Veiligheidsregio
Groningen

Informatieveiligheid en privacybeleid

Strategie VRG voor Security & Privacy

Versie 1.0, 2025

Veiligheidsregio Groningen

Inhoudsopgave

Veiligheidsregio Groningen

1 De beleidskaders voor informatieveiligheid en privacy

1.1 Achtergrond

Informatiebeveiliging en privacybescherming is belangrijk, zo ook voor Veiligheidsregio Groningen (hierna ook te noemen: VRG). VRG is in toenemende mate afhankelijk van informatie die is opgeslagen in (veelal geautomatiseerde) systemen. Deze afhankelijkheid brengt kwetsbaarheden en risico's met zich mee waar we ons tegen willen en moeten beschermen om de bedrijfscontinuïteit te kunnen waarborgen. Mede door de sterke toename van cybercriminaliteit, de veranderende en onzekere machtsverhoudingen in de wereld en de steeds prominentere rol van de veiligheidsregio als vitale organisatie de laatste jaren, neemt VRG maatregelen om de organisatie, de medewerkers, vrijwilligers en de inwoners te beschermen. Waar het soms wettelijke maatregelen zijn die VRG moet implementeren (BIO2), kan er vaak ook een afweging worden gemaakt om de balans tussen veiligheid en werkbaarheid te behouden. Tevens worden de mogelijke risico's en de kosten van eventuele maatregelen afgewogen en op basis van een gedegen risicoanalyse gemaakt.

De kern van privacybescherming is ervoor zorgen dat er zorgvuldig wordt omgegaan met de verwerking van persoonsgegevens. Hiertoe is reeds in 2018 Europa-breed de Algemene Verordening Gegevensbescherming (hierna: AVG) ingevoerd. Hiermee zijn de eisen verscherpt waaraan verwerking en bescherming van persoonsgegevens moeten voldoen. Eén van deze eisen is dat VRG een privacybeleid moet hebben. In 2019 is beleid hieromtrent reeds vastgesteld, maar door actuele ontwikkelingen in maatschappij, wet- en regelgeving is het van belang nieuw beleid op te stellen dat beter aansluit bij de huidige richtlijnen en ook de komende jaren voldoet.

Vanwege de samenhang tussen informatieveiligheid en privacybescherming is er gekozen voor één beleidsstuk voor beide onderwerpen. Dit document, het Informatieveiligheid en privacy beleid (hierna: IPB) beschrijft het kader voor de inrichting van privacybescherming en informatieveiligheid. Het beschrijft de missie en visie van VRG ten aanzien van informatieveiligheid en privacy, alsook de verantwoordelijkheden, bevoegdheden en de manier waarop een continue verbetercyclus wordt ingericht. Het is essentieel om te benadrukken dat het borgen van de veiligheid van inwoners, ongeacht de uitwerking de belangrijkste taak van VRG is. Er kunnen zich situaties voordoen waarin een afweging moet worden gemaakt tussen de belangen van privacy en/of informatieveiligheid van inwoners en andere beschermingsbelangen, waarbij dit latere belang prevaleert omwille van de bescherming van hun (fysieke) veiligheid of die van anderen.

Naast diverse securitymaatregelen waar medewerkers tijdens hun werk mee moeten omgaan, voorziet de AVG ook in diverse rechten (en plichten) voor medewerkers. Zo hebben betrokkenen (de medewerkers van VRG en externe personen van wie persoonsgegevens bij VRG berusten) onder meer het recht op inzage, correctie en verwijdering van de persoonsgegevens waarover we beschikken. Betrokkenen hebben ook het recht om 'vergeten' te worden. Er kleven echter grenzen aan deze rechten, zo kunnen bijvoorbeeld wettelijk voorgeschreven bewaarplichten in de weg staan aan het recht op vergetelheid.

De uitwerking van en het handelen naar dit beleid binnen VRG betreft niet alleen het team IM/ICT, maar de organisatie in haar geheel. De veilige omgang met informatie raakt de gehele organisatie. Incidenten en inbreuken in de werkprocessen kunnen leiden tot een verminderde dienstverlening richting de inwoner, financiële schades en imagoschade. Het is daarom noodzakelijk om systematisch en structureel aandacht te besteden aan het bewustzijn op het gebied van informatieveiligheid en privacy.

1.2 Totstandkoming

Het IPB is gebaseerd op de internationale standaarden voor informatieveiligheid: ISO 27001 en ISO 27002 en aangevuld met privacyaspecten. Bij het opstellen van het beleid is rekening gehouden met de ISO 27001 & 27002 versie 2022, de Baseline Informatiebeveiliging Overheid (BIO), NIS2 en de Algemene Verordening Gegevensbescherming. Ook is gekeken naar 'best practice' voorbeelden van andere organisaties.

Het IPB is een richtinggevend document. De intentie is niet dat alle medewerkers exact weten wat er in het IPB staat, maar men moet wel weten dat het beleid er is, hoe het te gebruiken en wat de belangrijkste uitgangspunten zijn. De uitgangspunten worden op basis van dit beleid verder uitgewerkt in aanvullende procedures, die onder de aandacht gebracht worden van de medewerkers en vrijwilligers van VRG (zie hoofdstuk 6). Separaat van dit document zal er een roadmap worden opgesteld, waarin staat beschreven hoe en wanneer deze procedures worden opgesteld of geüpdatet, zodat ze aansluiten bij de huidige ontwikkelingen op het gebied van Security en Privacy.

1.3 Definitie en doelstelling informatieveiligheid en privacy

Informatieveiligheid en privacy

Informatieveiligheid beschermt informatie tegen een breed scala aan bedreigingen en heeft tot doel de bedrijfscontinuïteit te waarborgen. Onder privacy wordt verstaan de bescherming van persoonsgegevens en naleving van de persoonlijke levenssfeer. In dit beleid betreffen informatieveiligheid en privacy alle beheersingsmaatregelen die gericht zijn op het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens[1] en het beperken van de eventuele gevolgen van beveiligingsincidenten tot een acceptabel niveau (dit niveau wordt bepaald op basis van een risico-analyse) Hierbij worden zowel elektronische gegevens en informatiesystemen, maar ook bijvoorbeeld papieren dossiers met de dezelfde mate van aandacht behandeld.

De BIO is een vertaling van de ISO 27001/2 waar Nederlandse overheidsinstellingen aan moeten voldoen. Naar verwachting zal eind 2025 de vernieuwde BIO (= BIO2) van kracht worden. De BIO2 beschrijft een groot aantal beveiligingsrichtlijnen die door de opstellers ervan als (minimaal) noodzakelijk worden beschouwd. De richtlijnen zijn functioneel ingedeeld in hoofdstukken die gaan over beleid, organisatie, personeel, beheer, toegangsbeveiliging, fysieke beveiliging, cryptografie, beveiliging van de bedrijfsvoering, communicatie, ontwikkeling, leveranciersrelaties, beveiligingsincidenten, continuïteit en naleving. Middels externe toetsing wordt gemeten of de veiligheidsregio's in control zijn betreffende de BIO maatregelen, en waar ze nog moeten verbeteren.

1.4 Verwerken van persoonsgegevens

Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon. Persoonsgegevens mogen alleen worden verwerkt voor een bepaald doel en slechts als daarvoor een van de volgende grondslagen aanwezig is:

- De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
- De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.
- De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
- De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

In de AVG wordt onderscheid gemaakt tussen 'gewone persoonsgegevens' en 'bijzondere categorieën van persoonsgegevens'. Bijzondere persoonsgegevens zijn gegevens die vanwege hun aard extra gevoelig zijn. Het betreft bijvoorbeeld informatie over:

- Ras of etnische afkomst.
- Politieke opvattingen.
- Religieuze of levensbeschouwelijke overtuigingen.
- Lidmaatschap van een vakbond.
- Genetische gegevens.
- Biometrische gegevens.
- Medische gegevens.
- Seksueel gedrag of seksuele gerichtheid.

Het verwerken van bijzondere persoonsgegevens is verboden, tenzij een wettelijke uitzondering van toepassing is, of de betrokkene uitdrukkelijk toestemming heeft verleend voor de verwerking. Ook gegevens van strafrechtelijke aard zijn dermate gevoelig dat voor de verwerking ervan specifieke regels gelden. Het verwerken van zulke gegevens is alleen toegestaan als dat gebeurt door of onder toezicht van de overheid, of als de verwerking ervan specifiek is geregeld in de wet.

