Veiligheidsregio Amsterdam-Amstelland

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 84
15 januari 2024

Officiële uitgave van de gemeenschappelijke regeling Veiligheidsregio Amsterdam-Amstelland

Privacy-beleid Veiligheidsregio Amsterdam-Amstelland (VrAA)

1. Inleiding
De Veiligheidsregio Amsterdam-Amstelland werkt met (persoons)gegevens van medewerkers, burgers, ondernemers en (keten)partners. De VrAA verzamelt deze gegevens om de wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken zoals incidentbestrijding en risicobeheersing. Om deze taken goed te volbrengen, is het noodzakelijk dat de VrAA persoonsgegevens verwerkt. Iedereen moet erop kunnen vertrouwen dat de VrAA zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De VrAA is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

Geldigheidsduur
Dit beleid is vastgesteld op 18 december 2023 door het dagelijks bestuur als eindverantwoordelijke voor de gegevensverwerking binnen de VrAA. Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Als daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's[1]/GEB's[2] kan het dagelijks bestuur besluiten tot een tussentijdse herziening.

2. Begripsbepalingen
De definities van art. 4 AVG hebben in dit beleidsdocument dezelfde betekenis.

3. Visie
De komende jaren zet de VrAA in op het verhogen van de privacy-bewustwording en verdere professionalisering van de privacy-functie in de organisatie. Een goede privacy-boekhouding is noodzakelijk voor het goed functioneren van de VrAA en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen de VrAA.

4. Doel
Met dit privacy-beleid geeft de VrAA een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de VrAA persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacy-beleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.
De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de VrAA, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken.
Naast dit door het dagelijks bestuur vastgestelde privacy-beleid is een informatiebeveiligings-beleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het privacy-beleid kan daarom niet los worden gezien van het informatiebeveiligingsbeleid.
Verantwoordelijkheid van iedere werknemer
Iedereen werkzaam binnen de VrAA is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. We verlangen van alle medewerkers en alle personen die werkzaam zijn voor de VrAA dat de voorschriften van dit privacy-beleid worden opgevolgd en actief worden uitgedragen.

5. Reikwijdte
De VrAA verzamelt en gebruikt persoonsgegevens van medewerkers, burgers en leveranciers en andere natuurlijke personen (hierna te noemen: betrokkenen).
Dit privacy-beleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de VrAA, waaronder:
1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de VrAA;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de VrAA aan een rechtspersoon die voor de VrAA bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen, zoals bij samenwerkingsverbanden of leveranciers.

6. Principes voor de verwerking van persoonsgegevens
De AVG geeft een aantal uitgangspunten voor het gebruik van persoonsgegevens. De VrAA houdt zich aan deze uitgangspunten.

6.1 Bewustwording
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de VrAA voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

6.2 Doorgifte buiten de EER
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacy-beleid.

6.3 Gegevenseffectbeoordeling (GEB)/Data Protection Impact Assessment (DPIA)
Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de VrAA een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De VrAA voert in dat geval een GEB/DPIA uit. Als uit de GEB blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de VrAA 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 VrAA met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging[3] genoemd.

6.5 Gegevens worden op tijd vernietigd
De VrAA stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. De VrAA heeft op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard. Er wordt aangesloten bij de VNG selectielijst.
Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de VrAA de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De VrAA bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

6.6 Geschillenbeslechting
Als de betrokkene van mening is dat de VrAA niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website. 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.

6.7 Inbreuk in verband met persoonsgegevens
Bij toegang tot, verlies of wijziging van persoonsgegevens bij de VrAA, 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 VrAA 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.

6.8 Integriteit en vertrouwelijkheid
De VrAA neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De VrAA handelt hierbij volgens het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht de VrAA om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige verwerkingen.

6.9 Juiste en actuele gegevens
De VrAA 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 VrAA zorgt ervoor dat persoonsgegevens juist en actueel worden gehouden en actualiseert of wist onjuiste persoonsgegevens.

