe bevoegde personen. Inzage voor anderen dient afgeschermd te worden en daar waar dit (technisch of organisatorisch) niet mogelijk is, maakt het management afspraken om deze gegevens voldoende te beschermen. In alle gevallen is inzage in het dossier pas mogelijk na toestemming van de behandelaar of betrokkene zelf.

3.8 Gebruik van gegevens voor (wetenschappelijk) onderzoek en statistische doelen
De VRR mag persoonsgegevens gebruiken voor (wetenschappelijk) onderzoek en statistische doelen mits betrokkene(n) van wie de data voor het onderzoek wordt gebruikt hierover is/zijn geïnformeerd en passende waarborgen zijn genomen. Wanneer persoonsgegevens worden gedeeld met derde partijen voor (wetenschappelijk) onderzoek of statische doeleinden moet de VRR toestemming vragen aan betrokkenen.

Het kan ook zijn dat het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd. In dit geval kan de VRR de gegevens verstrekken wanneer de herleiding tot individuele natuurlijke personen wordt voorkomen. In dat geval kunnen gegevens zonder toestemming worden gedeeld.

3.9 Doorgifte buiten de EU/EER
Soms geeft een organisatie persoonsgegevens door naar een ander land. Bijvoorbeeld bij gebruik van een clouddienst met de servers in een ander land. Doorgeven van persoonsgegevens is volgens de AVG alleen toegestaan binnen de Europese Economische Ruimte (EER) of naar landen die een passend beschermingsniveau bieden.

De AVG (EU: GDPR) geldt voor alle lidstaten van de Europese Unie en daarom is het voor de VRR mogelijk om persoonsgegevens door te sturen naar een andere EU-lidstaat zonder daarvoor extra maatregelen te nemen, omdat deze landen hetzelfde beschermingsniveau hebben als Nederland. De Europese Commissie heeft daarnaast ook beoordeeld dat Liechtenstein, Noorwegen en IJsland voldoen aan een adequaat beschermingsniveau. Dit zijn geen EU-lidstaten maar deze drie landen vormen samen met de EER. Binnen deze ruimte mogen persoonsgegevens doorgegeven en verwerkt worden.

VRR geeft in principe geen persoonsgegevens door buiten de EER. Als dit toch onvermijdelijk of noodzakelijk is, dan is een passend beschermingsniveau vereist. Wat een passend beschermingsniveau is, verschilt per verwerking.

Voor de VRR betekent dat doorgifte van persoonsgegevens buiten de EER niet plaatsvindt zonder de uitdrukkelijke toestemming van de VRR. Dit dient standaard opgenomen te worden in het programma van eisen dat vooraf opgesteld wordt bij het aankopen van nieuwe systemen.

Hoofdstuk 4 Richtlijnen voor bescherming van persoonsgegevens

4.1 Bescherming van persoonsgegevens
De VRR treft passende technische en organisatorische maatregelen ter bescherming, bevordering van de juistheid en volledigheid van de persoonsgegevens en ter voorkoming van inbreuk, verlies en on-

rechtmatige verwerking van de persoonsgegevens. De bescherming van persoonsgegevens heeft raakvlakken met informatiebeveiliging. Zie hiervoor ook het Strategisch Informatiebeveiligingsbeleid VRR. Dit hoofdstuk beschrijft richtlijnen die persoonsgegevens extra beschermen.

4.2 Data Protection Impact Assessment

Een data protection impact assessment (DPIA), ook wel bekend als een gegevensbeschermingseffect-beoordeling, is een instrument om vooraf de privacyrisico's van een verwerking in kaart te brengen. De VRR neemt vervolgens maatregelen om deze risico's te verkleinen. Volgens de AVG is de VRR niet verplicht om voor elke verwerking een DPIA uit te voeren, maar alleen voor verwerkingen die naar verwachting een hoog privacyrisico opleveren voor de betrokkenen. Bijvoorbeeld bij heimelijk onderzoek, cameratoezicht, grootschalige verwerkingen van gezondheidsgegevens, communicatiegegevens, controle werknemers, locatiegegevens en biometrische gegevens.

