Nota voor : vergadering algemeen bestuur

Datum : 24 maart 2022

Onderwerp : Actieplan BIO AVG 2022-2024

Agendapunt : 9

Kenmerk : AB/2207

Portefeuillehouder: H.J. van Schaik

Bijlage: Actieplan BIO AVG 2022-2024

Inleiding
Het goed en veilig kunnen werken met beschikbare informatie is een voorwaarde voor de taakuitvoering door de VNOG. Informatieveiligheid en -beveiliging zijn hierbij van groot belang. Kwetsbaarheid op dit gebied is in toenemende mate een risicofactor voor overheden, bedrijven en instellingen.
De VNOG heeft zich bestuurlijk en ambtelijk gecommitteerd aan het Versnellingsprogramma Informatieveiligheid van het Veiligheidsberaad. Dit programma voorziet in een versnelde invoering van maatregelen op het gebied van informatieveiligheid aan de hand van de Baseline Informatiebeveiliging Overheid (BIO)[1], die voor de gehele overheid verplicht is. De Baseline Informatiebeveiliging Gemeenten (BIG), die de VNOG sinds 2018 toepast, is opgegaan in de BIO.

Tegelijk met de BIO-maatregelen worden maatregelen op het gebied van de bescherming van persoonsgegevens doorgevoerd. Deze zijn gebaseerd op de Algemene verordening gegevensbescherming (AVG).

Om in een relatief korte periode de voorgenomen maatregelen te kunnen invoeren is een Actieplan BIO AVG 2022-2024 opgesteld. Dit plan geeft inzicht in de maatregelen en de prioritering ervan. Gedurende de uitvoering van het plan en in de periode daarna zijn extra investeringen in middelen en mensuren nodig.

Advies-besluit
1. Het Actieplan BIO AVG 2022-2024 vast te stellen;
2. De benodigde middelen voor de uitvoering van de maatregelen BIO-AVG beschikbaar te stellen:
   a. voor 2022 € 147.000 en voor 2023 € 39.500, en deze bedragen ten laste te brengen van de Bedrijfsvoeringsreserve;
   b. voor 2024 € 7.000 en dit bedrag te verwerken in de begroting 2024.

Beoogd effect
De VNOG voldoet aan de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene verordening gegevensbescherming (AVG) en heeft de daarbij openstaande maatregelen doorgevoerd.

---

[1] https://www.bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf

Argumenten

1.1 De Baseline Informatiebeveiliging Overheid (BIO) en de Algemene verordening gegevensbescherming (AVG) zijn verbindend

Voor het inrichten van de informatieveiligheid en privacy moet de VNOG voldoen aan de eisen van de BIO en van de AVG, de laatste specifiek voor de bescherming van (persoons)gegevens. De BIO, die voor de gehele overheid verplicht is, en de AVG bevatten normen die worden vertaald naar concrete maatregelen op het gebied van informatieveiligheid en -beveiliging.

1.2 De VNOG heeft zich aangesloten bij het Versnellingsprogramma Informatieveiligheid van de gezamenlijke veiligheidsregio's

Om te bereiken dat de veiligheidsregio's voldoen aan de BIO heeft het Veiligheidsberaad een versnellingsprogramma ingesteld, dat de veiligheidsregio's faciliteert in het maken van een inhaalslag op het doorvoeren van maatregelen BIO. Het bestuur van de VNOG volgt het versnellingsprogramma met een daarbij passende invulling voor de VNOG. Omdat veiligheidsregio's in hetzelfde domein werken en in toenemende mate gebruik maken van elkaars informatie en met dezelfde systemen werken is het noodzakelijk dat de individuele regio's zoveel mogelijk aan gelijke standaarden voldoen. Het karakter van het versnellingsprogramma benadrukt deze noodzaak.

1.3 De informatieveiligheid en informatiebeveiliging van de VNOG worden in korte tijd vergroot en versterkt

Het element van 'informatieonveiligheid' vraagt steeds meer aandacht: overheden, bedrijven en particulieren worden in toenemende mate geconfronteerd met nieuwe bedreigingen van de informatieveiligheid. Zo heeft het fenomeen 'gijzelsoftware' in de afgelopen jaren een grote vlucht genomen en is het verworden tot een verdienmodel. Dat maakt organisaties en systemen extra kwetsbaar. De VNOG voldoet per 31 december 2023 aan de BIO/AVG op volwassenheidsniveau 3+ (op een schaal van 5) volgens het BIO-SA volwassenheidsmodel/CIP-PRISA AVG, waarbij de processen zijn geïntegreerd in de organisatie en proactief zijn. Op niveau 1 is sprake van een informele werkwijze, die in stappen verloopt naar niveau 5, waarin de werkwijze organisatiebreed is geoptimaliseerd en cyclisch wordt gemonitord. De VNOG bevindt zich momenteel op volwassenheidsniveau 1.7 (rapport Fox IT, november 2021).