Ook gegevens die volgens de AVG niet bijzonder of strafrechtelijk van aard zijn, kunnen volgens de Autoriteit

[1] In het informatieveiligheid en privacy beleid hanteren we de volgende definities:
Beschikbaarheid, i.e. het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.
Integriteit, i.e. het waarborgen van de juistheid en de volledigheid van informatie en verwerking.
Vertrouwelijkheid, i.e. het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe geautoriseerd zijn.

Persoonsgegevens gevoelig zijn. Het gaat bijvoorbeeld om financiële gegevens. Afhankelijk van het risico van het verwerken van zulke gegevens voor de betrokkenen, moeten voor de bescherming van dergelijke gevoelige gegevens specifieke maatregelen worden getroffen.

1.5 Reikwijdte

Het IPB is een zelfstandig document, maar kan niet los worden gezien van de visie, strategie en doelstellingen van de sectoren binnen en de overkoepelende visie van Veiligheidsregio Groningen en architectuurprincipes, die richting geven aan de invulling van het IBP-beleid. Het beleid, de hieruit afgeleide richtlijnen en de op basis van deze richtlijnen ingevoerde maatregelen, gelden voor zowel vast als tijdelijk (ingehuurd) personeel als alle partijen die diensten voor de veiligheidsregio verrichten. Met de komst van BIO2 moeten we als VRG erop toezien dat onze ketenpartners ook de juiste security- en privacy vereisten toepassen. Dit beleid is van toepassing op de omgang met informatie door of namens VRG, in welke vorm dan ook (dus inclusief persoonsgegevens).

2 Strategie voor informatieveiligheid en privacy

2.1 Ambitie

VRG kiest ervoor om informatieveiligheids- en privacyrisico's tenminste op het beveiligingsniveau van de BIO2 te implementeren. De BIO2 beschrijft de (minimale) maatregelen waaraan VRG moet voldoen om de informatieveiligheid en privacy te waarborgen. De BIO2 is het vervolg op de BIO (Baseline Informatieveiligheid Overheid), en het is verplicht om als overheidsorganisatie hieraan te voldoen. VRG kiest daarom net als de andere veiligheidsregio's voor de BIO2 als beveiligingsniveau. Doordat de veiligheidsregio's in 2025 vitaal worden verklaard en informatie over cyberdreigingen uit de eerste hand krijgt van het NCSC, hebben veiligheidsregio's ook de verplichting interne cyberincidenten te melden aan het NCSC. De maatregelen in de BIO2 vormen ook de basis voor de externe toetsing op het gebied van informatieveiligheid en privacy.

Als blijkt dat in sommige situaties of voor sommige systemen het beveiligingsniveau van de BIO2 niet volstaat of dat juist de maatregelen het effect hebben dat er een onwerkbare situatie ontstaat, dan bepalen directie en/of het lijnmanagement welke (aanvullende) risico's zij, in het licht van de doelstellingen, bereid zijn te lopen. Hiertoe worden jaarlijks onder meer voor de meest kritische processen, bij belangrijke wijzigingen in de VRG strategie, systemen en/of verwerkingen van persoonsgegevens risicoanalyses uitgevoerd en/of herijkt. Denk hierbij bijvoorbeeld aan risico's die worden veroorzaakt door calamiteiten en storingen van belangrijke informatiesystemen en de verwerking van persoonsgegevens. Tevens zal na implementatie van de BIO2, jaarlijks gekeken moeten worden of er extra maatregelen geïmplementeerd moeten worden, rekening houdend met de laatste stand van zaken van de techniek en ontwikkelingen op het gebied van wet- en regelgeving en in de maatschappij. Denk bijvoorbeeld aan cyberrisico's.

Informatieveiligheid en privacy zijn geen doel op zich maar dienen een integraal onderdeel van de bedrijfsprocessen en informatievoorziening van de Veiligheidsregio te zijn. De doelstellingen worden verder uitgewerkt in hoofdstuk 5.2 van dit beleidsdocument in een procesmodel informatieveiligheid en privacy (afgeleid van de kwaliteitscirckel van Deming, Plan/Do/Check/Act).

2.2 Doelstellingen van informatieveiligheid en privacy

Een belangrijk doel van informatieveiligheid en privacy is het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie voor Veiligheidsregio Groningen. Hieronder zijn de doelstellingen van het informatieveiligheid en privacy beleid van de Veiligheidsregio geformuleerd:

- De continuïteit van de bedrijfsvoering binnen VRG beschermen;
- Het waarborgen van de privacy van betrokkenen;
- Het voldoen aan de wet- en regelgeving;
- De bescherming van middelen en kapitaal;
- Het voorkomen en beheersbaar maken van calamiteiten;
- Het beschermen van het imago van de Veiligheidsregio Groningen;
- Zorgdragen voor risicobewust handelen van medewerkers;
- Het minimaliseren van de kosten van herstel;
- Bewustwording medewerkers creëren en verhogen;
- Transparant (kunnen) zijn naar diverse belanghebbenden.

3 Strategische uitgangspunten

VRG hanteert, afgeleid van de doelstellingen betreffende Informatieveiligheid en privacy (zie 2.2), een aantal strategische uitgangspunten ten aanzien van informatieveiligheid en privacy. Een strategisch uitgangspunt is een criterium waaraan de richtlijnen en maatregelen op het gebied van informatieveiligheid en privacy binnen Veiligheidsregio Groningen moeten voldoen. De strategische uitgangspunten hebben betrekking op de aandachtsgebieden organisatie, proces, mens en techniek en zijn enerzijds gebaseerd op het beleid van de veiligheidsregio en anderzijds op 'best practices'.

VRG hanteert de volgende strategische uitgangspunten ten aanzien van informatieveiligheid en privacy:

- Informatieveiligheid en privacy worden beschouwd als een vanzelfsprekend en integraal onderdeel van de bedrijfsvoering van Veiligheidsregio Groningen.
- Veiligheidsregio Groningen hanteert de BIO2 (ISO 27001/2) als basis voor het inrichten en onderhouden van maatregelen voor het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van haar bedrijfsgegevens.
- Bij het inrichten en onderhouden van de maatregelen houdt Veiligheidsregio Groningen rekening met de geldende wet- en regelgeving en in het werkveld gestelde kaders op gebied van informatieveiligheid en privacy. De volgende wet- en regelgeving zijn in ieder geval van toepassing:
  - Baseline Informatieveiligheid Overheid 2 (BIO2);
  - Algemene Verordening Gegevensbescherming (AVG);
  - Wet Veiligheidsregio's;
  - Archiefwet;
  - Telecommunicatiewet;
  - Cyberbeveiligingswet;
  - Europese AI-act.
- Het IPB is leidend voor alle activiteiten die voor en/of onder verantwoordelijkheid van Veiligheidsregio Groningen worden uitgevoerd. Het betreft organisatie, afdelingen en medewerkers die bij de activiteiten betrokken zijn. In de verschillende procedures die onder dit beleid hangen, wordt dit verder uitgewerkt.
- Relaties tussen Veiligheidsregio Groningen en externe partijen die betrekking hebben op de informatievoorziening van de veiligheidsregio dan wel de informatievoorziening van deze organisatie, gaan vergezeld van schriftelijke afspraken over het vereiste beveiligings- en privacyniveau en de wijze waarop zekerheid wordt verkregen over de realisatie daarvan.
- Om invulling te geven aan het IPB voert Veiligheidsregio Groningen concrete, transparante en controleerbare maatregelen in op basis van richtlijnen die worden opgesteld door de organisatie.
- Het management en/of de teamleiders van de afdelingen van Veiligheidsregio Groningen besluit op basis van risicoanalyses welke aanvullende maatregelen noodzakelijk zijn. Dit kan bijvoorbeeld zijn omdat ze wettelijk zijn voorgeschreven of omdat ze naar mening van het management voor een bepaald proces noodzakelijk zijn. Het management krijgt hierover (on)gevraagd advies van de CISO (Chief Information Security Officer) en/of de FG (Functionaris Gegevensbescherming).
- Veiligheidsregio Groningen beoogt een sterke verbinding met de medewerkers, het werkveld en de omgeving. Hiervoor is een open en flexibele inrichting op diverse terreinen noodzakelijk. Het IPB sluit hier zoveel mogelijk op aan, door te kiezen voor het BIO2 beveiligingsniveau met algemeen bekende en landelijk vastgestelde maatregelen, om complexiteit zoveel mogelijk te voorkomen.