Bij het aanpassen van een bestaande verwerking of bij het starten van een nieuwe verwerking moet een DPIA worden uitgevoerd indien de verwerking een hoog privacyrisico bevat.

Een DPIA dient door de proces- of taakverantwoordelijke uitgevoerd te worden. De Privacy officer of SPS'er biedt de proces- of taakverantwoordelijke ondersteuning. De risico's die door middel van een DPIA worden vastgesteld, worden meegenomen in een planning- en controlproces (PDCA).

4.3 Dataminimalisatie

Eerder is al genoemd dat de VRR niet meer persoonsgegevens mag gebruiken dan nodig is om het doel te bereiken. Dit wordt dataminimalisatie genoemd. Om dataminimalisatie toe te kunnen passen is het belangrijk dat de VRR goed in het verwerkingsregister vastlegt op welke manier de gegevens zijn verkregen en voor welk doel de gegevens worden gebruikt, waarbij de duur van het gebruik van de gegevens een bepalende factor is.

4.4 Bewaren en vernietigen van gegevens

Iedere leidinggevende is voor de eigen afdeling verantwoordelijk voor het zorgdragen van een goed informatiebeheer en archief. Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, dient de VRR termijnen vast te stellen voor het wissen van gegevens. De toegestane bewaartermijnen van persoonsgegevens lopen uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Zo zijn er papieren en elektronische documenten welke onder de Archiefwet vallen.

Persoonsgegevens moeten aan het einde van hun bewaartermijn verwijderd worden. Indien gegevens daarna nog gebruikt worden voor statistische- of onderzoeksdoeleinden, dan dienen de gegevens geanonimiseerd te worden. Het tijdig en gecontroleerd vernietigen van persoonsgegevens wordt meegenomen in het ontwerp van de verwerking. (Zie 4.5)

4.5 Privacy by design en Privacy by default

Met de invoering van de AVG is het verplicht om privacy te waarborgen door middel van Privacy by Design en Privacy by Default.

Privacy by Design houdt in dat privacy zorgvuldig vanaf het begin van het ontwerpproces van producten en diensten moet worden geïntegreerd. Dit omvat zowel technische als organisatorische maatregelen.

Privacy by Default vereist dat standaardinstellingen ontworpen zijn om de privacy van gebruikers te maximaliseren. Dit betekent dat de automatische instellingen privacyvriendelijk moeten zijn. Bijvoorbeeld een invulformulier op een website is op een manier ontworpen waardoor de bezoeker geen persoonsgegevens kan invullen die niet noodzakelijk zijn.

De principes Privacy by design en Privacy by default zijn standaard opgenomen in het programma van eisen dat bij het aankopen van nieuwe systemen wordt gebruikt.

4.6 Dataclassificatie

De maatregelen die getroffen moeten worden om de gegevensbescherming te kunnen borgen zijn niet voor elk proces en informatiesysteem hetzelfde. Daarom is het nodig dat alle processen en informatiesystemen die gegevens verwerken een dataclassificatie krijgen. Het heeft als doel om de beschikbaarheid, integriteit en vertrouwelijkheid van het proces en het informatiesysteem te benoemen. Dataclassificatie is het labelen van informatie om te kunnen bepalen welk niveau van bescherming er nodig is. Hoe gevoeliger deze gegevens zijn hoe hoger de bescherming hoort te zijn. De VRR hanteert hier voor de Classificatierichtlijn VRR.

4.7 Registratielogboek gegevensgebruik

Elk geautomatiseerd systeem dat hoofdzakelijk het doel heeft om persoonsgegevens te verwerken, moet een registratielogboek bijhouden van de verwerkingen. In dit logboek staat minimaal vermeld welke gebruiker, op welk moment, welke gegevens heeft verwerkt. Het registreren van gegevensgebruik is standaard opgenomen in het programma van eisen voor de verwerving van nieuwe systemen.