1.4 De maatregelen zijn gecategoriseerd en de verbeteringen van de informatieveiligheid worden gemonitord

De door te voeren maatregelen BIO zijn gerubriceerd naar de vier categorieën Governance, Preventie, Detectie en Response. De 183 maatregelen zijn gegroepeerd naar de indeling van de BIO. Enkele groepen zijn: informatiebeveiligingsbeleid, organiseren van informatiebeveiliging, veilig personeel, toegangs- en fysieke beveiliging en beveiliging bedrijfsvoering.
Voor de 85 maatregelen AVG is aan de hand van de indeling van de AVG een vergelijkbare groepering gemaakt. Enkele groepen zijn: privacybeleid, organieke inbedding, register van gegevensverwerkingen, beveiligen van de verwerking van persoonsgegevens en meldplicht datalekken.
Vervolgens is het mogelijk om te monitoren in welke mate doorgevoerde maatregelen bijdragen aan het verhogen van het volwassenheidsniveau.

1.5 De maatregelen leveren een specifieke bijdrage aan de beveiliging van de informatie

De uit te voeren maatregelen kunnen worden onderscheiden in beleidsmatige maatregelen en het voorzien in concrete maatregelen, die de informatieveiligheid moeten waarborgen:

Beleid
Deze categorie betreft met name het beschikken over privacybeleid en een privacyregeling, informatiebeveiligingsbeleid (uitgangspunten en randvoorwaarden, taken, rollen, verantwoordelijkheden en bevoegdheden van functionarissen), maatregelen ter voorkoming van onbevoegde of ongeautoriseerde toegang tot informatie en -systemen, omgaan met geclassificeerde informatie, wachtwoord- en telewerkbeleid en toegangsbeleid voor gebouwen.

Voorzieningen
Deze categorie is uiteenlopend van karakter en varieert van het inrichten van een tweede datacentrum als uitwijkmogelijkheid, plaatsing van no-breaksystemen (bescherming tegen stroomuitval), verbeteren van antimalware-software, opleidingen, het overleggen van een VOG door medewerkers, het aansluiten bij een klokkenluidersregeling en het informeren en bewustmaken van medewerkers tot het beschikken over benodigde en vereiste licenties.

1.6 De benodigde extra inzet wordt deels binnen bestaande capaciteit gevonden
Voor het realiseren van de maatregelen BIO en AVG zijn aanvullende mensuren nodig. Daarbij is onderscheid gemaakt naar de jaren 2022-2023 en de jaren vanaf 2024. Voor de periode 2022-2023 worden de mensuren incidenteel geput uit de bestaande formatie van de VNOG, met name van de afdeling Bedrijfsvoering, met op de inhoud ondersteuning van de andere afdelingen. Zo zal, naast de inhoudelijke deskundigheid van het team Informatie en van privacy, gebruik gemaakt worden van de capaciteit van de beleidsadviseurs, onder meer voor het onderdeel ‘governance’. Daarnaast is er via interne communicatie aandacht voor het versterken van de bewustwording rond informatieveiligheid en het bieden van handelingsperspectieven voor de medewerkers op dit gebied. Met waar mogelijk prioriteren en temporiseren van overige werkzaamheden wordt voorrang gegeven aan de uitvoering van het Actieplan. Voor de periode vanaf 2024 zal een nieuw actieplan worden opgesteld.

2.1 De invoering van de maatregelen BIO en AVG vraagt om aanvullende middelen
Voor het realiseren van de BIO- en AVG-maatregelen zijn aanvullende financiële middelen nodig voor zowel de jaren 2022-2023 als voor de periode daarna:

- voor 2022 betreft het € 147.000 en voor 2023 € 39.500. Voorgesteld wordt deze bedragen ten laste te brengen van de Bedrijfsvoeringreserve;
- de kosten vanaf 2024 betreffen € 7.000. Voorgesteld wordt deze te verwerken in de begroting 2024.