Als veiligheidsregio houden we ons bij het verwerken van persoonsgegevens aan de wet. Los van de verplichtingen uit de wet vinden we dat inwoners, medewerkers en vrijwilligers moeten kunnen vertrouwen op een veilige en zorgvuldige omgang met hun persoonsgegevens. Tegelijkertijd zijn we belast met een aantal primaire taken, waarbij soms een afweging moet worden gemaakt tussen de adequate uitoefening van de publiekrechtelijke taak en de privacy van betrokkenen. Als deze situaties zich voordoen, hanteren we voor de te maken afweging altijd de volgende uitgangspunten en leggen we de beoordeling en de uitkomst vast. Bij het beoordelen van privacy risico's via een Data Protection Impact Assessment[2] (hierna ook te noemen DPIA) worden deze punten behandeld. De FG ziet hierop toe. De volgende principes zijn leidend voor een zorgvuldige omgang met persoonsgegevens:

Rechtmatigheid, behoorlijkheid en transparantie
Persoonsgegevens mogen alleen worden verwerkt als daarvoor een formele grondslag aanwezig is, zoals eerder benoemd in hoofdstuk 1.4 van dit beleid . De verwerking moet op behoorlijke en verantwoordbare wijze plaatsvinden. Ook moet duidelijk

[2] Een instrument waarmee organisaties privacyrisico's in een vroegtijdig stadium op een gestructureerde en heldere manier in kaart kunnen brengen

zijn voor welke doelen en op welke wijze persoonsgegevens worden verwerkt.

Doelbinding
Het verwerken van persoonsgegevens mag uitsluitend voor welbepaalde, uitdrukkelijk beschreven en gerechtvaardigde doeleinden. Het gebruik van de persoonsgegevens voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verwerkt is niet toegestaan.

Minimale gegevensverwerking / dataminimalisatie
Uitgangspunt is dat er niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk is voor het doel van de verwerking.

Gegevenskwaliteit
De verwerkte persoonsgegevens dienen correct en actueel te zijn. Persoonsgegevens die niet actueel, juist en volledig zijn moeten worden verwijderd of gecorrigeerd.

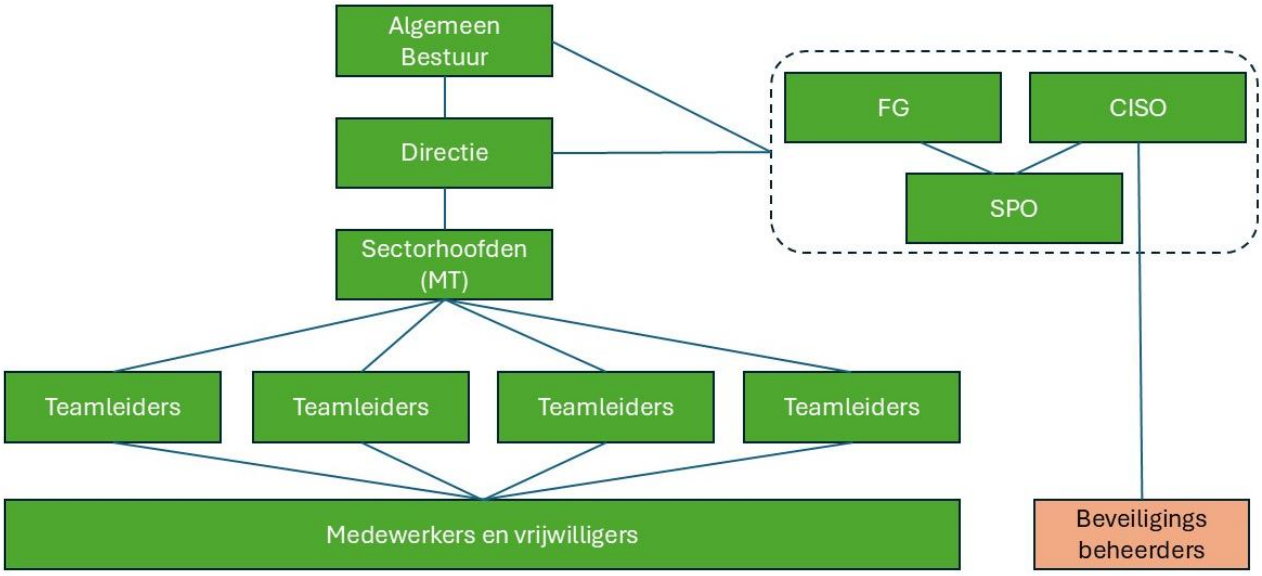
Opslag van persoonsgegevens
Het bewaren van persoonsgegevens mag niet langer dan noodzakelijk is voor het doel van de verwerking en/of om te voldoen aan specifieke wetgeving. Als het niet langer noodzakelijk is om gegevens te verwerken, dan moeten ze worden vernietigd of gewist. Het voor langere perioden opslaan van persoonsgegevens mag uitsluitend met het oog op archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek of statistische doeleinden.

Integriteit en vertrouwelijkheid
Er moeten passende beveiligingsmaatregelen worden getroffen om persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. De verwerkingsverantwoordelijke moet aan kunnen tonen dat persoonsgegevens worden verwerkt in overeenstemming met voornoemde beginselen voor gegevensbescherming.

4 De organisatie van informatieveiligheid en privacy

4.1 Organisatiestructuur

In dit hoofdstuk worden de taken, bevoegdheden en verantwoordelijkheden voor informatieveiligheid en privacy voor alle medewerkers en vrijwilligers benoemd en wordt aangegeven bij welke functionarissen in het bijzonder deze worden belegd. Door het expliciet beleggen van de verantwoordelijkheden wordt informatieveiligheid en privacy verankerd in de bestaande organisatie. Gelet op de mogelijke impact van verstoringen op de continuïteit van VRG berust de eindverantwoordelijkheid voor dit beleid bij de directie van VRG (gemandateerd vanuit het Algemeen Bestuur). De CISO ziet erop toe dat tenminste iedere vijf jaar een herijking plaatsvindt van dit beleid. De afbeelding hieronder illustreert de organisatiestructuur. *Let wel: het gaat hier om de logische structuur betreffende verantwoordelijkheden voor Informatieveiligheid en Privacy en niet over de hiërarchische inbedding van de rollen van CISO en FG in de organisatie.*



Figuur 1: Organisatie van informatieveiligheid en privacy

Hoewel de CISO en de FG kaders stellen, zorgdragen dat de VRG aan wetgeving voldoet, technisch de nodige maatregelen doorvoeren en verantwoordelijk zijn voor het continu meer bewust maken van medewerkers op het gebied van Security en Privacy, hebben de CISO, de SPO (Security & Privacy Officer) en FG wel alle medewerkers nodig. Informatieveiligheid en privacy is namelijk een integrale verantwoordelijkheid van de gehele organisatie en van iedere medewerker, waarvoor dit beleid slechts het kader vormt. Van het management wordt verwacht dat zij hieraan nader invulling geven. Voorop staat dat directie en management hierin een voorbeeldfunctie hebben. De wijze waarop die voorbeeldfunctie wordt ingevuld, bepaalt in belangrijke mate de informatieveiligheid en privacy cultuur van VRG als geheel. Hiermee zijn ze dus óók verantwoordelijk voor de informatieveiligheid en privacy binnen die processen.