De VRR houdt rekening met het volgende:
- Bij een registratielogboek wordt een chronologische registratie van gegevens over feitelijk uitgevoerde verwerkingen en/of pogingen daartoe, die zich gedurende een periode in een verwerking voordoen, bijgehouden;
- Dit wordt vastgelegd in een logbestand, bijvoorbeeld een systeemlog of een securitylog.

4.8 Meldplicht voor inbreuken in verband met persoonsgegevens (datalekken)

Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is, waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek. Indien zich een datalek voordoet, handelt de VRR in overeenstemming met het vastgestelde werkproces ten aanzien van incidentmanagement. In dit proces worden stappen ondernomen om de eventuele schade of de kans hierop bij een 'datalek' te beperken en de getroffen perso(o)n(en) te beschermen.

De VRR heeft de verplichting om een datalek te melden aan de Autoriteit Persoonsgegevens (AP) wanneer er sprake is van een hoog risico op nadelige gevolgen voor betrokkene, dan wel nadelige gevolgen voor de bescherming van persoonsgegevens. Het gaat dan om omstandigheden waarbij de VRR de verantwoordelijkheid draagt voor de betreffende gegevensverwerking.

Medewerkers melden een inbreuk in verband met persoonsgegevens bij het Servicedesk. Meldingen aan de Autoriteit Persoonsgegevens worden in beginsel gedaan door de Functionaris Gegevensbescherming of bij diens afwezigheid door de Privacy officer of Jurist. De Privacy officer houdt namens de VRR een datalekregister bij waarin alle datalekken zijn opgenomen. De VRR maakt haar register van datalekken niet openbaar.

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

Hoofdstuk 5 Rechten van betrokkenen

5.1 Rechten van betrokkenen

De AVG brengt betrokkenen (medewerkers, zakelijke relaties en burgers) sterkere privacyrechten dan in voorgaande privacywetgeving. Om gebruik te maken van hun rechten kunnen betrokkenen een verzoek indienen. Een verzoek kan worden gedaan door een betrokkene die 16 jaar of ouder is. Voor iemand tussen de 12 en 16 jaar kan een verzoek worden gedaan door de jeugdige zelf of door een ouder met gezag of een wettelijke vertegenwoordiger. Als iemand jonger is dan 12 jaar of onder curatele staat, kan hij of zij niet zelf een verzoek doen. De ouder met gezag of een wettelijke vertegenwoordiger moet het verzoek indienen op zijn of haar naam.

De rechten van de betrokkene zijn binnen de VRR op transparante wijze ingericht. De VRR heeft een duidelijke privacyverklaring waar de wijze waarop betrokkenen hun rechten kunnen uitoefenen in zijn opgenomen.

Alvorens het verzoek te kunnen behandelen moet de identiteit van de verzoeker op deugdelijke wijze worden vastgesteld. De VRR heeft per organisatieonderdeel een proces ingericht voor het afhandelen van de volgende verzoeken:
- Recht op inzage en afschrift van gegevens. Betrokkenen kunnen altijd hun persoonsgegevens inzien wanneer zij hierom vragen. Betrokkene heeft de mogelijkheid om te controleren of en op welke manier zijn/haar gegevens worden verzameld en verwerkt.
- Recht op rectificatie (correctie, aanvulling) van gegevens. Als de VRR persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij de VRR om feitelijke onjuistheden te corrigeren.