6.10 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 VrAA 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 kiest de VrAA voor die mogelijkheid.

6.11 PDCA Cyclus
De VrAA streeft ernaar om rondom de verwerking van persoonsgegevens *in control* te zijn en daarover op professionele wijze verantwoording af te leggen. *In control* betekent in dit verband dat de VrAA weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

6.12 Privacy by Default en Privacy by Design
De VrAA houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met privacy en gegevensbescherming, om Persoonsgegevens zo goed mogelijk te beschermen. Dit uitgangspunt wordt *Privacy by Design* (PbD) genoemd. De VrAA draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de VrAA *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

6.13 Rechten van betrokkenen
Iedereen heeft het recht om te vernemen welke persoonsgegevens de VrAA over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten:
1. recht van inzage,
2. recht op rectificatie,
3. recht op verwijdering,
4. recht op bezwaar,
5. recht op beperking en
6. recht op overdraagbaarheid.

Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de procedure rechten van betrokkenen.

6.14 Rechtmatige grondslag
Persoonsgegevens worden door de VrAA alleen gebruikt als hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij de VrAA voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

6.15 Samenwerking
De VrAA schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacy-beleid van de VrAA. De AVG verplicht de VrAA tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten. Het model van de VNG/IBD wordt hierin gevolgd.

6.16 Samenwerkingsverbanden
Verder kan het voorkomen dat de VrAA 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). De VrAA maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de VrAA.

6.17 Toegang tot gegevens
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 binnen de VrAA geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De VrAA 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.

6.18 Transparantie
De VrAA 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 wanneer de wet anders bepaalt, wijkt de VrAA van deze informatieplicht af.

6.19 Verantwoording
Binnen de VrAA 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 VrAA over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De VrAA stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

6.20 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 VrAA 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.
6.21 Verwerkingsregister
De VrAA beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

6.22 Welbepaalde doeleinden
De VrAA verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. De VrAA verwerkt alleen persoonsgegevens die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De VrAA 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.

7. Rollen en Verantwoordelijken
Het governancemodel van de VrAA biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van het algemeen bestuur, dagelijks bestuur, het managementteam en medewerkers, de Functionaris voor de Gegevensbescherming (FG), de privacy-officer (PO) en de Chief information-security-officer (CISO).

Wat?!	**Wie?!**
Responsible - verantwoordelijk	1. MT VrAA (sectormanagers & commandant) 2. Afdelingsmanagers 3. Medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
Accountable - eindverantwoordelijk	1. Dagelijks Bestuur
Consulted - geraadpleegd	1. Privacy Officer (PO) 2. Chief Information Security Officer (CISO)/ISO 3. Functionaris Gegevensbescherming (FG)
Informed - geïnformeerd	1. Algemeen bestuur 2. Functionaris Gegevensbescherming 3. Belanghebbende(n)/Betrokkene(n)

Rollen en verantwoordelijkheden Dagelijks bestuur
Het dagelijks bestuur is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de VrAA. Het dagelijks bestuur heeft de volgende rollen en verantwoordelijkheden:
1. is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de VrAA;
2. stelt het privacy-beleid vast;

MT VrAA
1. geeft sturing aan privacy-beleidsvoering en legt rekenschap af over privacy-beleidsvoering aan het dagelijks bestuur;
2. evalueert de toepassing en werking van het privacy-beleid op basis van de rapportage van de FG;
3. bevordert een duurzame privacy-cultuur.

