IV experts

Een veilige informatievoorziening: waar begin je?

Een praktische blik op de implementatie van BIO, NIS2 en AVG

IV experts

Augustus 2025

Voorwoord

'De informatievoorziening op orde'... is niet eenvoudig. Er zijn veel dingen om rekening mee te houden, zoals visie, sturing, organisatiestructuur, mensen en kennis. Grip hebben op informatie betekent goed organiseren. Organiseren betekent keuzes maken, prioriteiten stellen en plannen maken.

In deze whitepaper leggen we uit wat de belangrijkste regels zijn voor informatieveiligheid en privacy. We kijken naar de samenhang tussen deze regels en geven praktische tips voor prioriteiten en plannen in de praktijk.

Inleiding

Overheidsorganisaties moeten steeds vaker rekening houden met regels over informatiebeveiliging en privacy. Drie belangrijke regels zijn de Baseline Informatiebeveiliging Overheid (BIO), de Netwerk- en Informatiebeveiligingsrichtlijn 2 (NIS2) en de Algemene Verordening Gegevensbescherming (AVG).

Deze regels geven aan hoe een organisatie informatie moet beschermen en persoonsgegevens veilig moet houden. Ze hebben invloed op verschillende lagen in een organisatie: van het dagelijks werk (operationeel), het beleid en de manier van werken (tactisch), tot de strategie en visie van de organisatie (strategisch).

Het niet volgen van deze regels kan grote gevolgen hebben, zoals boetes of verlies van vertrouwen van burgers. Daarom is het belangrijk dat organisaties hier actief mee aan de slag gaan. In deze whitepaper kijken we verder naar deze regels en hun betekenis.

BIO, NIS2 en AVG: wat en wanneer

BIO

De BIO is sinds 2019 het afgesproken normenkader voor informatiebeveiliging binnen alle Nederlandse overheidsorganisatie. De BIO is geen wet, maar overheidsorganisaties moeten deze wel gebruiken. Zij zijn namelijk wettelijk verplicht om de vertrouwelijkheid, juistheid en beschikbaarheid van informatie te beschermen.

De BIO is gebaseerd op internationale normen zoals ISO 27001 en ISO 27002. Gemeenten, provincies en het Rijk hebben de BIO officieel vastgesteld via afspraken en regels. Wie de BIO niet volgt krijgt meestal geen directe boete, maar bij incidenten of controles kan dit wel problemen opleveren.

De BIO helpt organisaties om risico's in kaart te brengen, processen goed te regelen en regelmatig te controleren of de informatiebeveiliging op orde is. Het doel is altijd om de gegevens van de burgers en van de overheid te beschermen.

NIS2

De NIS2-richtlijn is een Europese regel die vanaf 17 oktober 2024 geldt. Organisaties in belangrijke sectoren, zoals energie, vervoer en overheid, moeten hierdoor beter beschermd zijn tegen digitale aanvallen. Ze moeten bijvoorbeeld risico's onderzoeken, noodplannen maken en ernstige incidenten binnen 24 melden.

Alle Europese landen moeten de NIS2-richtijn in hun eigen wet opnemen. Nederland heeft dit nog niet op tijd gedaan. De verwachting is nu dat dit via de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten in het derde kwartaal van 2025 gebeurt.

De NIS2-richtlijn legt een zorgplicht op voor informatieveiligheid. Dit sluit goed aan bij de bestaande regels van de BIO. Het ministerie van Binnenlandse Zaken wil de BIO ook wettelijk vastleggen om aan deze zorgplicht te voldoen.

AVG

De AVG geldt sinds 2018 en regelt hoe organisaties met persoonsgegevens moeten omgaan. Organisaties moeten bijvoorbeeld:

- Duidelijk maken wat ze met persoonsgegevens doen
- Zo min mogelijk gegevens verzamelen
- Mensen het recht geven om hun gegevens te bekijken of te laten verwijderen

Ook moeten organisaties kunnen laten zien dat ze zich aan deze regels houden en datalekken voorkomen. Waar de BIO en NIS2 vooral gaan over de technische en organisatorische beveiliging van informatie, gaat de AVG over de rechten van mensen en het correct gebruiken van hun gegevens.

Een belangrijk onderdeel van de AVG is de verantwoordingsplicht. Organisaties moeten laten zien dat ze de regels volgen. Dit doen ze bijvoorbeeld door:

- Een register bij te houden van gegevenswerkingen
- Risicoanalyses te maken bij gevoelige verwerkingen (DPIA's)
- Datalekken binnen 72 uur te melden

Overheidsorganisaties moeten ook een functionaris voor gegevensbescherming (FG) aanstellen. Kleine en middelgrote bedrijven hoeven dat meestal niet.

De AVG versterkt de BIO en NIS2. Door de extra juridische laag zijn organisaties verplicht hun systemen goed te beveiligen, maar ook zorgvuldig en transparant om te gaan met de gegevens die ze verwerken. Samen vormen deze drie kaders een compleet raamwerk voor informatieveiligheid en privacy.