- Recht op wissing. Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien de VRR niet langer een goede grond heeft voor het gebruik hiervan. De VRR voert een beleid ten aanzien van bewaartermijnen en vernietiging dat bij de beoordeling van het verzoek gebruikt kan worden. Het geldt niet voor (persoons)gegevens, zoals financiële gegevens die de VRR op andere gronden moet bewaren.
- Recht op beperking van de verwerking. Het recht op beperking van de verwerking van persoonsgegevens houdt in dat de gegevens wel beschikbaar blijven, maar dat ze tijdelijk niet gebruikt mogen worden. De persoonsgegevens mogen dan alleen nog worden gebruikt met toestemming van de betrokkene, of als dat nodig is voor het instellen, uitoefenen of onderbouwen van een rechtsvordering of ter bescherming van de rechten van andere natuurlijke personen of rechtspersonen.
- Recht op overdraagbaarheid van gegevens (dataportabiliteit). De VRR is vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens voor zover het werkzaamheden betreft in het kader van algemeen belang of op basis van een wettelijke verplichting. Het recht om gegevens te mogen meenemen geldt voor persoonsgegevens die de betrokkene zelf actief en bewust heeft verstrekt (eigen data).
- Recht van bezwaar tegen verwerking. De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem of haar betreffende persoonsgegevens.
- Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming waaronder profilering. Bij geautomatiseerde individuele besluitvorming is geen sprake van (noemenswaardige) menselijke tussenkomst zodat eventuele uitkomsten kunnen worden gecorrigeerd.

Iedere betrokkene kan schriftelijk een verzoek conform AVG indienen bij de VRR. Binnen een maand beoordeelt de VRR of het verzoek ontvankelijk is en handelt dit verzoek binnen die termijn ook af.

Als het verzoek niet (tijdig) kan worden opgevolgd, deelt de VRR uiterlijk binnen een maand waarom het verzoek zonder gevolg is gebleven en dat de VRR de termijn verlengt met twee maanden.

5.2 Recht op informatie

Tijdens het eerste contact informeert de VRR betrokkene(n) over de verwerking van hun persoonsgegevens. Als het niet mogelijk is om de betrokkene tijdens het eerste contact te informeren, dan zorgt de VRR dat de betrokkene zo spoedig als de situatie toe laat, alsnog over de gegevensverwerking wordt geïnformeerd. Van het uitstellen of niet informeren van de betrokkene kan een aantekening worden gemaakt in het verwerkingsregister. Hierbij dient in ieder geval gecommuniceerd te worden wat het doel is, welke persoonsgegevens worden verwerkt, wie daarvoor verantwoordelijk is en of de gegevens aan derden worden verstrekt.

5.3 Klachten en verzoeken

De betrokkene heeft de mogelijkheid om bezwaar te maken over de afhandeling van het verzoek en de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of het bezwaar aan een bevoegd rechter voor te leggen.

Daarnaast kan elke betrokkene een klacht indienen. De VRR behandelt klachten volgens de vastgestelde en bekendgemaakte klachtenregeling.

De VRR informeert relevante (keten)partners indien een klacht of verzoek wordt ingewilligd wanneer het verzoek ook betrekking heeft op dezelfde gegevensverwerking die zij van de VRR ontvangen heeft. Dit betreft onder andere organisaties met wie een verwerkersovereenkomst, een overeenkomst gezamenlijk verwerkersverantwoordelijken dan wel een gezamenlijke uitwisselingsovereenkomst is afgesloten. Indien relevant vraagt de VRR actief om bevestiging van de betreffende (keten)partners dat aan het verzoek is voldaan.

Hoofdstuk 6 Vaststelling Privacybeleid

Dit privacybeleid treedt in werking na vaststelling door het dagelijks bestuur van de Veiligheidsregio Rotterdam-Rijnmond. Het beleid wordt iedere 4 jaar geëvalueerd en indien nodig herzien, tenzij er wijzigingen voordoen in de AVG. In dit geval zal het beleid eerder herzien moeten worden. Aanpassingen van dit beleid worden aangekondigd via het publicatieblad gemeenschappelijke regeling. De meest actuele versie van het beleid is te vinden op http://vr-rr.nl.

Aldus vastgesteld door het dagelijks bestuur van de Veiligheidsregio Rotterdam-Rijnmond op 8 april 2026,

De Voorzitter,
C. Schouten

De Secretaris,
A. Littooij

Bijlage 1 Juridisch kader

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

Europees Verdrag voor de Rechten van de Mens, artikel 8
1. Eenieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Grondwet, artikel 10
1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Hieruit volgend hecht de VRR dan ook grote waarde aan de gegevensbescherming, zoals opgenomen in de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). De AVG welke sinds 25 mei 2018 van kracht is, heeft als doel om de privacy van burgers in Europa beter te beschermen. In de UAVG is een nadere uitwerking vastgelegd. Daarnaast is er specifieke wetgeving van kracht waarin ook een kader voor privacy is weggelegd, zoals in de zorg.