Kanttekeningen
1.1 Het totaal aantal maatregelen maakt een prioritering noodzakelijk
De omvang van het aantal maatregelen, 268, vraagt om een prioritering bij de uitvoering. De gradaties in prioritering zijn als volgt:

1	Hoog	(levert een direct risico op)
2	Midden	(dringend, geen direct risico)
3	Laag	(noodzakelijk, niet dringend)
4	Best Effort	(niet noodzakelijk, wel wenselijk).

Daarbij is ook gekeken naar de mate waarin de maatregel bijdraagt aan het behalen van het volwassenheidsniveau 3+, in relatie tot de inspanning in financiën en mensuren die hiermee is gemoeid. Bij de uitvoering van de maatregelen wordt begonnen met de prio 1-maatregelen.
Uit het geheel van maatregelen zijn er inmiddels twaalf geselecteerd, die binnen bestaande middelen en bevoegdheden en al beschikbare mensuren kunnen worden gerealiseerd. Met de uitvoering van deze maatregelen is onlangs een start gemaakt.

1.2 De planningshorizon is beperkt
Het overzicht met maatregelen en de wijze waarop deze kunnen worden doorgevoerd is gebaseerd op de huidige inzichten rond informatiebeveiliging en naar de huidige stand van de techniek.
Met het oog hierop wordt een scope van twee jaar gehanteerd voor het doorvoeren van de geplande maatregelen, mede ook vanwege het moeilijk voorspelbare karakter van informatie(on)veiligheid.
Voor 2024 en verder wordt u te zijner tijd een nieuw actieplan voorgelegd, waaraan eveneens een uitvoeringsplanning ten grondslag zal liggen.

1.3 Landelijk is afgesproken om te streven naar een volwassenheidsniveau 4
De VNOG verkeert momenteel op volwassenheidsniveau 1.7. De stap van hieruit naar volwassenheidsniveau 4 zou een onevenredige inzet van (extra) middelen (financieel en mensuren) vragen. Daarnaast hebben de maatregelen op de niveaus 4 en 5 veelal een cyclisch karakter. Dat veronderstelt dat er al veel maatregelen zijn doorgevoerd, die met een cyclische aanpak versterkt kunnen worden. Evenals meerdere andere veiligheidsregio's is de VNOG nog niet in dit stadium. Inmiddels is dit probleem ook landelijk onder de aandacht gebracht.

Uitvoering/ communicatie/ inwerkingtreding
Het dagelijks bestuur wordt per kwartaal geïnformeerd over de stand van de uitvoering van het Actieplan. Majeure afwijkingen worden zo spoedig mogelijk gecommuniceerd met de portefeuillehouder Informatie in het dagelijks bestuur en zo nodig met het dagelijks bestuur. Het algemeen bestuur wordt jaarlijks in de P&C-cyclus over de voortgang geïnformeerd.

De medewerkers van de VNOG worden, in overleg met het team Communicatie, op gezette tijden geïnformeerd over de voortgang, onder meer via Mijn VNOG.

Personele consequenties
Geen.

Financiële consequenties
De kosten BIO-AVG 2022 (€ 147.000) en 2023 (€ 39.500): ten laste van de Bedrijfsvoeringsreserve.
De kosten BIO-AVG 2024 ev. (€ 7.000): verwerken in de begroting 2024.

Het algemeen bestuur van de Veiligheidsregio Noord- en Oost-Gelderland;

Bijeen in de vergadering d.d. 24 maart 2022;

Gelezen het voorstel van het dagelijks bestuur d.d. 10 maart 2022;

Besluit:

1. Het Actieplan BIO AVG 2022-2024 vast te stellen;
2. De benodigde middelen voor de uitvoering van de maatregelen BIO-AVG beschikbaar te stellen:
   a. voor 2022 € 147.000 en voor 2023 € 39.500, en deze bedragen ten laste te brengen van de Bedrijfsvoeringsreserve;
   b. voor 2024 € 7.000 en dit bedrag te verwerken in de begroting 2024.