Eén gezamenlijke aanpak voor veiligheid en privacy

De BIO, NIS2 en AVG leggen ieder andere accenten, maar hebben ook veel gemeen. Ze hebben allemaal hetzelfde doel: gevoelige informatie beschermen en risico's beperken.

- **BIO** gaat over hoe de overheid informatiebeveiliging moet organiseren.
- **NIS2** kijkt breder en gaat over de digitale weerbaarheid in de hele Europese Unie.
- **AVG** richt zich op het beschermen van persoonsgegevens van burgers.

Voor overheidsorganisaties is het slim om deze regels niet apart te behandelen. Beter is om één gezamenlijke aanpak te maken.

Een gezamenlijke aanpak betekent dat BIO, NIS2 en AVG als één geheel worden toegepast. Processen, technologie en afspraken sluiten dan goed op elkaar aan. Dit kan betekenen dat er bijvoorbeeld één overkoepelend beleid wordt opgesteld, waarin zowel informatiebeveiliging als privacybescherming staan. Dit beleid wordt daarna uitgewerkt in praktische stappen, zoals risicoanalyses, plannen voor incidenten en het continue monitoren van IT-systemen.

Daarnaast is het belangrijk dat er duidelijke rollen en verantwoordelijkheden worden vastgesteld. Zo kan een security officer samenwerken met een privacy officer. Dat is niet ondenkbaar in een governance structuur met de CISO en de Functionaris Gegevensbescherming (FG).

Door deze wet- en regelgeving te verbinden binnen één breed informatiebeleid, kunnen organisaties efficiënter voldoen aan de eisen, dubbel werk voorkomen en een sterke, duidelijke beveiligingsstrategie opzetten. Dat vergroot niet alleen de naleving van de regels, maar versterkt ook de bescherming tegen digitale dreigingen en datalekken.

Belangrijkste knelpunten bij het uitvoeren van wet- en regelgeving

Veel organisaties vinden het lastig om met al deze regels tegelijk te werken. Soms overlappen de regels, maar soms vullen ze elkaar ook aan. Daarom is het belangrijk om duidelijk in kaart te brengen wat nodig is en hoe dit het beste georganiseerd kan worden. Het maken van een overzicht van verplichtingen en het kiezen van een aanpak die alles samenbrengt, helpt hierbij. Denk hierbij aan het uitvoeren van GAP-analyses, risicoanalyses en het opzetten van een gecombineerd ISMS en PMS.

Daarnaast is er vaak te weinig tijd en geld. Niet alles kan tegelijk. Een oplossing is om te beginnen met de grootste risico's en eerst de belangrijkste maatregelen uit te voeren. Zo kan een organisatie stap voor stap werken aan betere informatiebeveiliging.

Ook verandert het dreigingsbeeld voortdurend. Hackers worden slimmer en de risico's veranderen snel. Daarom is het belangrijk dat organisaties niet alleen regels volgen, maar ook flexibel blijven en zich blijven aanpassen. Dat betekent: de omgeving blijven volgen, nieuwe dreigingen herkennen en snel maatregelen nemen.

Aanpak in de praktijk: van beleid naar uitvoering

Een goede aanpak begint met meer kennis en bewustzijn. Alle medewerkers – van uitvoerend tot leidinggevend – moeten weten waarom informatiebeveiliging belangrijk is. Regelmatige trainingen en praktische oefeningen helpen daarbij. Denk aan het oefenen in het herkennen van phishingmails of het naspelen van een datalek.

Daarna moeten risico's in kaart worden gebracht. Welke systemen en gegevens zijn het belangrijkst? Waar zitten de grootste kwetsbaarheden? Op basis daarvan kunnen maatregelen worden genomen. Bijvoorbeeld door sterke wachtwoorden en tweefactorauthenticatie te gebruiken, of gevoelige date te versleutelen.

Ook moeten er duidelijke regels en procedures zijn. Wie mag welke informatie gebruiken? Hoe wordt bijgehouden wie toegang heeft? Hoe wordt gecontroleerd of alles goed gaat? Deze afspraken moeten regelmatig worden aangepast aan nieuwe technologie en risico's.

Tot slot is het belangrijk om voortdurend te controleren of alles werkt. Monitoring van systemen, regelmatige controles en het testen van noodplannen zijn nodig om goed voorbereid te zijn op incidenten. Als er toch iets misgaat, moet duidelijk zijn wie wat doet en hoe de schade beperkt wordt.

Conclusie

Voor overheidsorganisaties is het naleven van de BIO, NIS2 en AVG niet alleen verplicht, maar ook belangrijk voor het goed functioneren van de organisatie. Door informatiebeveiliging serieus te nemen en als vast onderdeel van het werk te zien, kunnen risico's worden verkleind en wordt er voldaan aan de wet. Dit vraagt om samenwerking in alle lagen van de organisatie, van medewerker tot directie. Alleen zo blijft de informatievoorziening betrouwbaar en veilig. Nu en in de toekomst.