Bij dit beleid wordt onder meer in aanmerking genomen:
- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG);
- Burgerlijk Wetboek (BW);
- Wet op de Veiligheidsregio's (WVr)
- Wet houdende regels inzake de telecommunicatie (Telecommunicatiewet)
- Wet geneeskundige behandelingsovereenkomst (WGBO)
- Wet ambulancezorgvoorzieningen
- Aanbestedingswet
- Wet open overheid (Woo)
- Archiefwet

Bijlage 2 Categorieën persoonsgegevens

De VRR verwerkt persoonsgegevens van diverse categorieën betrokkenen. In hoofdzaak zijn er drie categorieën betrokkenen te onderscheiden:
- Medewerkers van de VRR, waaronder ook inhuur, stagiaires en gedetacheerd personeel
- Zakelijke relaties (in dienst van overheden/bedrijven/instellingen waar wij mee samenwerken).
- Burgers

De VRR verwerkt gewone persoonsgegevens, maar in specifieke gevallen ook bijzondere persoonsgegevens zoals gezondheidsgegevens en biometrische gegevens.

Medewerkers
Met betrekking tot medewerkers worden zowel gewone persoonsgegevens verwerkt als ook bijzondere persoonsgegevens. Veelal met als doel verplichtingen die samenhangen met werkgeverschap. Onder de categorie 'medewerkers' vallen in ieder geval gegevens zoals:
- Naam en achternaam
- Geslacht en geboortedatums
- Contactgegevens, adres, telefoon, email
- Nummer van paspoort of de identiteitskaart
- Burgerservicenummer
- Locatiegegevens van mobiele apparatuur
- IP-adres
- Herleidbare gegevens, zoals de locatiegegevens van een dienstvoertuig
- Opleiding en oefen gegevens
- Keuringen, assessments
- Functioneren en beoordelen
- Financiële en fiscale gegevens
- Lidmaatschap van een vakbond of vakvereniging
- Gezondheidsgegevens
- Biometrische gegevens ten behoeve van identificatie d.m.v. gezichtsherkenning en/ of vingerafdruk
- Verklaring omtrent gedrag
- Beeld- en geluidmateriaal

Zakelijke relaties
Hieronder vallen medewerkers zoals contactpersonen van bedrijven, maar ook functionarissen van ketenpartners, zoals andere VR's, NIPV, ministeries, politie, defensie, waterschappen etc. Gegevens worden meestal verwerkt met als doel het uitvoeren van wettelijke taken of voor het algemeen belang. In andere gevallen wordt specifiek om toestemming gevraagd. Onder de categorie 'zakelijke relaties' van derden vallen gegevens zoals:
- Naam en achternaam
- Contactgegevens, adres, telefoon, email
- Locatiegegevens van mobiele apparatuur
- IP-adres
- Herleidbare gegevens, zoals de locatie van een dienstvoertuig
- Opleidings- en oefengegevens
- Keuringen, assessments
- Functioneren en beoordelen
- Verklaring omtrent gedrag

Burgers
De VRR heeft taken op het gebied van ambulancezorg, brandweerzorg, rampenbestrijding, crisisbeheersing en risicobeheersing. Onder de categorie 'burgers' vallen in ieder geval gegevens zoals:
- Naam en achternaam
- Geslacht en geboortedatums
- Contactgegevens, adres, telefoon, email
- Burgerservicenummer
- Gezondheidsgegevens
- Incidentgegevens
- Kennis en kunde rond veiligheidsbewustzijn
- Beeld- en geluidmateriaal

Bijlage 3 Functies en verantwoordelijkheden

Medewerkers kennen hun rol en verantwoordelijkheid op het gebied van persoonsgegevensverwerking en -bescherming.