De secretaris | De voorzitter

drs. D.G.L. Kransen | A.J.M. Heerts

Apeldoorn, 24 maart 2022

Actieplan BIO AVG

2022 – 2024

Veiligheidsregio Noord- en Oost-Gelderland

Datum: 17 januari 2022
Versie: 1.0
Auteur: Hans Veldkamp / André Renkens
Organisatieonderdeel: Bedrijfsvoering

Inhoudsopgave

Inleiding 3
Informatiebeveiliging 3
De uitgangspunten 3
De maatregelen BIO en AVG 5
Hoe ziet dat er dan uit? 6
Prioritering van de maatregelen 7
Vertaling van de maatregelen naar financiën en mensuren 8
De besluitvorming 9
Voortgangsrapportage 9
Communicatie 9
Het vervolg 10

Inleiding

Het dagelijks bestuur van de VNOG heeft de ambitie uitgesproken om als VNOG versneld de Baseline Informatiebeveiliging Overheid (BIO) geheel in te voeren. De veiligheidsregio's in Nederland, verenigd in het Veiligheidsberaad, hebben op dit punt nadere afspraken gemaakt en een Versnellingsprogramma uitgerold. In het kader van deze operatie is eveneens gekeken naar het invoeren van maatregelen die nodig zijn om als VNOG ook (geheel) aan de Algemene verordening gegevensbescherming (AVG) te voldoen. Beide onderwerpen worden tegelijk opgepakt.

Het bestuur van de VNOG heeft in 2018 de BIG (Baseline Informatiebeveiliging Gemeenten), een van de voorlopers van de BIO, als uitgangspunt genomen voor de vormgeving van de informatiebeveiligingsbeleid. De invoering van de BIO is een logisch vervolg hierop.

Voor de invoering van de benodigde maatregelen hebben de Functionaris Gegevensbescherming (FG) en de Chief Information Security Officer (CISO) een Actieplan opgesteld. Aan de hand van de BIO en de AVG is inzichtelijk gemaakt welke maatregelen uit beide regelingen in de VNOG-organisatie moeten worden doorgevoerd en wat de VNOG daarvoor moet doen. Hieraan gekoppeld zijn de uitkomsten in de vorm van aanbevelingen uit de door Fox IT uitgevoerde Cyber Security Scan naar aanleiding van de hack met gijzelsoftware die de VNOG in september 2020 trof. Deze aanbevelingen betreffen de verdere invoering van de BIO.

De door te voeren maatregelen zijn vertaald naar hiervoor benodigde investeringen in geld en mensuren. De omvang van het aantal maatregelen vraagt om een prioritering op basis van realiseerbaarheid en effectiviteit. Daarin voorziet het Actieplan.

Informatiebeveiliging

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit en het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen. De BIO beoogt zo de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel is continuïteit in de bedrijfsprocessen door waarborgen van juiste en tijdige informatie. De BIO is verplicht van toepassing op de gehele overheid.

De uitgangspunten

De uitvoering van het Actieplan BIO AVG is gebaseerd op de volgende uitgangspunten:

- De VNOG hanteert de Baseline Informatiebeveiliging Overheid (BIO) voor het inrichten van de informatieveiligheid en voldoet aan de eisen van de BIO. Dit betreft een herbevestiging van het standpunt inzake informatiebeveiliging uit 2018;
- De VNOG voldoet aan de eisen die de Algemene verordening gegevensbescherming stelt aan de bescherming van (persoons)gegevens;

- De VNOG volgt het Versnellingsprogramma Informatieveiligheid van het Veiligheidsberaad, waaraan het dagelijks bestuur van de VNOG zich heeft gecommitteerd, waarbij de VNOG per 1 januari 2023 aan de minimale voorwaarden van de BIO en de AVG voldoet;
- De VNOG voldoet per 31 december 2023 aan de BIO/AVG op volwassenheidsniveau 3+ (op een schaal van 5[1]) volgens het BIO-SA volwassenheidsmodel/CIP-PRISA AVG, waarbij de processen zijn geïntegreerd in de organisatie en proactief zijn.

De vijf niveaus van volwassenheid volgens het landelijk gehanteerde BIO-SA (CIP-CMM-)model[2] zijn[3]:

Niveau 1	Informeel	de werkzaamheden worden op verwerkingsniveau informeel uitgevoerd
Niveau 2	Beheerst	de werkzaamheden vinden in herhaalbare en binnen een afdeling beheerste processen plaats
Niveau 3	Vastgesteld	de werkzaamheden vinden plaats in herhaalbare en beheerste processen, die zijn gebaseerd op een bedrijfsbreed vastgestelde werkwijze
Niveau 4	Voorspelbaar	de werkzaamheden vinden plaats terwijl de prestaties van de processen wordt gemeten door het verzamelen van gedetailleerde gegevens over de processen en hun kwaliteit
Niveau 5	Geoptimaliseerd	de werkzaamheden vinden plaats terwijl de prestaties van de organisatie wordt gemeten door het verzamelen van gedetailleerde gegevens over de processen en hun kwaliteit.

