BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 501

6 maart

2025

Officiële uitgave van de gemeenschappelijke regeling Veiligheidsregio Noord-Holland Noord

Strategisch privacybeleid Veiligheidsregio Noord-Holland Noord 2024 e.v.

1. Inleiding en overzicht

Inleiding

De missie van VR NHN is leed en schade voorkomen en beperken. Wij zijn hulpvaardig, professioneel en betrouwbaar. Het voorkomen van incidenten heeft ook betrekking op informatieveiligheid en privacy. De ambitie van VR NHN is te voldoen aan de wet- en regelgeving op deze gebieden en voor privacy in ieder geval te acteren op volwassenheidsniveau 3.

Deze beleidsnota beschrijft het strategisch privacybeleid 2024 e.v. Dit beleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor privacy op tactisch niveau en werkinstructies op operationeel niveau. Vele documenten hiervan zijn reeds opgesteld en vastgesteld.

Met dit strategisch privacybeleid 2024 e.v. zet VR NHN een volgende stap om de beveiliging van persoonsgegevens binnen de veiligheidsregio te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is het VNG Borgingsproduct AVG versie 3.0. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens. Dit strategisch beleid heeft een relatie met het strategisch informatiebeveiligingsbeleid 2024.

2. Over dit document

Documentinformatie

Dit document heeft als bron de template van de Informatiebeveiligingsdienst (IBD). Deze template staat bekend onder de naam : "Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten", licentie onder: CC BY-NC-SA 4.0.
In hoofdstuk 3 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het VRNHN privacyplan (vastgesteld door de directie) worden deze tactische en operationele aspecten van privacy verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de teammanagers, de privacy functionarissen (PO, complianceofficers en FG), en de uitkomsten van risicoanalyses en DPIA's. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist.
Hoofdstuk 4 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

Dit document

1. is vastgesteld door het dagelijks bestuur op 6 februari 2025
2. is behandeld in het directieoverleg van 26 november 2024 en het MTVR van 5 november 2024
3. is opgesteld door teammanager stafbureau Bestuur & Directie
4. is beoordeeld door de FG, de Ciso, de PO.
5. Versienummer 1.0.

Definities

Informatieveiligheid

Informatieveiligheid is de overkoepelende term waarin informatiebeveiliging en privacy zijn samengenomen. Als professionele organisatie dient VRNHN de beveiliging van informatie professioneel te organiseren en te borgen. Informatie moet immers beschikbaar en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling van informatie moet VR NHN voldoende rekening houden met beveiligings- en privacyaspecten.

Privacy & Gegevensbescherming (AVG)

VR NHN werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt VR NHN voor het goed kunnen uitvoeren van wettelijke taken. Denk hierbij aan taken zoals vergunningsverlening advies, hulpverlening aan slachtoffers en crisisbeheersing . Om als VR NHN deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

Bij de omgang met persoonsgegevens van inwoners en personeel heeft VR NHN een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele organisatie en verdient, samen met informatiebeveiliging, continu aandacht. Individuen moeten erop kunnen vertrouwen dat VR NHN zorgvuldig en veilig met deze persoonsgegevens omgaat.

Doel

Het doel van dit document is het presenteren van het 'Strategisch privacybeleid voor 2024 e.v. De organisatie maakt in dit beleid duidelijk op welke wijze de bescherming van privacy in de organisatie wordt verankerd. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen privacyplan.
Het beleid op privacy dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van persoonsgegevens.

Voor wie

Dit document is bestemd voor alle medewerkers, management, bestuur, leveranciers en bekend gemaakt/ingevoerd door middel van publicatie op het interne intranet Victor en publicatie op de overheidssite officiëlebekendmakingen.nl.

Actualisatie

De taken, verantwoordelijkheden en bevoegdheden bij actualisatie van dit document zijn:

Wie	TVB
Directie VRNHN	Stelt het document vast
Teammanager stafbureau Bestuur & Directie	Houdt toezicht op actualiteit van het document
Privacy Officer	Houdt het document actueel

Andere documenten

Dit document heeft een sterke relatie met het strategisch informatiebeveiligingsbeleid, waarin met name de technische, organisatorische en menselijke factoren van informatiebeveiliging worden geduid.

Wat	Relatie
Strategisch informatiebeveiligingsbeleid	Beide strategische documenten geven aan hoe het informatieveiligheidsbeleid in de organisatie wordt gerealiseerd.
Regeling privacy	Uitwerking uit strategisch beleid: geeft inzicht hoe om te gaan met privacy in de dagelijkse praktijk.
Regeling gebruik e-mail, internet, social media en ICT middelen met het hierop van toepassing zijnde privacyreglement	Uitwerking uit strategisch beleid: gedragscode gebruik ICT middelen ter voorkoming van privacyschending
Beleid informatieverwerkende apparatuur	Uitwerking van strategisch beleid: hoe om te gaan met ICT apparatuur ter voorkoming van o.a. privacy schending.
Begrippenlijst privacy	Geeft toelichting op begrippen die in het kader van bescherming persoonsgegevens worden gebruikt.
Privacyverklaring vrijwilligers	Uitwerking van strategisch beleid: uitleg hoe VRNHN met persoonsgegevens van vrijwilligers omgaat en welke rechten zij hebben.