Algemeen directeur/Directieraad
• eindverantwoordelijke in de zin van AVG.
• Aanstellen van een Functionaris Gegevensbescherming om namens het bestuur toezicht te houden en te adviseren.
• Vaststellen van gewenste niveau van privacy, implementatie, en aanwijzing van procesverantwoordelijke per informatiesysteem.
• Bevordert de beschikbaarheid van voldoende middelen om gegevensbescherming passend te waarborgen.

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

Functionaris voor de gegevensbescherming (FG)
De FG heeft een wettelijke positie. De FG is onafhankelijk en is verantwoording verschuldigd aan het bestuur en afgeleid daarvan aan de directie. De FG heeft de volgende taken:
• Toezicht houden op een juiste en zorgvuldige omgang met persoonsgegevens en het naleven van het privacybeleid, de AVG en andere privacywetgeving.
• Gevraagd en ongevraagd adviseren en informeren van bestuur, directie en organisatie ten aanzien van privacy, de omgang met persoonsgegevens, klachten en verzoeken.
• Het geven van aanwijzingen aan de organisatie ten aanzien van privacy en de omgang met persoonsgegevens. (Adviezen en aanwijzingen zijn niet vrijblijvend).
• Formeel aanspreekpunt voor de Autoriteit Persoonsgegevens.
• Rapporteert tenminste jaarlijks aan het bestuur, directie en MT over de manier waarop de VRR de afgelopen periode met persoonsgegevens-verwerking en -bescherming is omgegaan.
• Het afhandelen van klachten ten aanzien van de omgang met persoonsgegevensverwerking en -bescherming.
• Beoordelen van meldingen van datalekken.
De FG is geregistreerd bij de Autoriteit Persoonsgegevens. De FG is bereikbaar via fg@vr-rr.nl.

Privacy Officer (PO)
De Privacy Officer heeft een adviserende taak richting de organisatie. Daarnaast verzorgt en coördineert de PO de uitvoerende taken die uit het privacybeleid volgen:
• Opstellen van procedures en richtlijnen ten uitvoering van het privacybeleid.
• Advisering over en ondersteunen bij privacy- en gegevensbescherming gerichte zaken en de uitvoering en naleving van dit privacybeleid en de privacywetgeving.
• Het creëren van bewustzijn en kennisontwikkeling binnen de organisatie ten aanzien van privacy.
• Beoordelen van- en adviseren over de verwerking van persoonsgegevens.
• Het verzorgen van de formele afhandeling ten aanzien van rechten en plichten van (externe) betrokkenen.
• Verzorgen van overige privacy-werkzaamheden zoals inzage- en correctieverzoeken.
• Het vertegenwoordigen van de organisatie in landelijke overleggen en gremia met betrekking tot privacy.
• Het ondersteunen in het uitvoeren van DPIA's.
• Mede beoordelen van meldingen van datalekken.
• Advisering en ondersteuning bij het afsluiten van verwerkersovereenkomsten.
• Beheren van het register van de verwerkingsactiviteiten (verwerkingsregister).
• Beheren van het overzicht van datalekken (datalekregister).
• De PO vervangt de FG bij verlof en verzuim.

Chief Information Security Officer (CISO)

• Ontwerpen van het Strategisch Informatiebeveiligingsbeleid VRR en de Baseline Informatiebeveiliging VRR.
• Stimuleren, adviseren en ondersteunen van de diverse organisatieonderdelen bij de implementatie van informatiebeveiligingsmaatregelen.
• De CISO houdt algemene toezicht op de status en de voortgang van de implementatie-inspanningen binnen de organisatieonderdelen en rapporteert hierover aan de directie(raad).
• De CISO vormt de vraagbaak binnen de organisatie met betrekking tot organisatie brede security-vraagstukken en adviseert het management gevraagd en ongevraagd.
• Bevorderen van het algehele informatiebeveiligingsbewustzijn.

Security & Privacy Support (SPS'er)
• Ondersteuning van leidinggevende in bovengenoemde verantwoordelijkheid.
• Uitvoeren van specifieke taken en activiteiten op het gebied van informatiebeveiliging en privacy.

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