4.2 Eindverantwoordelijk

De eindverantwoordelijkheid voor informatieveiligheid en privacy ligt bij het Algemeen Bestuur van de Veiligheidsregio Groningen. De gemandateerde verantwoordelijkheid voor informatieveiligheid en privacy ligt bij de directie van VRG. De CISO en FG kunnen (on)gevraagd direct adviseren en rapporteren aan de directie. Tevens wordt door de CISO en FG verantwoording afgelegd aan het Algemeen Bestuur middels een jaarrapportage, waarin staat beschreven wat er in het afgelopen jaar is gebeurd, inclusief een overzicht van eventuele afwijkingen. Verder wordt ook in jaarrapportage een doorkijkje gegeven met welke (nieuwe) ontwikkelingen rekening moet worden gehouden op de gebieden van Informatieveiligheid en privacy. Ook zullen dreigingsbeelden en handelingsperspectieven op het gebied van Cybersecurity worden gedeeld met het Algemeen Bestuur, wanneer dit relevant is voor VRG.

Het management team (MT) is (mede)verantwoordelijk voor het coördineren van de implementatie van het beleid en de richtlijnen door de verschillende onderdelen van Veiligheidsregio Groningen en het toezicht op de handhaving van deze richtlijnen. De CISO zal beleid op het gebied van Informatieveiligheid en Privacy ook altijd eerst langs het MT laten gaan, zodat het hier kan worden vastgesteld en MT op de hoogte is van gekozen richting en maatregelen. Per sector is de sectordirecteur (MT-lid) verantwoordelijk voor het inrichten van adequate informatieveiligheid en privacy binnen de processen die vallen binnen zijn/haar verantwoordelijkheidsgebied. Dit natuurlijk in overeenstemming met het gestelde beleid en de richtlijnen

4.3 Verantwoordelijkheid teamleiders

De teamleider is, binnen het beleid van VRG als geheel, verantwoordelijk voor de (integrale) uitvoering van de informatieveiligheid bevorderende beheersing in haar domein, binnen door de directie gestelde kaders. De verantwoordelijkheid van de teamleider brengt onder meer mee dat de risico's gekend, geanalyseerd en beheerst worden. De teamleider draagt zorg dat binnen VRG de verplichtingen van VRG worden nageleefd. Hieronder valt ook het nemen van gepaste acties, na overleg met CISO en/of FG, om incidenten te voorkomen en te herstellen. Een teamleider van VRG heeft verder een actieve, sturende en faciliterende rol bij het stimuleren van het handelen en het zetten van de juiste 'toon'. Hierdoor creëert VRG voor haar medewerkers een open en veilige omgeving waarbij ruimte bestaat om dilemma's bespreekbaar te maken.

De teamleider is onder meer verantwoordelijk voor:
- Het hanteren en uitdragen van de beleidsuitgangspunten en richtlijnen;
- Het aan de hand van de richtlijnen invoeren van maatregelen;
- Het waarborgen van de naleving van het beleid;
- Het bevorderen van het beveiligings- en privacy bewustzijn;
- Het zelf melden en het wijzen op het belang van melden door teamleden, van beveiligingsincidenten/datalekken aan de CISO, FG of SPO.

Voor bovenstaande kan altijd de hulp worden gevraagd van de CISO, FG en SPO. Het is hierbij van belang dat door de teamleiders niet slechts incidenteel, maar structureel en planmatig aandacht wordt besteed aan informatieveiligheid en privacy.

4.4 Verantwoordelijkheid medewerkers

Alle medewerkers inclusief tijdelijk ingehuurde medewerkers en vrijwilligers hebben toegang tot informatie en zijn primair verantwoordelijk voor en aanspreekbaar op hun eigen gedrag. Zij bepalen in eerste instantie zelf op welke wijze zij, binnen het raamwerk van regels en organisatorische maatregelen, kunnen handelen overeenkomstig de door de organisatie gestelde normen. Met vragen en dilemma's kunnen ze contact opnemen met hun teamleider, beveiligingsbeheerder of de CISO, FG en/of SPO.

4.5 Beveiligingsbeheerders

Zoals hiervoor al geschetst zijn Security en Privacy onderwerpen binnen VRG waar de gehele organisatie en ieder individu verantwoordelijk voor is. Hiervoor hebben de CISO, de SPO (Security & Privacy Officer) en FG wel alle medewerkers nodig. Om alle medewerkers nog sneller en beter te kunnen bereiken, maar ook om meer inzicht te krijgen op de gehele omgeving van VRG zijn er 'ambassadeurs voor beveiliging' binnen VRG aangesteld, bestaande uit medewerkers van verschillende teams. Dit beveiligingsbeheerdersteam valt onder regie van de CISO, die ook verantwoordelijk is voor de werking van, kennis binnen en continuïteit van dit multidisciplinaire team.

Naast de CISO, de FG en de SPO bestaat het team uit dagdienst medewerkers van VRG die onderstaande rol invullen:

Omschrijving
Beveiligingsbeheerder technisch IM/ICT
Beveiligingsbeheerder applicaties
Beveiligingsbeheerder fysieke toegang
Beveiligingsbeheerder websites en externe communicatie

Beveiligingsbeheerder Veilig personeel & Screening
Beveiligingsbeheerder Vakbekwaamheid
Beveiligingsbeheerder S&O
Beveiligingsbeheerder T&O / Informatievoorziening (operationeel)
Beveiligingsbeheerder Technische Dienst
Beveiligingsbeheerder Crisisbeheersing en opschaling
Beveiligingsbeheerder Risicobeheersing

4.5.1 Wat doet de beveiligingsbeheerder

Naast dat een aantal beveiligingsbeheerders ook vanuit hun dagelijkse functie te maken hebben met Security en Privacy – en verantwoordelijk zijn voor een bepaald deel van het veiligheidsdomein, denk aan toegangscontrole, screening personeel etc. - kunnen zij ook gezien worden als de (extra) ogen en oren voor de CISO, SPO en de FG. Zij horen wat er speelt binnen een afdeling/team en op het gebied van informatieveiligheid en privacy. Zij kunnen eventueel directe collega's helpen, wanneer deze een vraag hebben met betrekking tot informatieveiligheid en privacy. Natuurlijk kunnen ze een directe collega ook doorverwijzen naar de CISO, SPO en de FG, als dat nodig blijkt te zijn. Aangezien de beveiligingsbeheerders op de hoogte zijn en kennis hebben van de werkprocessen die spelen binnen hun afdeling/team, wijzen ze ook collega's op eventuele security- en privacyvraagstukken. Hierbij kan gedacht worden aan een wijziging in het werkproces, aanschaf nieuwe applicatie/module waarbij er iets wezenlijks verandert, waar Security of Privacy iets mee moet. Tenslotte zijn de beveiligingsbeheerders in grote lijnen op de hoogte van het informatieveiligheids- en privacybeleid en de maatregelen voortkomend uit onder andere de BIO. Zij ondersteunen de CISO, SPO en de FG bij implementatie en naleving van de maatregelen en kijken kritisch of de getroffen maatregelen ook werken binnen VRG.

De CISO organiseert 4 keer per jaar een (fysiek) beveiligingsbeheerder overleg. Daarnaast zorgen de CISO en Security & Privacy Officer ervoor dat de beveiligingsbeheerders worden geïnformeerd over updates en/of wijzigingen in beleid en maatregelen. Dit zodat ze altijd op de hoogte zijn van de laatste stand van zaken betreffende de informatieveiligheid en privacy maatregelen van VRG.

4.6 CISO, FG en SPO

De CISO en de FG zijn verantwoordelijk ten aanzien van het opstellen van, het communiceren over en het toezien op de naleving van het beleid betreffende informatieveiligheid en privacy. In die hoedanigheid initiëren zij activiteiten binnen de lijnorganisatie ten aanzien van de uitvoering en naleving van de getroffen maatregelen en ook het bewaken van de actualiteit van het beleid (IPB), de richtlijnen en de maatregelen. Daarnaast kunnen zij het Algemeen Bestuur, de directie en het lijnmanagement (gevraagd en ongevraagd) adviseren over de stand van zaken en inrichting van de informatieveiligheid en privacy. Ze zijn verantwoordelijk voor controle op de algehele en organisatie-brede naleving van het IPB en de daarvan afgeleide instructies en rapporteren over de bevindingen aan de directie. Vanuit deze verantwoordelijkheid kunnen zij zelfstandig controles uitvoeren of deze initiëren om de naleving van het beleid te garanderen.