Sectormanagers en commandant
De sectormanagers, en commandant zijn (eind)verantwoordelijk voor de naleving van de privacywetgeving binnen de organisatie-onderdelen, alsmede voor de uitvoering van het privacy-beleid.
De sectormanagers en commandant hebben de volgende rollen en verantwoordelijkheden:

1. eindverantwoordelijk voor de naleving van de privacywetgeving binnen het eigen organisatieonderdeel;
2. verantwoordelijk voor implementatie en uitvoering van het privacy-beleid binnen de eigen sector;

Afdelingsmanagers
1. verantwoordelijk voor implementatie en uitvoering van het privacy-beleid binnen de eigen afdeling;
2. verantwoordelijk voor het informeren van de FG op welke manier het eigen organisatieonderdeel compliant is aan de privacywetgeving;
3. verantwoordelijk voor het (laten) volgen van trainingen door werknemers binnen het eigen organisatieonderdeel;
4. verantwoordelijk voor het (laten) registreren van de gegevensverwerkingen in het verwerkingenregister, voor zover dit betrekking heeft op het eigen organisatieonderdeel;
5. verantwoordelijk voor autorisaties en intrekken van autorisaties van medewerkers die persoonsgegevens verwerken;
6. verantwoordelijk voor het aansturen van de privacy-contactpersonen, voor zover benoemd binnen het eigen organisatieonderdeel;
7. verantwoordelijk voor het bevorderen van een duurzame privacy-cultuur;
8. verantwoordelijk voor het in een vroeg stadium betrekken van de PO en/of FG bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris Gegevensbescherming (FG)
Op basis van de AVG is het aanstellen van een FG verplicht voor de VrAA. 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 VrAA:
1. is interne toezichthouder op de naleving van de AVG namens de Autoriteit Persoonsgegevens;
2. monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
3. neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
4. draagt privacy-beleid actief uit binnen de gehele VrAA en bevordert een cultuur van duurzame gegevensbescherming;
5. adviseert verwerkingsverantwoordelijken bij privacy-klachten en -verzoeken van betrokkenen (ombudsfunctie);
6. adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy-risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
7. adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
8. beheert het centrale verwerkingenregister;
9. beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
10. rapporteert aan het dagelijks bestuur.

Privacy Officer
De Privacy-officer (PO) is het eerste aanspreekpunt voor de VrAA rondom privacy-gerelateerde vraagstukken en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacy-beleid. De PO heeft de volgende rollen en verantwoordelijkheden:
1. adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacy-beleid;
2. stelt privacy-beleid en modellen, formats en standaard-overeenkomsten op, waaronder de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
3. monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacy-beleid;
4. monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkings-register door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
5. adviseert de verwerkingsverantwoordelijke bij het uitvoeren van gegevenseffect-beoordeling (GEB) en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
6. adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
7. adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;
8. adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;

9. adviseert over de verwerkingsgrondslag
10. ontwikkelt de bewustmakingsprogramma's- en privacy-trainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
11 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;
12 ondersteunt en faciliteert verwerkingsverantwoordelijken bij het afhandelen van datalekken (volgens de meldprocedure).

Andere rollen en verantwoordelijkheden

Organisatieonderdeel	**Betrokkenheid**
Juridische Zaken	Ondersteunen van de Privacy Officer bij privacyvraagstukken. Adviseren over privacy-gerelateerde bepalingen in overeenkomsten.
CISO	Toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens. Adviseren van de organisatie bij datalekken (volgens de meldprocedure). Tijdig melden van informatie-beveiligingsincidenten bij PO/FG als er sprake is van mogelijke betrokkenheid van persoonsgegevens bij het incident.
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt, worden medewerkers van communicatie betrokken. Adviseren van de organisatie over de communicatie bij datalekken (volgens de meldprocedure).
Audit / Concern Control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).
Privacy Contactpersonen	De Privacy Contactpersoon is het eerste aanspreekpunt binnen het organisatieonderdeel waar de Privacy Contactpersoon werkzaam is en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacy-beleid.

[1] DPIA = Data-protection impact-assessment
[2] GEB = Gegevensbeschermings-effectbeoordeling
[3] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging

Aldus vastgesteld in de vergadering van het Bestuur gehouden op 18 december 2023.