Informatieveiligheid en-beveiliging is dynamisch en vraagt voortdurend flexibiliteit om in te kunnen spelen op nieuwe ontwikkelingen. Enerzijds gaat het hierbij om technologische ontwikkelingen met nieuwe mogelijkheden voor informatieveiligheid en het versterken ervan.
Anderzijds vraagt het element van 'informatieonveiligheid' steeds meer aandacht: overheden, bedrijven en particulieren worden in toenemende mate geconfronteerd met nieuwe bedreigingen van de informatieveiligheid. Zo heeft het fenomeen 'gijzelsoftware' in de afgelopen jaren een grote vlucht genomen en is het verworden tot een verdienmodel. Dat maakt organisaties en systemen extra kwetsbaar.
Dat betekent ook dat er altijd ruimte moet zijn om te kunnen inspelen op nieuwe ontwikkelingen en bedreigingen. Een gedetailleerd informatieveiligheidsbeleid zal dan ook niet altijd een antwoord geven op de uitdagingen die voorliggen.

Het overzicht met maatregelen en de wijze waarop deze kunnen worden doorgevoerd is gebaseerd op de huidige inzichten rond informatiebeveiliging en naar de huidige stand van de techniek.
Met het oog hierop wordt een scope van twee jaar gehanteerd voor het doorvoeren van de geplande maatregelen, mede ook vanwege het moeilijk voorspelbare karakter van informatie(on)veiligheid.

---

[1] De VNOG bevindt zich op dit moment op niveau 1.7 (rapport Fox IT, november 2021).
[2] BIO-SA staat voor BIO Self Assessment. CIP staat voor Centrum Informatiebeveiliging en Privacybescherming. CMM staat voor Capability Maturity Model, een model dat is ontwikkeld voor het beoordelen van IT-ontwikkeling.
[3] Fox IT hanteert andere benamingen voor de volwassenheidsniveaus. Deze zijn eveneens gebaseerd op het CMM-model en daarmee vergelijkbaar.

Landelijk is afgesproken te streven naar een volwassenheidsniveau 4. De VNOG verkeert momenteel op niveau 1.7. De stap van hieruit naar niveau 4 is te groot om in een keer te maken, mede omdat dit een onevenredige inzet van extra middelen (€ en mensuren) vraagt. Het Assessment van FOX-IT onderschrijft dit. Voor de VNOG is het derhalve niet redelijk deze stap nu te willen of kunnen zetten. Daarnaast hebben de maatregelen op de niveaus 4 en 5 veelal een cyclisch karakter. Dat veronderstelt dat er al veel maatregelen zijn doorgevoerd, die met een cyclische aanpak versterkt kunnen worden. Evenals meerdere andere veiligheidsregio's is de VNOG nog niet in dit stadium. Inmiddels is dit probleem ook landelijk onder de aandacht gebracht.

De maatregelen BIO en AVG

Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. In de BIO zijn op basis van de generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus (BBN's) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. In de BIO staat per BBN beschreven aan welke controls uit de Code voor Informatiebeveiliging (ISO 27002) moet worden voldaan. Bij alle controls dient, op basis van een individuele risicoafweging, bepaald te worden hoe aan de beveiligingsdoelstelling van de control voldaan kan worden. Hiermee is risicobeheersing, in tegenstelling tot eerdere baselines, het uitgangspunt voor de BIO en de basis voor de systematiek.

Daarbij zijn de controls, waar van toepassing, gedeeltelijk uitgewerkt in verplichte, concrete overheidsmaatregelen. De maatregelen zijn toebedeeld aan rollen, waarmee de verdeling over verantwoordelijken makkelijker is. Ten slotte moet verantwoording worden afgelegd over de risicoafweging en over de effectieve invulling van de maatregelen. Deze verantwoording is onderdeel van de bestuurlijke verantwoording over de beveiliging van informatiesystemen.

De BIO

Aan de hand van de BIO en de daarin opgenomen controls is een overzicht gemaakt van de maatregelen die door de VNOG moeten worden doorgevoerd en de werkzaakheden die daarvoor moeten worden uitgevoerd.