4.6.1 Chief Information Security Officer

De CISO is hiërarchisch gezien onderdeel van team IM/ICT en treedt op als adviseur, sparringpartner van en eerste aanspreekpunt voor de directie en kan bij ernstige beveiligingsrisico's of non-compliance rechtsreeks escaleren naar de directie. Verder heeft de CISO een centrale rol in de strategische en tactische beveiliging van de informatievoorzieningen van VRG. De CISO richt zich op de interne bedrijfsvoering, de ontwikkelingen op het gebied van Cybersecurity en is onderdeel van verschillende landelijke (strategische) overleggremia. Tevens is de CISO een belangrijke pion in diverse interne en externe projecten om de Informatieveiligheid en de continuïteit van VRG te borgen, waarbij in het geval van onvoldoende beveiligingsborging de CISO het (dwingende) advies kan geven het (IT)-project aan te passen of zelfs stop te zetten.

De CISO rapporteert rechtstreeks aan de directie en eventueel het Algemeen Bestuur, is bevoegd om binnen de hele organisatie gevraagd en ongevraagd onderzoek te (laten) doen en is verantwoordelijk voor de informatiebeveiligingsstrategie. De activiteiten van de CISO zijn onder meer de volgende[3]:

- De CISO vertaalt de strategie en doelstellingen van VRG naar informatieveiligheid-gerelateerde projecten en jaarplannen.

[3] In het functieprofiel van de CISO staan alle werkzaamheden van de CISO beschreven.

- De CISO stelt beleid op betreffende informatieveiligheid en privacy.
- De CISO voert risicoanalyses om risico's en kansen in kaart te brengen uit en maakt impactanalyses.
- De CISO identificeert en adviseert om informatiebeveiligingsrisico's te mitigeren
- De CISO rapporteert aan de directie en bestuur ook over zaken als non-compliance.
- De CISO zorgt dat VRG op de hoogte blijft van trends en ontwikkelingen op het gebied van digitale informatieveiligheid en houdt VRG op dat vlak in beweging.
- De CISO zorgt ervoor dat de medewerkers van VRG zich bewust zijn van het belang van informatieveiligheid.
- De CISO ondersteunt het lijnmanagement bij het vertalen van informatieveiligheidsdoelstellingen naar maatregelen en/of concrete projecten.
- De CISO initieert en coördineert audits en certificeringstrajecten.
- De CISO selecteert (in overleg met de FG) de te nemen maatregelen voor het beschermen van persoonsgegevens. De FG ziet toe op naleving van deze maatregelen.

4.6.2 Functionaris Gegevensbescherming

Net als de CISO is de FG hiërarchisch gezien onderdeel van team IM/ICT. De FG informeert en adviseert VRG en de medewerkers die persoonsgegevens verwerken over hun verplichtingen op grond van de AVG. De FG houdt toezicht op de toepassing en naleving van de AVG. De VRG is verantwoordelijk om een overzicht van gegevensverwerkingen bij te houden en de FG houdt hier toezicht op. Ook heeft de VRG de taak om DPIA 's uit te laten voeren, waarbij het verplicht is om de FG vooraf om advies te vragen. Tot slot fungeert de FG als (eerste) aanspreekpunt en sparringpartner voor de Autoriteit Persoonsgegevens (AP) en handelt mogelijke datalekken af.

De maatregelen zijn niet alleen van technische aard maar met name ook gericht op het correct inrichten van de processen en de uitvoering daarvan. Maar misschien nog wel het belangrijkste is de bewustwording rondom het gebruik van persoonsgegevens en de mogelijke impact van het gebruik daarvan. De activiteiten van de FG omvatten onder meer:

- Het houden van toezicht op de naleving van privacywetgeving;
- Het inventariseren van (persoons)gegevensverwerkingen;
- Het ontwikkelen van interne regelingen, zoals bijvoorbeeld een gedragscode, inzageverzoeken, etc. ;
- Het bijhouden van meldingen van (persoons)gegevensverwerkingen;
- Het behandelen van vragen en klachten van personeelsleden, vrijwilligers, burgers en anderen van wie persoonsgegevens worden verwerkt;
- Het accorderen van opgestelde DPIA's en toezien op de in de DPIA benoemde maatregelen;
- Het geven van voorlichting op het gebied van privacy en omgang met (persoons)gegevens.

Daarnaast geeft de FG net als de CISO (gevraagd en ongevraagd) advies aan de directie en het lijnmanagement en werkt nauw samen met de CISO voor het actueel houden van het beleid. Van groot belang is dat de FG onafhankelijk te werk kan gaan. De FG en CISO werken samen bij bijvoorbeeld het toetsen van projecten op informatieveiligheid en privacy risico's). De FG rapporteert, net als de CISO, ook aan de directie.

4.6.3 Security en Privacy Officer

Binnen VRG is ook de functie van Security en Privacy Officer (SPO) belegd. De SPO is verantwoordelijk voor het uitvoeren van het informatiebeveiligings en privacy beleid en maakt de vertaalslag van de strategie die door de CISO is bepaald naar tactisch/operationeel niveau. De SPO biedt op het vlak van security ondersteuning aan de CISO en adviseert de organisatie omtrent risico's met betrekking tot informatiebeveiliging en de te nemen maatregelen.

De SPO heeft geen wettelijke taken op het gebied van privacy, maar is direct betrokken bij de uitvoering van de AVG-verplichtingen en biedt ondersteuning aan de FG. Daarbij fungeert de SPO als (eerste) aanspreekpunt voor privacyvraagstukken die spelen binnen de organisatie. Hierbij kan gedacht worden aan het beoordelen van verwerkingsovereenkomsten (afstemming met interne jurist), het geven van concrete adviezen bij de uitvoer van DPIA 's en het registreren van verwerkingen in het verwerkingsregister.'

De SPO kan bij afwezigheid en/of uitval van de CISO en/of FG een groot deel van de taken overnemen, waardoor de dagelijkse werkzaamheden gewoon gecontinueerd kunnen worden. Verder houdt de SPO zich bezig met:

- Het leveren van een bijdrage aan het bewustwordingscampagnes betreffende security en privacy;
- Het opzetten en uitvoeren van en rapporteren over controles op informatieveiligheid en privacy;
- De ondersteuning van de proceseigenaren bij het handhaven van beveiligingseisen;
- De ondersteuning bij projecten waar security en privacy risico's in kaart moeten worden gebracht;
- Het aannemen en uitwerken van meldingen in het kader van datalekken en de afhandeling daarvan;

- Het mede zorgdragen voor implementatie van nieuwe wet- en regelgeving (BIO2, AI-act) en dit laten landen in een PDCA-cyclus.

4.7 Externe toetsing

De veiligheidsregio's hebben zich in 2022 gecommitteerd aan het Versnellingsplan Informatieveiligheid. Een van de belangrijkste onderdelen van dit Versnellingsplan is dat veiligheidsregio's de richtlijnen en maatregelen van de BIO implementeren. In 2025 is een eerste externe audit uitgevoerd, naar opdracht van het Veiligheidsberaad om te meten hoe de (individuele) veiligheidsregio's er nu voorstaan voor wat betreft het compliant zijn aan de BIO. Verwachting is dat de komende jaren deze externe toetsing een vervolg krijgt en steeds uitgebreider zal worden. Hierdoor zal niet alleen gekeken worden of de maatregelen zijn geïmplementeerd, maar ook of VRG werkt volgens deze maatregelen.

4.8 Jaarplan, -verslag en Roadmap

De CISO en FG zijn verantwoordelijk voor het opstellen van een jaarplan en een jaarverslag. In het jaarverslag wordt een terugblik gegeven over de behaalde resultaten van het voorgaande jaar en de incidenten die er hebben plaatsgevonden. In het jaarplan wordt (kort) aangegeven welke zaken er op de planning staan in het komende jaar. Dit om het Algemeen Bestuur en de directie op hoofdlijnen te informeren.

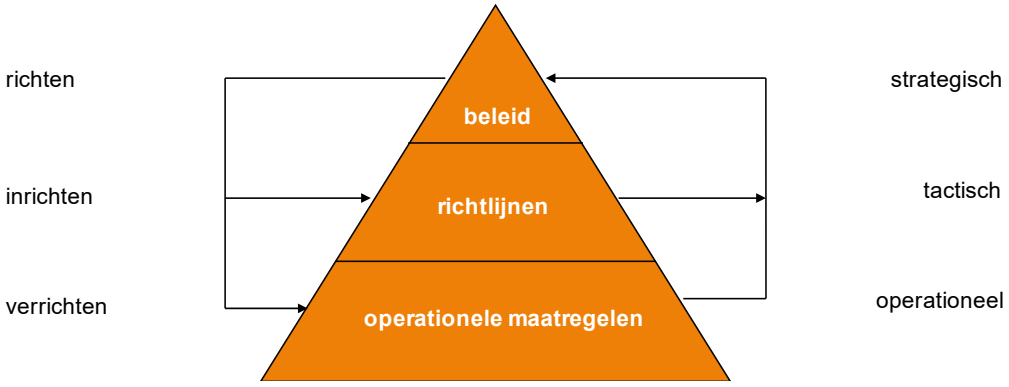
Tevens stelt de CISO een roadmap Informatieveiligheid en Privacy op. Hierin is een meerjarenplanning opgenomen, waarin staat aangeven welk beleid en welke procedures wanneer worden beschreven en geïmplementeerd. Tevens is hier ook de Auditkalender in opgenomen, die een overzicht geeft van wanneer welke systemen en processen aan een audit worden onderworpen. Hierbij wordt rekening gehouden met het belang van het systeem en de processen. Dit belang kan wijzigen door nieuwe ontwikkelingen of (onvoorziene) gebeurtenissen, waardoor de planning in de roadmap zal veranderen. De roadmap is dan ook een document dat continu kan worden gewijzigd en niet voor meerdere jaren vastgesteld wordt.

5 Procesbenadering informatieveiligheid en privacy

In de voorgaande hoofdstukken zijn de doelstellingen, kaders, taken en verantwoordelijkheden, die binnen de veiligheidsregio voor informatieveiligheid en privacy worden gehanteerd en beschreven. Maar hoe worden deze nu in de dagelijkse praktijk tot uitvoering gebracht binnen VRG? In dit hoofdstuk wordt dit concreet gemaakt. Om ervoor te zorgen dat dit beleid ook daadwerkelijk zijn vruchten afwerpt, is ervoor gekozen om te werken met het model van Deming (zie hoofdstuk 5.2), dat zowel rekening houdt met planning en implementatie van maatregelen, maar vervolgens ook met het meten van resultaten en het verbeteren van deze resultaten. Aangezien het een cyclisch model is, wordt hierdoor de informatieveiligheid en privacy binnen VRG stapje voor stapje naar een hoger plan getild.

5.1 Opbouw informatieveiligheid en privacy

Veiligheidsregio Groningen geeft op drie niveaus invulling aan informatieveiligheid en privacy. Het is voor informatieveiligheid en privacy als volgt opgebouwd:

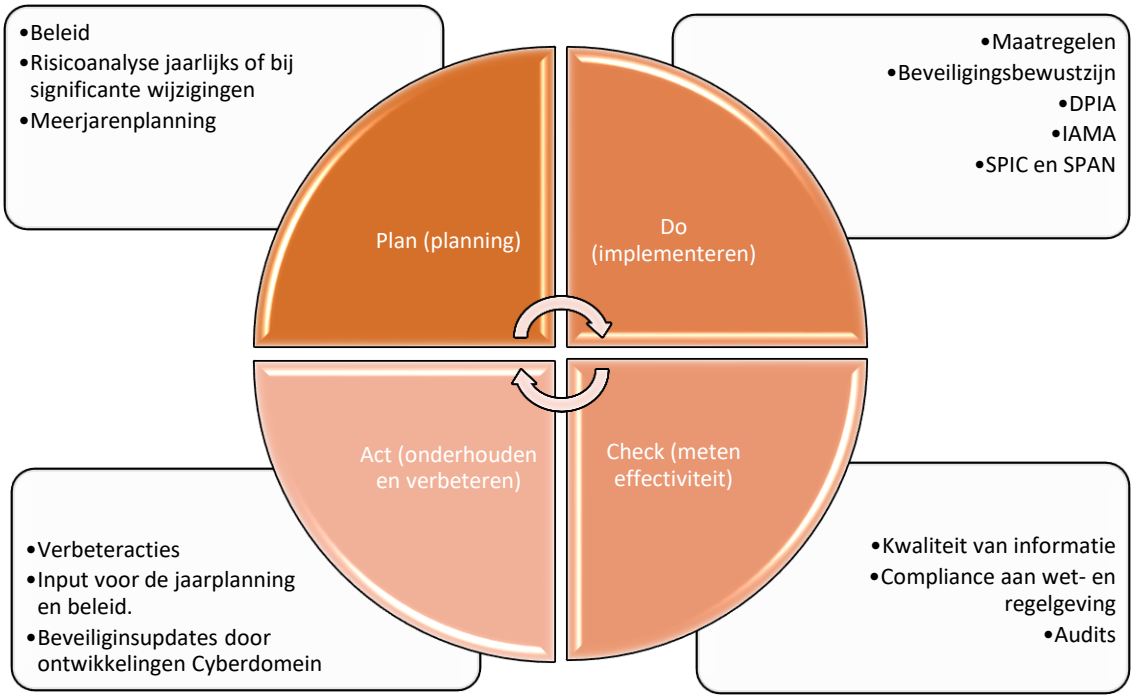


Figuur 2: Opbouw informatieveiligheid en privacy

Afgeleid van de strategische uitgangspunten gedefinieerd in dit beleidsdocument worden richtlijnen opgesteld. De richtlijnen bevatten de tactische uitwerking van de eisen aan informatieveiligheid en privacy binnen de veiligheidsregio. Deze richtlijnen zijn onder andere gebaseerd op de BIO2 waar VRG wettelijk aan moet (gaan) voldoen en aanvullend met richtlijnen gebaseerd op de uitgangspunten zoals deze in dit beleid zijn beschreven. De richtlijnen dienen door de verantwoordelijken te worden vertaald naar operationele maatregelen. De CISO en FG zullen het lijnmanagement hierin gevraagd en ongevraagd ondersteunen en adviseren.

5.2 Procesmodel informatieveiligheid en privacy

Informatieveiligheid en privacybescherming zijn een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatieveiligheid (ISO 27001/2) en sluiten dus volledig aan bij de BIO2. Deze kwaliteitscyclus is in onderstaande figuur 3 weergegeven.



Figuur 3: Kwaliteitscyclus Informatieveiligheid en Privacy

- Plan: De cyclus start met het beleid. Eens per jaar of bij significante wijzigingen (bijvoorbeeld nieuwe wet- en regelgeving, aanschaf nieuwe applicatie etc.) wordt een risicoanalyse uitgevoerd om te toetsen of getroffen operationele maatregelen afdoende zijn of dat aanvullende maatregelen nodig zijn. Dat zorgt dat VRG een goed uitgangspunt heeft om ieder jaar te verbeteren. Risico's worden afgewogen, maar een maatregel moet altijd een doel dienen. Maatregelen worden in een meerjarenplanning gegoten, waarmee de verbetercyclus wordt geborgd. Risicoanalyses kunnen zowel betrekking hebben op de bestaande organisatie als op projecten/business cases.

- Do: Het beleid is de kapstok voor risicomanagement, uitvoering van (technische) maatregelen (bijvoorbeeld het systeem laten afdwingen dat medewerkers alleen kunnen inloggen middels 2 factor authenticatie) en bevordering van beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van de werkprocessen. In bepaalde situaties kunnen veranderingen op de werkvloer minimaal zijn, echter zijn er ook veranderingen die een grote impact kunnen hebben. Ingrijpende veranderingen zullen projectmatig moeten worden geïmplementeerd. Voor de verwerking van persoonsgegevens wordt een zogeheten Data Protection Impact Assessment uitgevoerd. Ook met de nieuwe ontwikkelingen betreffende de toename van het gebruik van algoritmen en AI, dient de zogenaamde Impact Assesment Mensenrechten en Algoritmes (IAMA) in toenemende mate uitgevoerd te worden.

- Check: Het doel van de checkfase is een meting op werking en naleving van het managementsysteem (ISMS) voor beleid en de genomen maatregelen. Dit betekent dat periodiek controles moeten worden uitgevoerd door interne auditoren. Dit kunnen naast de CISO en de FG ook de AO/IC-medewerkers van VRG zijn. Tevens zullen er ook externe audits worden uitgevoerd, door bijvoorbeeld de accountant of een externe Security-audit. Deze resultaten worden in rapportagevorm voorgelegd aan Directie en het MT.

- Act: De resultaten van de checkfase vormen de input om bij te sturen. De cyclus is rond met de uitvoering van verbeteracties voor verschillende richtlijnen, beveiligingsupdates en het beleid. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning en beveiligingsplannen. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd aan het MT.

5.3 Instrumenten Informatieveiligheid en privacy

De cirkel van Deming die voor Informatieveiligheid en privacy wordt gebruikt, wordt ook breder binnen VRG voor andere onderdelen waarbij altijd de volgende stappen gelden: beleid, analyse, plan implementatie, uitvoering, controle en evaluatie. In het kader van Informatieveiligheid en privacy worden hiervoor de volgende instrumenten gebruikt en activiteiten uitgevoerd:

5.3.1 Het Informatieveiligheid & privacybeleid

Het IPB is zoals eerder aangegeven de basis voor de aanpak van informatieveiligheid en privacybescherming binnen de organisatie. In het beleid worden de kaders, randvoorwaarden en uitgangspunten gedefinieerd en in andere documenten, zoals een wachtwoordprocedure, vertaald in concrete maatregelen. Het management speelt een belangrijke rol in het borgen dat het beleid gedragen en uitgevoerd wordt. Het IPB is opgesteld door de CISO met medewerking van de Functionaris Gegevensbescherming van VRG en wordt door het MT goedgekeurd.

5.3.2 BIO2 (wettelijke minimale maatregelen)

De BIO2 beschrijft de minimale maatregelen, die nodig zijn om VRG breed een (verplicht) minimaal niveau van informatieveiligheid en privacybescherming te waarborgen. Als er systemen zijn die na een risicoanalyse hogere eisen nodig hebben, dan worden deze genomen. De maatregelen vanuit de BIO2 plus de eventuele extra maatregelen worden vastgelegd door de CISO in het ISMS.

5.3.3 Risicoanalyses, self assessments en audits

Periodieke evaluatie van informatieveiligheids- en privacyrisico's is noodzakelijk om vast te stellen of de maatregelen nog voldoende bescherming bieden. Bedreigingen zijn in de loop der tijd bijvoorbeeld veranderd, informatiesystemen en/of de organisatie en haar werkwijzen kunnen inmiddels zijn aangepast en maatregelen werken mogelijk anders dan oorspronkelijk bedoeld. De risicoanalyses worden besproken met de systeemeigenaren en/of de proceseigenaren en over maatregelen wordt geadviseerd aan het MT (in sommige gevallen kan rechtstreeks geadviseerd worden aan de directie). Een evaluatie kan overigens ook aanleiding zijn tot het bijstellen van de minimale maatregelen.

5.3.4 Jaarplan/verslag

Elk jaar leveren de CISO en de Functionaris Gegevensbescherming een gezamenlijk jaarverslag en een jaarplan voor het volgende jaar aan bij de directie en het Algemeen Bestuur. Er wordt onder meer ingegaan op incidenten, afwijkingen, resultaten van risicoanalyses incl. genomen maatregelen en andere initiatieven die in het afgelopen jaar hebben plaatsgevonden. Ook wordt hierin vooruitgeblikt op het komende jaar en zullen actiepunten en specifieke aandachtsgebieden worden gedefinieerd. Het verslag wordt ter kennisneming ook gestuurd aan het MT.

5.3.5 (Plan van aanpak) beveiligings- en privacy bewustzijn

Beleid en technische maatregelen alleen zijn niet voldoende om risico's op het terrein van Informatieveiligheid en privacybescherming uit te sluiten. In de praktijk blijkt de mens vaak de zwakste schakel. Daarom verdient bewustwording continue aandacht. Expliciet onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers en vrijwilligers. Deze worden georganiseerd door de CISO, FG en SPO. Hierbij worden ze waar nodig ondersteunt door andere teams binnen VRG zoals bijvoorbeeld Communicatie en P&OO.

5.3.6 Bedrijfscontinuïteitsplan

Business Continuity Management (BCM) is de benaming van het proces dat potentiële bedreigingen voor een organisatie identificeert en bepaalt wat de impact op de "operatie" van de organisatie is als deze bedreigingen daadwerkelijk manifest worden. Het Bedrijfscontinuïteitsplan (BCP) gaat over onverwachte gebeurtenissen ofwel calamiteiten met als gevolg uitval van:

- Medewerkers van/gerelateerd aan VRG;
- Locaties of toegang tot locaties;
- Nutsvoorzieningen inclusief telecom;
- ICT infrastructuur of toegang tot informatie;
- Producten/dienstverlening van leveranciers.

In 2025 is het vernieuwde Bedrijfscontinuïteitsplan voor VRG vastgesteld, om uitval van hiervoor geschetste assets zoveel als mogelijk te voorkomen. Naast een onderbreking van de dienstverlening en eventuele (hoge) herstelkosten, is ook de insteek van het BCP eventuele imagoschade te voorkomen. De CISO en SPO hebben een belangrijke rol in dit plan, want naast het toetsen of de systemen van VRG voldoen aan zaken als betrouwbare back-ups en de mogelijkheden deze snel uit te rollen, moeten medewerkers ook geïnformeerd en geïnstrueerd worden betreffende de security en privacy maatregelen tijdens een eventuele crisis.

5.3.7 Incidentregistratie en respons

Een actuele en betrouwbare registratie van informatieveiligheids- en privacygeralateerde incidenten is een essentiële randvoorwaarde voor een goede inbedding van informatieveiligheid en privacybescherming. De CISO, SPO en de Functionaris

Gegevensbescherming dragen zorg voor het registreren van incidenten, maar ook voor de evaluatie en op basis daarvan een eventuele aanscherping van de baseline. De belangrijkste incidenten worden jaarlijks besproken en geëvalueerd in het jaarverslag.
Tevens zal de CISO bij een beveiligingsincident met de nodige impact de coördinatie op zich nemen om een team samen te stellen en aan te sturen om het incident zo snel mogelijk te mitigeren of op te lossen. Onderdeel van dit team kunnen ook externe leveranciers zijn, denk bijvoorbeeld aan een Security Operations Center (SOC) of een forensisch onderzoeker.

5.3.8 SLA's en verwerkersovereenkomsten

Contractmanagers behoren met de ICT-leverancier en externe leveranciers zogeheten Service Level Agreements af (afgekort: SLA's) af te sluiten. Hierin zijn afspraken en randvoorwaarden over te leveren diensten opgenomen. Een SLA bevat altijd een paragraaf over informatieveiligheid en de verantwoordelijkheden van de leverancier. Ook in geval van clouddienstverlening is de opdrachtnemer (en dus de leverancier) gehouden aan het VRG informatieveiligheid en privacy-beleid en de minimale maatregelen. Tijdens het aanbesteding- en/of inkoopproces draagt de CISO en/of SPO er zorg voor dat altijd de relevante Security en Privacy eisen worden meegenomen. Na de aanschaf zal de CISO en/of SPO ook altijd bij het opstellen (en eventueel herzien) van SLA's toetsen of de geëiste maatregelen ook daadwerkelijk zijn meegenomen. Specifieke afspraken over de verwerking van persoonsgegevens dienen te worden vastgelegd in een verwerkersovereenkomst. Deze verwerkingsovereenkomsten worden geregistreerd in het verwerkingsregister van de VRG.

5.4 Overleg

Om de samenhang in de organisatie van de informatieveiligheid en privacy functie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatieveiligheid en privacy binnen de verschillende onderdelen op elkaar af te stemmen wordt gestructureerd overleg gevoerd over het onderwerp informatieveiligheid en privacy in:

- Een wekelijks terugkerend overleg tussen de CISO, de FG en de SPO;
- Maandelijks tactisch/operationeel overleg tussen CISO en SOC dienstverlener;
- CISO en/of SPO schuiven periodiek aan bij intern overleg van de functionele beheerders van VRG;
- Op strategisch niveau overleg tussen de CISO, FG en de directie;
- 4 keer per jaar overleg met de beveiligingsbeheerders;
- 3 keer per jaar samenwerking- en afstemmingsoverleg in 3Noord;
- CISO heeft 6 keer per jaar strategisch/tactisch overleg in VR-ISAC;
- CISO en SPO hebben 8 keer per jaar tactisch/operationeel overleg in landelijke vakgroep Informatieveiligheid;
- FG en SPO hebben 6 keer per jaar tactisch/operationeel overleg in landelijke vakgroep FG.

Overleg biedt de mogelijkheid om kennis en ervaring binnen de organisatie te delen en te voorkomen dat "het wiel opnieuw wordt uitgevonden". In de genoemde overleggen kunnen o.a. de volgende onderwerpen aan de orde worden gesteld:

- Herziening van het Informatieveiligheid en Privacy beleid en de minimale maatregelen
- Voortgang en doorontwikkeling van het Bedrijfscontinuïteitsplan
- Bespreking van risicoanalyses systemen
- Toezicht op de belangrijkste bedreigingen waaraan de informatie is blootgesteld
- Bespreking van en toezicht op beveiligingsincidenten en datalekken
- Bespreking van initiatieven ter verbetering van de Informatieveiligheid en Privacy
- Coördinatie van de implementatie van nieuwe systemen, diensten, etc.
- Bespreken en mede bepalen koers en richting informatieveiligheid op landelijk niveau.

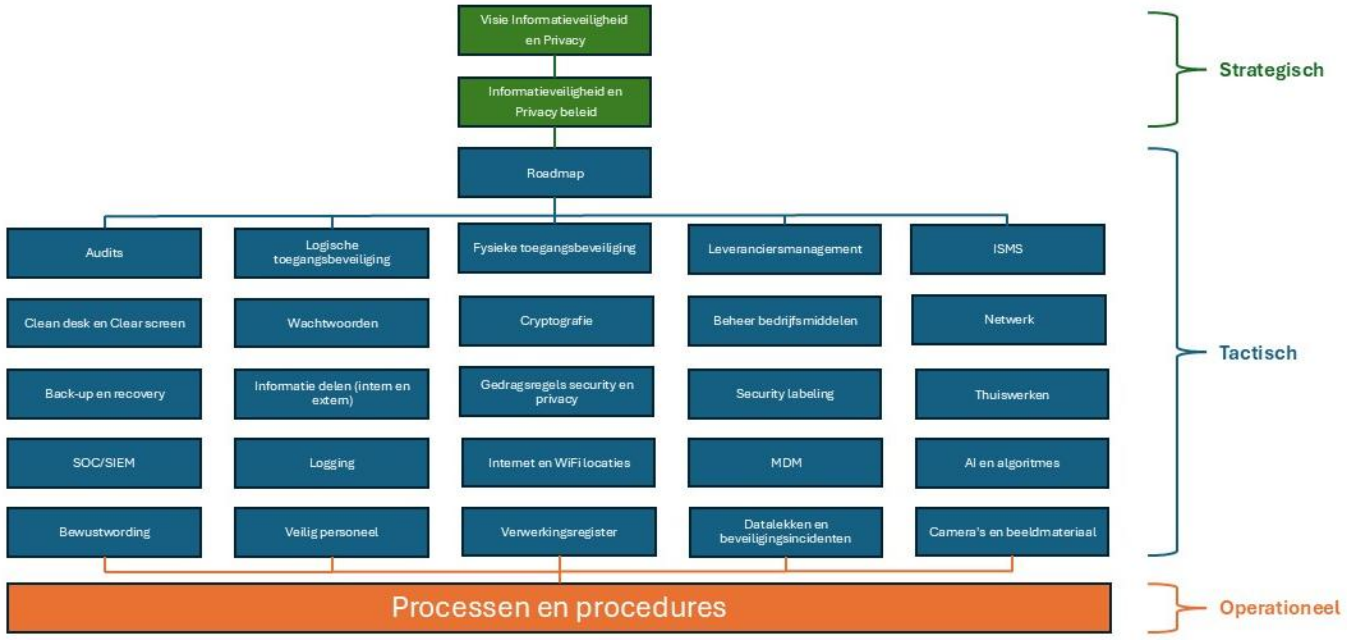
De CISO en FG dragen zorg voor het organiseren van de bovengenoemde interne overleggen.

6 Aan de slag

Met dit IPB is er een kapstok gecreëerd waar diverse procedures betreffende informatieveiligheid en Privacy aan opgehangen kunnen worden. De komende jaren worden de reeds bestaande procedures vernieuwd en aangepast aan huidige stand van de ontwikkelingen en worden nieuwe processen en procedures in de organisatie geïmplementeerd, waarbij telkens de doelstellingen alsook de strategische uitgangspunten van dit IPB worden meegenomen. Het gaat hierbij in ieder geval om de volgende procedures:

- Securitylabeling
- Leveranciersmanagement
- Procedure informatiebeveiligingsincidenten
- Cryptografie
- Fysieke toegangsbeveiliging
- Verwerkingsregister
- Bewustwording
- Beheer van ICT (gerelateerde) bedrijfsmiddelen

In het onderstaande plaatje (figuur 4) staat weergegeven, welke onderdelen allemaal vallen onder Informatiebeveiliging en Privacy en waar het een en ander over vastgelegd/beschreven moet worden. Zo vind je onder meer de hiervoor genoemde procedures terug.



Figuur 4: Kapstok Informatieveiligheid en Privacy

6.1 Financiële middelen

Voor de te nemen maatregelen die voortvloeien uit dit IPB en gezien de importantie en het wettelijk kader, zorgt de sector Bedrijfsvoering voor voldoende middelen, kennis en kunde. Dit is opgenomen in het jaarplan van Team IM/ICT. Dit is nodig voor eventuele externe ondersteuning, materialen nodig voor bewustwording en technische ondersteuning bij zaken als bijvoorbeeld pentesten en phishing mails. Als er door gewijzigde wet- en regelgeving of (grote) ontwikkelingen in de wereld die veel invloed hebben op Informatieveiligheid en Privacy, dan zal een separaat voorstel worden opgesteld, met hierin de aanvraag voor middelen.

6.2 Beleid actualiseren

Dit beleid wordt elke 2 jaar, of zodra zich belangrijke wijzigingen voordoen beoordeeld en zo nodig bijgesteld en opnieuw vastgesteld. Daarbij wordt het IPB, zoals al eerder in hoofdstuk 4 is aangeven, om de vijf jaar volledig herijkt. Over de wijzigingen wordt vervolgens gecommuniceerd naar alle belanghebbenden, waarbij rekening wordt gehouden met eventuele extra werkzaamheden die voortvloeien uit een aanpassing.

7 Bijlagen

7.1 Bijlage 1: Aangestelde Beveiligingsbeheerders

In de onderstaande tabel staan de mederwerkers (functies) die zijn aangesteld als beveiligingsbeheerders. De CISO, de FG en de SPO zijn verantwoordelijk voor het goede functioneren van het team met beveiligingsbeheerder, zorgen voor de agenda en zitten het (periodieke) overleg voor.

omschrijving	medewerker
Beveiligingsbeheerder technisch IM/ICT	Technisch beheerder ICT
Beveiligingsbeheerder applicaties	Functioneel beheerder ICT
Beveiligingsbeheerder fysieke toegang	Vakspecialist Facilitaire Zaken
Beveiligingsbeheerder websites en externe communicatie	Communicatiemedewerker
Beveiligingsbeheerder Veilig personeel & Screening	Medewerker Personeels- en Salarisbeheer
Beveiligingsbeheerder Vakbekwaamheid	Vakspecialist vakbekwaamheid
Beveiligingsbeheerder S&O	Vakspecialist Strategie en Ontwikkeling
Beveiligingsbeheerder T&O / Informatievoorziening (operationeel)	Medewerker Techniek en Ondersteuning
Beveiligingsbeheerder Technische Dienst	Coördinator kleding
Beveiligingsbeheerder Crisisbeheersing en opschaling	Beleidsadviseur Crisisbeheersing
Beveiligingsbeheerder Risicobeheersing	Veiligheidsconsulent