3. Ontwikkelingen: Ambitie en visie van VR NHN op het gebied van privacy

Ontwikkelingen
De ontwikkelingen die van belang zijn voor het privacy beleid zijn de volgende:

De AVG
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. VR NHN 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).

De 10 principes voor informatiebeveiliging[1]
De 10 principes voor informatiebeveiliging, vastgesteld door het VNG gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:
1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in VR NHN. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen VR NHN processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van VR NHN. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

Informatie uit incidenten, inbreuken op de beveiliging en datalekken
VR NHN kent een systeem waarin incidenten worden vastgelegd. Dit systeem geeft waardevolle informatie om van te leren en dus zijn incidenten uit het verleden nadrukkelijk input bij het actualiseren van het beleid.

Standaarden informatiebeveiliging
De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2012. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2012 genomen. Voor de ondersteuning van VR NHN bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.

Plaats en scope van het strategisch beleid
Het strategisch privacybeleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van privacy op tactisch en operationeel niveau. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven VR NHN privacyplan'.

Scope privacy
De scope van deze beleidsnota omvat alle VR NHN processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van VR NHN en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit strategisch VR NHN privacybeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG, .

Alle informatie en informatiesystemen waar persoonsgegevens in worden verwerkt, zijn van belang voor VR NHN, bepaalde informatie bevat bijzondere persoonsgegevens. Het dagelijks bestuur is eind-

1) **https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf**
2) De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

verantwoordelijk voor de informatiebeveiliging en privacy. Dit geldt voor alle VR informatiesystemen ongeacht waar deze worden gehost.

Uitgangspunten

Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit strategische privacybeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor VR NHN hebben, de privacyrisico's die VR NHN hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele management geeft een duidelijke richting aan privacy en demonstreert dat zij privacybescherming ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van dit beleid van en voor de hele VR NHN. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en (persoons)gegevens(verzamelingen). Het privacybeleid is in lijn met relevante landelijke en Europese wet- en regelgeving.

Taken, verantwoordelijkheden en bevoegdheden van privacybeleid

Wie	TVB
Directie VRNHN	Integrale verantwoordelijkheid en kaderstelling
Management teams VR NHN	Implementatie van het privacybeleid
Lijnmanagement (direct leidinggevenden)	Sturing op privacy, controle op naleving, uitvoering privacy plannen van aanpak
Medewerkers	Handelen conform afgesproken beleid
Proceseigenaren	Zorgen ervoor dat de processen voldoen aan de uitgangspunten van dit beleid. In processen wordt vastgelegd welke informatie wordt verwerkt, welke maatregelen ter bescherming van privacy getroffen zijn en hoe de rechten vanuit AVG worden gewaarborgd.
Functionaris Gegevensbescherming	Houdt toezicht op de verwerking van persoonsgegevens, rapporteert periodiek aan directie en evt. bestuur.
Privacy Officer	Ondersteunt proceseigenaren bij uitvoering taken op AVG-gebied.

Strategische doelen

De strategische doelen van het privacybeleid zijn:

- Het managen van de privacy.
- Adequate bescherming van persoonsgegevens.
- Het toepassen van dataminimalisatie.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van (kritieke) bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de (U)AVG en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door VR NHN hebben een interne eigenaar die de vertrouwelijkheid, privacy-eisen en/of waarde bepaalt van de informatie die ze bevatten.

De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.

- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het privacybeleid vormt samen met het privacy jaarplan het fundament onder een betrouwbare informatievoorziening en privacy bescherming. In het privacy jaarplan wordt de betrouwbaarheid van de informatievoorziening en privacy organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor en privacy.
- Privacybescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van privacybescherming.
- VR NHN stelt de benodigde mensen en middelen beschikbaar om te voldoen aan de privacy eisen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het privacybeleid worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- Het borgen van privacy in de uitvoering van processen vindt risicogestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.

Privacygovernance

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het dagelijks bestuur stelt als eindverantwoordelijke het strategisch privacybeleid vast.
- De directie stelt jaarlijks het privacyplan vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd en gearchiveerd in het daarvoor bestemde systeem.
- De directie is verantwoordelijk voor het vragen om informatie bij de afdelingsmanagers en ziet erop toe dat de afdelingsmanagers adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens die onder hun verantwoordelijkheid vallen.
- De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van Bestuur en Directie over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin zij haar bevindingen en aanbevelingen vastlegt.
- De directie en de afdelingsmanagers stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de FG. Desgevraagd verstrekken zij aanvullende informatie aan deFG.
- Tijdens Marap-gesprekken dient er aandacht te zijn voor de privacy n.a.v. de rapportage van de FG. De onderwerpen, die als risicovol worden gezien, moeten worden opgenomen in de interne auditplannen.
- De afdelingsmanagers zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- De afdelingsmanagers zijn verantwoordelijk voor het oefenen met privacy incidenten en bedrijfscontinuïteit.
- Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
- Afdelingsmanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingsmanagers voeren bij verwerken van persoonsgegevens (Pre-)DPIA's uit op basis van de AVG om deze risicoafwegingen te kunnen maken.
- Privacybescherming maakt onderdeel uit van de werkoverleggen op de afdelingen.

Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- Privacy eisen maken deel uit van afspraken met ketenpartners en leveranciers en worden periodiek geëvalueerd/gecontroleerd.

- Kennis en bewustzijn van privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een privacyplan opgesteld onder leiding van de directeur belast met Bedrijfsvoering, gebaseerd op:
- Dit strategisch privacybeleid;
- Audit resultaten;
- Uitkomsten risico-analyses en DPIA's
- De door de afdelingsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).
- Om uitvoering te kunnen geven aan dit strategisch beleid en het privacy plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

4. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij het in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defense'). In dit model is het lijnmanagement verantwoordelijk voor het realiseren van privacy binnen de eigen processen. De tweede lijn (compliance officers, PO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering.

Aansturing: directie

De directie zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager. De directie zorgt dat de afdelingsmanagers zich verantwoorden over de bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouder binnen het dagelijks bestuur gevraagd en ongevraagd geïnformeerd wordt over de mate waarin privacybescherming een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan de directie zich ook verantwoorden naar het dagelijks en algemeen bestuur.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische privacybeleidsonderwerpen en laat zich hierin bijstaan door de PO en adviseren door de FG van VR NHN. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp privacybescherming wordt bij VR NHN gezien als een integraal onderdeel van risicomanagement.

Uitvoering: afdelingsmanagers

Privacybescherming valt onder de verantwoordelijkheden van alle afdelingsmanagers en onder hen werkende andere leidinggevenden. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. Alle processen, systemen, (persoons)gegevens, applicaties hebben altijd minimaal 1 eigenaar; er moet dus altijd iemand verantwoordelijk zijn. Afdelingsmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde privacybeschermende activiteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door 3 keer per jaar het onderwerp privacy te bespreken in het marap-overleg.

Taken van de afdelingsmanagers in het kader van privacybescherming zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wet- en regelgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht is.
- Het binnen de eigen afdeling uitdragen van het privacybeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste privacybedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het vroegtijdig betrekken van PO of compliance officer bij nieuwe of gewijzigde processen
- Het (laten) uitvoeren van risicoanalyses en (pre-)DPIA's voor de processen waar zij verantwoordelijk voor zijn.
- Bespreking van beveiligingsincidenten en privacy inbreuken en de consequenties die dit moet hebben voor beleid en maatregelen.

Controle en verantwoording

Dit Strategisch privacybeleid is een verantwoordelijkheid van het bestuur van VR NHN. De bestuurders en directeuren van VR NHN zullen werken volgens de 10 principes voor informatiebeveiliging en de beginselen voor het verwerken van persoonsgegevens. Zij geven sturing aan het onderwerp privacy door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over privacy aan de portefeuillehouder in het dagelijks bestuur. De directie rapporteert daarnaast over de mate waarin zij invulling heeft gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.
De verantwoording over de privacybescherming komt in het jaarverslag tot uitdrukking in de verklaring Informatiebeveiliging en privacy. Met deze verklaring geeft de directie aan in hoeverre VR NHN voldoet aan de afspraken die gemaakt zijn ter naleving van de wettelijke eisen uit o.a. de AVG. Ook worden de eventuele verbetermaatregelen vermeld die VR NHN gaat treffen. De ingevulde zelfevaluatievragenlijst https://www.cip-overheid.nl/productcategorieen-en-workshops/producten?product=privacyselfassessmenttoolvormt de basis voor het opstellen van de directieverklaring aan het Dagelijks Bestuur.
Middels deze verantwoording wordt het Dagelijks Bestuur geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat VR NHN privacybescherming serieus neemt en het een onderdeel laat zijn van de ambities om persoonsgegevens van haar medewerkers en alle hulpbehoevende burgers in het verzorgingsgebied van VRNHN adequaat te beschermen.

Vastgesteld op: 6 februari 2025 door het dagelijks bestuur van VRNHN

Voorzitter
A.M.C.G. Schouten

Secretaris
K. Taneja