De maatregelen zijn gegroepeerd naar de indeling van de BIO als volgt[4]:

5. Informatiebeveiligingsbeleid; 6. Organiseren van informatiebeveiliging; 7. Veilig personeel; 8. Beheer van bedrijfsmiddelen; 9. Toegangsbeveiliging; 10, Cryptografie; 11. Fysieke beveiliging en beveiliging van de omgeving; 12. Beveiliging bedrijfsvoering; 13. Communicatiebeveiliging; 14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen; 15. Leveranciersrelaties; 16. Beheer van informatiebeveiligingsincidenten; 17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer; 18. Naleving.

[4] De groepering van de maatregelen volgt de indeling van de BIO. De eerste vier hoofdstukken van de BIO zijn inleidend en bevatten geen maatregelen.

De AVG

Voor de verdere invoering van de AVG is een vergelijkbaar overzicht gemaakt van door te voeren maatregelen. Deze komen voort uit een selfassessment CIP[5]-AVG, dat de VNOG heeft uitgevoerd. De maatregelen zijn als volgt gegroepeerd: 1. Privacybeleid; 2. Organieke inbedding; 3. Risicomanagement, Privacy by design en DPIA; 4. Doelbinding gegevensverwerking; 5. Register van gegevensverwerkingen; 6. Kwaliteitsmanagement; 7. Beveiligen van de verwerking van persoonsgegevens; 8. Informatieverstrekking aan betrokkenen bij verzameling persoonsgegevens; 9. Bewaren van persoonsgegevens; 10. Doorgifte van persoonsgegevens; 11. Intern toezicht; 12. Toegang gegevensverwerking voor betrokkenen; 13. Meldplicht datalekken.

De door te voeren maatregelen voor de BIO zijn vervolgens gerubriceerd naar de door Fox IT gehanteerde categorieën Governance, Preventie, Detectie en Responce.

Hoe ziet dat er dan uit?

BIO maatregelen per categorie en per prioriteit

Prioritering	Governance	Preventie	Detectie	Response
1	7	36	10	9
2	21	28	4	7
3	5	7	0	3
4	0	40	2	4
Totaal	33	111	16	23

Voor de BIO dienen in totaal 183 maatregelen te worden doorgevoerd. Bij de uitvoering wordt voorrang gegeven aan de met prioriteit 1 aangemerkte maatregelen.

[5] Het Centrum Informatiebeveiliging en Privacybescherming (CIP) is een publiek-private netwerkorganisatie die bestaat uit Participanten en Kennispartners. Participanten zijn overheidsbedrijven waarvan medewerkers meedoen aan een of meer van de werkverbanden in het netwerk. Kennispartners zijn marktpartijen die met een convenant verbonden zijn en een hoeveelheid uren hebben toegezegd in de samenwerking. De VNOG is een van de participanten in het CIP.

AVG maatregelen per prioriteit

Prioritering	AVG
1	30
2	18
3	37
4	0
Totaal	85

Voor de AVG dienen in totaal 85 maatregelen te worden doorgevoerd. Bij de uitvoering wordt voorrang gegeven aan de met prioriteit 1 aangemerkte maatregelen. Binnen het deel AVG is niet het onderscheid in categorieën als bij de BIO gemaakt.

De uit te voeren maatregelen kunnen worden onderscheiden in beleidsmatige maatregelen en het voorzien in concrete maatregelen, die de informatieveiligheid moeten waarborgen:

Beleid
Deze categorie betreft met name het beschikken over privacybeleid en een privacyregeling, informatiebeveiligingsbeleid (uitgangspunten en randvoorwaarden, taken, rollen, verantwoordelijkheden en bevoegdheden van functionarissen), maatregelen ter voorkoming van onbevoegde of ongeautoriseerde toegang tot informatie en -systemen, omgaan met geclassificeerde informatie, wachtwoord- en telewerkbeleid en toegangsbeleid voor gebouwen.

Voorzieningen
Deze categorie is uiteenlopend van karakter en varieert van het inrichten van een tweede datacentrum als uitwijkmogelijkheid, plaatsing van no-breaksystemen (bescherming tegen stroomuitval), verbeteren van antimalwaresoftware, opleidingen, het overleggen van een VOG door medewerkers, het aansluiten bij een klokkenluidersregeling en het informeren en bewustmaken van medewerkers tot het beschikken over benodigde en vereiste licenties.

Prioritering van de maatregelen

De inventarisatie van de uit te voeren maatregelen leidt tot 268 door te voeren maatregelen voor BIO en AVG samen, waarvan een belangrijk deel vanwege de uitgesproken ambitie in 2022 gerealiseerd moet worden. Een dergelijke inspanning noodzaakt tot prioritering en fasering. De geïnventariseerde maatregelen zijn voorzien van een prioriteit, van 1 tot 4.

De gradaties in prioritering zijn als volgt:

1	Hoog	(levert een direct risico op)
2	Midden	(dringend, geen direct risico)
3	Laag	(noodzakelijk, niet dringend)
4	Best Effort	(niet noodzakelijk, wel wenselijk).

Daarnaast is gekeken naar de mate waarin de maatregel bijdraagt aan het behalen van het volwassenheidsniveau 3+, in relatie tot de inspanning in financiën en mensuren die hiermee is gemoeid.

Top 12 van maatregelen

Uit het geheel van maatregelen zijn er twaalf geselecteerd, die binnen bestaande bevoegdheden en middelen en met inzet van al beschikbare mensuren kunnen worden gerealiseerd. Deze maatregelen hebben met name betrekking op het updaten en versterken van de beleids- en planmatige aspecten van informatiebeveiliging. Met de uitvoering van deze maatregelen is inmiddels een start gemaakt.

Daarbinnen worden ook enkele concrete maatregelen uitgevoerd, zoals het met voorrang aanvragen van een VOG voor medewerkers[6] die werkzaam zijn op het terrein van informatieveiligheid (privacy, ICT, functioneel beheer).

Nadere prioritering

De overige maatregelen worden volgens prioritering 1 tot en met 4 uitgevoerd in de jaren 2022, 2023 en 2024. Als eerste worden de maatregelen met prio 1 uitgevoerd. Deze hebben met name betrekking op de BIO en passen bij het streven om de VNOG per 1 januari 2023 te laten voldoen aan de eisen van volwassenheidsniveau 3.

Vertaling van de maatregelen naar financiën en mensuren

Om de maatregelen uit het Actieplan te kunnen realiseren is zijn aanvullende middelen in geld en in tijd nodig. Daarvoor is een raming gemaakt van financiële middelen en mensuren. Een deel van de middelen is al beschikbaar binnen de bestaande begroting en binnen de bestaande formatie. Dit betreft met name formatie voor informatieveiligheid (de Functionaris gegevensbescherming, FG), de Chief Information Security Officer (CISO) en functioneel beheer van de systemen). Om de inhaalslag verder mogelijk te maken zijn voor de BIO-AVG-maatregelen in de Kadernota al bedragen opgenomen. Daarnaast vraagt de invoering van BIO en AVG aanvullende financiële middelen. Daarbij wordt onderscheid gemaakt tussen de jaren 2022, 2023 en 2024 en volgende.

[6] Op basis van de BIO is het wenselijk van iedere medewerker vijfjaarlijks een Verklaring omtrent het Gedrag (VOG) te vragen.

De benodigde bedragen voor de maatregelen BIO en AVG zijn opgenomen in de onderstaande tabel.

Groep	Exploitatie 2022	Exploitatie 2023	Exploitatie 2024 ev
M01	€ 161.500	€ 172.500	€ 160.000
M02	€ 23.750	€ 23.750	€ 23.750
M03	€ 0	€ 0	€ 0
M04	€ 0	€ 0	€ 0
M05	€ 0	€ 0	€ 0
M06	€ 1.750	€ 1.750	€ 1.750
M07	€ 0	€ 30.000	€ 0
M08	€ 77.000	€ 77.000	€ 77.000
Prio1 overig	€ 0	€ 19.000	€ 29.000
AVG	€ 5.000	€ 4.000	€ 4.000
TOTAAL BIO-AVG	**€ 269.000**	**€ 328.000**	**€ 295.500**
minus totaal kadernota	*€ 100.000*	*€ 269.000*	*€ 269.000*
minus totaal uit begroting	€ 22.000	€ 19.500	€ 19.500
TOTAAL NOG TE BEGROTEN	**€ 147.000**	**€ 39.500**	**€ 7.000**

De raming van de mensuren voor de uitvoering van de BIO- en AVG-maatregelen is als volgt:

Mensuren BIO		Mensuren AVG	
2022-2023	2024 ev	2022-2023	2024 ev
1.244	468	638	548

De besluitvorming

Bij de besluitvorming over het Actieplan BIO AVG 2022-2024 ev. en de uitvoering ervan zijn het algemeen en het dagelijks bestuur betrokken, evenals het managementteam.

Voortgangsrapportage

Het Actieplan BIO AVG 2022-2024 vraagt om een dynamische uitvoering en kan gedurende de uitvoering waar nodig worden aangepast. Het dagelijks bestuur wordt per kwartaal geïnformeerd over de stand van de uitvoering van het Actieplan. Majeure afwijkingen worden zo spoedig mogelijk gecommuniceerd met de portefeuillehouder Informatie in het dagelijks bestuur en zo nodig met het dagelijks bestuur. Het algemeen bestuur wordt jaarlijks in de P&C-cyclus over de voortgang geïnformeerd.

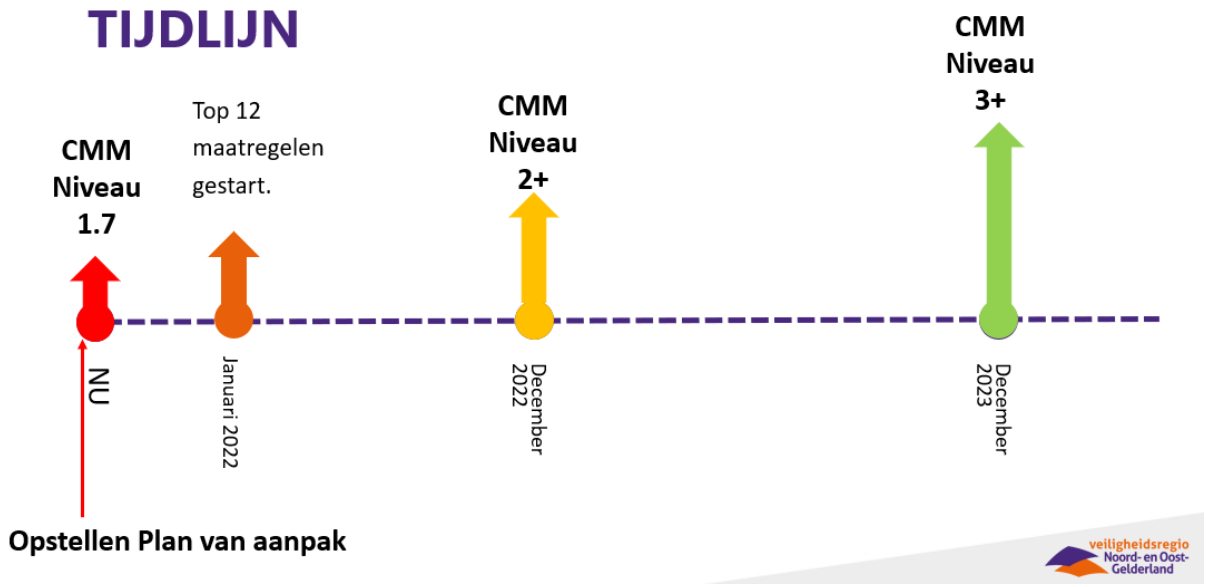
Communicatie

Naast de formele rapportages aan het bestuur en het managementteam worden in overleg met het team Communicatie op gezette tijden ook de medewerkers geïnformeerd over de voortgang, ondermeer via Mijn VNOG.

Het vervolg

Het realiseren van de benoemde maatregelen zal resulteren in nadere producten, in de vorm van beleidsvoorstellen, regelingen en concrete maatregelen en voorzieningen. Per maatregel wordt nagegaan of separate vaststelling door het algemeen dan wel het dagelijks bestuur nodig is. Daarbij wordt eveneens nagegaan op welke wijze de medezeggenschap in de vorm van de Ondernemingsraad betrokken dient te worden. Er kan immers sprake zijn van het vaststellen van een regeling op het gebied van privacybescherming en het verwerken of beschermen van persoonsgegevens van de medewerkers van de VNOG[7].

In de tijd ziet de uitvoering van het Actieplan er als volgt uit, waarbij het streven is om niveau 3 al in januari 2023 te halen:



[7] Zie Wet op de Ondernemingsraden artikel 27, eerste lid, sub k: een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen.