Handreiking beveiligingsplan bevoegd aftappen

Versie 2.3 — 2026

Wat is NBIP?

Nationale Beheersorganisatie Internet Providers (NBIP) is in 2001 opgericht als uitvoeringsinstituut voor tapbevelen. Aanbieders van openbare elektronische communicatiediensten en -netwerken zijn volgens de Telecommunicatiewet verplicht om dergelijke vorderingen uit te voeren en daar zelf zorg voor te dragen. NBIP neemt de uitvoering hiervan over van aanbieders.

Tegenwoordig is NBIP het expertisecentrum voor DDoS-mitigatie, Lawful Interception & Lawful Disclosure en Threat Intelligence-analyse voor aanbieders van digitale infrastructuur zoals telecom-, internet-, hosting- en cloudproviders in Nederland en Europa.

NBIP heeft geen winstoogmerk. De insteek is om gezamenlijk diensten te organiseren die te kostbaar of complex zijn om individueel te exploiteren. Door dit zonder winstoogmerk te doen, blijven de kosten voor alle deelnemers behapbaar. Omdat NBIP hoofdzakelijk aanbieders van digitale infrastructuur bedient, wordt die infrastructuur als geheel ook veiliger en meer betrouwbaar.

> “NBIP biedt gezamenlijke faciliteiten voor aanbieders van digitale infrastructuur en diensten zodat zij hun digitale weerbaarheid en naleving van wet- en regelgeving op orde hebben.”

Waarom een beveiligingsplan?

Aanbieders van openbare telecommunicatienetwerken en/of telecommunicatie-diensten* zijn verplicht medewerking te verlenen tot het aftappen of opnemen van telecommunicatie (die over hun telecommunicatienetwerken wordt afgewikkeld). De wettelijke basis hiervoor is gelegd in de Telecommunicatiewet artikel 13.2 lid 1 & 2 en het bijbehorende Besluit beveiliging gegevens telecommunicatie (Bbgt). Vanwege de gevoeligheid van de te verwerken informatie zijn extra maatregelen vereist voor de verwerking hiervan. In dit document lees je wat je als aanbieder van digitale infrastructuur en diensten moet doen om aan de wet-en regelgeving te voldoen.

Iedere aanbieder moet volgens het Bbgt onder andere beschikken over een **beveiligingsplan** waarin de door jouw getroffen beveiligingsmaatregelen zijn vastgelegd. De belangrijkste onderdelen die in het beveiligingsplan moeten staan, zijn opgenomen in dit document. Het document dient als hulpmiddel voor het zelf opstellen van je eigen beveiligingsplan.

In het plan moet worden aangegeven op welke wijze door een aanbieder uitvoering is gegeven aan zijn beveiligingsplicht en aan de maatregelen. **Let op**: dit is een aanvullend plan op de maatregelen die reeds zijn getroffen voor het voldoen aan de zorgplicht. Daarnaast moeten aanbieders inzage in het beveiligingsplan geven aan bevoegde autoriteiten als deze hiervoor een verzoek indienen (artikel 3, Telecommunicatiewet).

Wanneer je als organisatie 'tapplichtig' bent, kan je ook in aanraking komen met bevoegde autoriteiten. Zo ben je als organisatie verplicht inzage te geven in jouw beveiligingsplan bij controles van de Rijksinspectie Digitale Infrastructuur (RDI). Zij is uitvoerder en toezichthouder van wet- en regelgeving op gebied van telecommunicatie en onderdeel van het Ministerie van Economische Zaken. In het geval van een tapvordering, krijg je ook te maken met de autoriteiten die hier volgens de wet- en regelgeving voor bevoegd zijn.

Disclaimer: dit document kan alleen als leidraad worden gebruikt voor het beveiligingsplan van jouw organisatie. Er kunnen hieraan geen rechten worden ontleend.

Mijn organisatie is in het bezit van een ISO 27001 certificaat

Hoewel de vereisten van ISO 27001/2 veel gelijkenissen hebben met de vereisten aan het beveiligingsplan Bbgt, gaat het om twee wezenlijk verschillende zaken die los van elkaar benaderd moeten worden. Natuurlijk kunnen maatregelen die in het kader van ISO 27001 zijn ingericht ook worden toegepast om te voldoen aan het beveiligingsplan, denk bijvoorbeeld aan toegangsbeperkingen tot fysieke ruimtes.

Het is echter een misvatting dat een ISO 27001 certificering en bijbehorend beveiligingsplan ook zonder meer volstaat voor het Bbgt. NBIP adviseert dan ook om los van een eventueel aanwezig ISO 27001 certificaat om het beveiligingsplan zoals vereist in hoofdstuk 13 van de Telecommunicatiewet en het Bbgt up-to-date te maken en door te voeren in de gehele organisatie.

Mits zeer duidelijk beschreven, mag er naar onderdelen uit de ISO-documentatie worden verwezen in het op te stellen beveiligingsplan. NBIP adviseert niet alleen te verwijzen maar ook een kopie op te nemen van de artikelen uit de ISO-documentatie in het Bbgt beveiligingsplan. **Let op**: het beveiligingsplan moet up-to-date binnen de organisatie beschikbaar en te vinden zijn. Enkel verwijzingen naar andere documentatie, zoals een ISO-certificering, zullen tijdens een inspectie van de RDI niet volstaan.

** Ben je in Nederland actief als telecomaanbieder? Dan is jouw organisatie verplicht om zich te registreren bij de Autoriteit Consument en Markt (ACM). De ACM registreert aanbieders die openbare elektronische communicatie-activiteiten aanbieden en welke volgens de Telecommunicatiewet bepaalde rechten en plichten hebben. De ACM let erop of deze aanbieders zich aan de regels houden. Meer informatie hierover vind je op de website van de ACM.*

Het verschil tussen

Lawful Interception (LI) & Lawful Disclosure (LD)

Wanneer er wordt gesproken over bevoegd tappen zijn er twee verschillende typen: Lawful Disclosure (LD) en Lawful Interception (LI)

Wat is Lawful Disclosure (LD)?

Lawful Disclosure (LD) is gericht op het verkrijgen van sturingsinformatie door het verzamelen van achtergrondinformatie over een persoon of netwerk, het verkrijgen van bewijs en/of het verkrijgen van locatiegegevens van een getapte persoon. Dit gebeurt door het analyseren van de gespreksinhoud en verkeersgegevens of een combinatie van deze.

Enkele voorbeelden van deze gegevens zijn:

- Naam, adres, woonplaats (NAW);
- E-mailadressen;
- Gebruikersnaam;
- IP-adressen;
- Telefoonnummer(s) van de gebruiker;
- De soort (telecommunicatie)dienst die wordt afgenomen;
- Rekeningnummer(s).

Wat is Lawful Interception (LI)?

Bij Lawful Interception wordt een tap geplaatst die live de communicatie via telefoon of internet aftapt.

Belangrijk verschil tussen LI en LD

Lawful Disclosure wordt gezien als een lichter opsporingsmiddel dan Lawful Interception (het plaatsen van een live tap). Daarom kan de officier van justitie vordering van historische en toekomstige verkeergegevens zonder machtiging van de rechter-commissaris een goedkeuren voor bevoegde autoriteiten.

Lawful Interception (LI) is een zwaarder opsporingsmiddel waarvoor altijd een machtiging moet worden afgegeven door de rechter-commissaris. Bij LI moet de officier van justitie eerst zelf controleren of de aanvraag voor het inzetten van een tap voldoet aan de wettelijke eisen en in hoeverre de inzet van de tap bijdraagt aan de voortgang van het onderzoek. Hierna controleert de rechter-commissaris of de aanvraag van de officier van justitie inderdaad voldoet aan de gestelde eisen. Wanneer de rechter-commissaris de aanvraag vervolgens goedkeurt, kan de officier van justitie de tapvordering uitvaardigen waarna de tap wordt gevorderd bij de betreffende partij.

Wie kan gegevens opvragen?

De bevoegdheden van de opsporingsdiensten zijn beschreven in het Wetboek voor Strafvordering, Boek I, artikelen 126m tot en met 126nb. Net als de inlichtingendiensten mogen opsporingsdiensten, zoals de politie, verscheidene vormen van online dataverkeer aftappen en analyseren.

Wie kan een bevel geven om gegevens te leveren?

- De officier van justitie of de korpschef voor zijn korps, dan wel door het hoofd van een andere opsporingsdienst voor zijn dienst aangewezen opsporingsambtenaar;
- Het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), of de door hem aangewezen ambtenaar;
- Het hoofd van de Militaire Inlichtingen- en Veiligheidsdienst, of de door hem aangewezen ambtenaar.

Het inzetten van een tap moet in verhouding staan tot de ernst van het misdrijf. Zo mogen bevoegde opsporingsinstanties alleen live aftappen (lawful interception) als er verdenking is van een misdrijf dat een ernstige inbreuk op de rechtsorde vormt en waarop een gevangenisstraf van meer dan vier jaar staat. Voldoet het doelwit hieraan, dan moet bijvoorbeeld de politie toestemming vragen van een rechter-commissaris. De daadwerkelijke tap-periode mag niet langer dan 4 weken duren. Verlenging van de live tap is mogelijk, maar alleen met toestemming van de officier van justitie.

De inlichtingendiensten mogen de bewaarde informatie niet langer dan een jaar bewaren ter analyse. Deze periode kan met toestemming van de minister van Binnenlandse Zaken en Koninkrijksrelaties verlengd worden tot maximaal drie jaar. Anders dan de inlichtingendiensten mag de politie de ingewonnen gegevens tot dertig jaar bewaren.

Voor actuele persoonsgegevens wenden de inlichtingendiensten en opsporingsinstanties zich allereerst tot het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT), een onafhankelijke organisatie die binnen het ministerie van Justitie en Veiligheid valt. Het CIOT verzamelt dagelijks de gebruikersgegevens van telecomproviders en bewaart deze 24 uur. Elke dag worden de gegevens gewist en vervangen. Als aanbieder ben je verplicht om je te registreren bij het CIOT.

Jouw beveiligingsplan

In dit hoofdstuk vind je de benodigde informatie die kan worden gebruikt voor het opstellen van een beveiligingsplan. De basisopzet is gebaseerd op hoofdstuk 13 van de Telecommunicatiewet en het Bbgt. Het is altijd aan jou als aanbieder zelf om te zorgen dat het plan correct, compleet en up to date is.

De opzet is onder andere samengesteld op basis van de bijlage van het Bbgt, waarin puntsgewijs de gevraagde eisen staan vermeld. Voor de volledige toelichting kan je altijd de Telecommunicatiewet (hoofdstuk 13) en het Bbgt bekijken.

1 Beschrijving van het bedrijf en haar dienstverlening

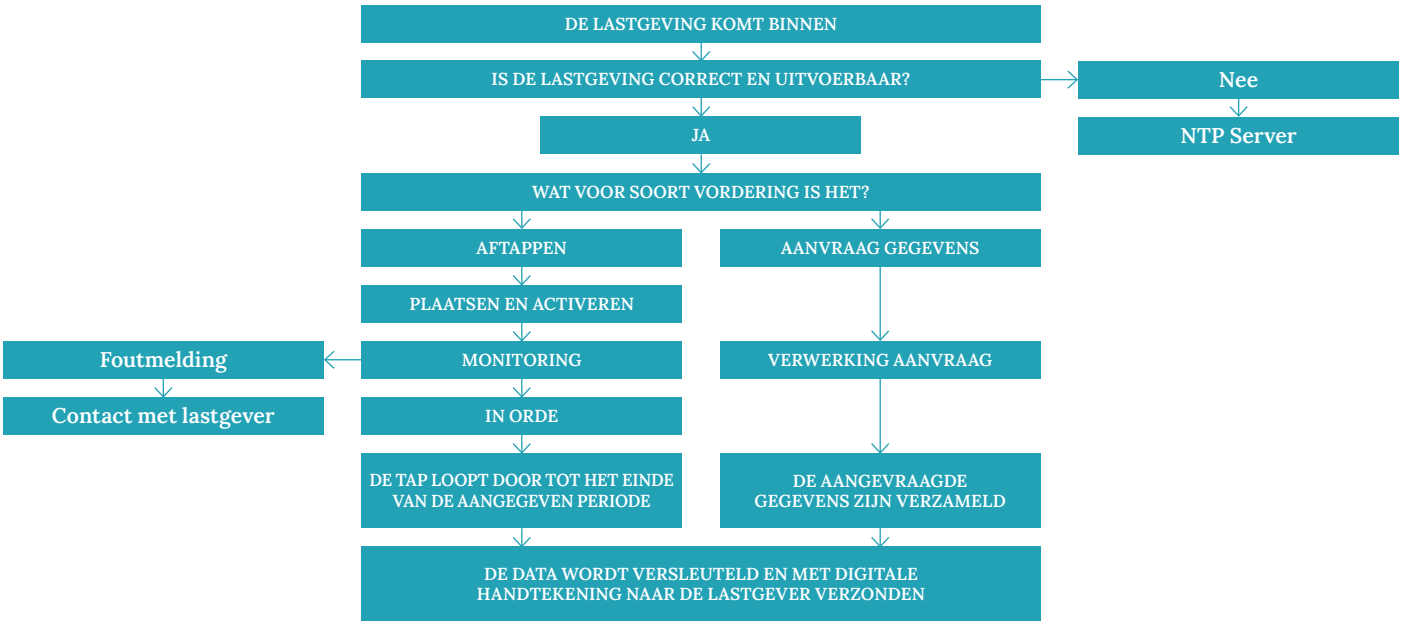
Het is in eerste plaats belangrijk dat je een **uitgebreide beschrijving** geeft van jouw bedrijf en jouw dienstverlening. Denk hierbij aan de diensten die je aanbiedt voor jouw (eind) klanten/gebruikers. Hierbij is het van belang dat in deze beschrijvingen ook staat hoe jouw diensten zijn ingericht.

Tip: Schrijf deze beschrijving zo gedetailleerd mogelijk, zodat er geen twijfels ontstaan over de diensten die je aanbiedt en vallen onder de 'tapplicht'.

2 Beschrijving van de LI/LD route

De insteek van een Bbgt-plan is dat nauwkeurig staat beschreven hoe binnen jouw dienstverlening de route van een tapbevel is vastgelegd. Hierbij dient het onderscheid te worden te gemaakt tussen de technische routes voor lawful interception (LI) én lawful disclosure (LD), toegespitst op jouw werkprocessen.

Schematische weergave van het tapproces



Jouw beveiligingsplan

Maatregelen die in jouw Bbgt-plan moeten zijn opgenomen

In dit hoofdstuk vind je de benodigde informatie die kan worden gebruikt voor het opstellen van een beveiligingsplan. De basisopzet is gebaseerd op hoofdstuk 13 van de Telecommunicatiewet en het Bbgt. Het is altijd aan jou als aanbieder zelf om te zorgen dat het plan correct, compleet en up to date is.

I Beveiligingseis algemeen

Er is een functionaris, belast met het toezicht op de uitvoering en naleving van de beveiligingsmaatregelen. De functionaris voert daartoe regelmatig controles uit en legt de resultaten daarvan vast.

Tip: Maak een document met daarin een roosteroverzicht van het bevoegd personeel wat betrokken is bij het werkproces. Je kan ook verwijzen naar een bestaand overzicht, maar dan moet dat wel als onderdeel van het beveiligingsplan worden toegevoegd. Ook toegang tot het (externe) rooster moet in het plan beschreven worden.

II Beveiligingseisen personeel

Binnen deze maatregel in jouw Bbgt-plan moeten de volgende aspecten wat betreft het bevoegde personeel worden vastgelegd:

De functieomschrijvingen

De functiebeschrijvingen van het personeel dat in aanraking komt met de gevraagde informatie en gegevens moeten worden vermeld. Binnen deze beschrijvingen dient ook de verantwoordelijkheid voor beveiliging van de gevraagde gegevens worden beschreven. Daarnaast moet worden aangetoond dat uitsluitend personeel dat volgens de functiebeschrijving belast is met de verwerking van de informatie en gegevens toegang heeft tot de informatie en de gegevens.

Geheimhoudingsverklaring en VOG

Personeel dat in aanraking komt met de informatie en gegevens tekent een geheimhoudingsverklaring én moeten beschikken over een verklaring omtrent goed gedrag (VOG-verklaring). ***Let op: bij inspecties van de Rijksinspectie Digitale Infrastructuur (RDI) moeten alle VOG-verklaringen van het bevoegde personeel fysiek aan de RDI overlegd kunnen worden.***

Tip: de functiebeschrijvingen moeten zijn voorzien van een herkenbaar hoofdstuk of taak. Zijn de functiebeschrijvingen niet beschikbaar? Dan kan een roosteroverzicht van het bevoegd personeel als basis worden gebruikt. Beschrijf vervolgens de aanvullingen op de bestaande functiebeschrijvingen. Daarnaast is het belangrijk te melden dat de functiebeschrijving én de geheimhoudingsverklaring een directe relatie moeten hebben met het LI/LD werk.

III Fysieke beveiliging en beveiliging van de omgeving

In dit deel van je Bbgt-plan beschrijf je nauwkeurig hoe in jouw organisatie de fysieke beveiliging en de beveiliging rondom het tapverwerkingsproces is ingericht.

Fysieke beveiliging (a t/m c)

De informatie en de gegevens moeten zoveel mogelijk in één ruimte zijn geconcentreerd. Dat betekent dat jouw organisatie in jouw bedrijfspand **een speciale toegewezen ruimte moet hebben.** Deze ruimte moet beschikken over een (elektronisch) slot dat alléén kan worden geopend door bevoegde medewerkers. Daarnaast moet de ruimte fysiek goed beveilig zijn. Het gaat hierbij niet alleen om toegangsbeveiliging zoals (elektronische) sloten op deuren, maar bijvoorbeeld ook een alarminstallatie en bijvoorbeeld, indien noodzakelijk, beveiliging van raamkozijnen. Ook is deze beveiliging zo ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.

Beveiliging rondom tapverwerkingsproces (punt d t/m g)

Alleen geautoriseerde personen, voor zover dit voor hun functie noodzakelijk is, hebben toegang tot de ruimte waar de gegevens of de informatie zich bevindt. Dit kan bijvoorbeeld geregeld worden door te werken met persoonlijke toegangspassen, tags of druppels. Zorg ervoor dat je dit als organisatie inzichtelijk hebt. Denk bijvoorbeeld aan een (actueel!) document voor de toewijzing en registratie van toegangspassen, pincodegebruik en de toegang tot patchkasten.

Ook het betreden en verlaten van de ruimte moet zo zijn geregeld dat er sprake is van gecontroleerde en achteraf herleidbare toegang voor ieder persoon. Verder geldt dat personen die onderhouds- en reparatiewerkzaamheden verrichten in deze ruimte door eigen geautoriseerd personeel moeten worden begeleid.

Documenten waarin de informatie en de gegevens zijn vastgelegd, worden in sterk beveiligde opbergmiddelen bewaard. Dat geldt indien de informatie en gegevens op verwisselbare gegevensdragers staan opgeslagen. Een voorbeeld hiervan is een kluis.

Tip: beschrijf in het plan de fysieke en organisatorische zaken van én over de ruimte waar de tapgegevens zich behoren te bevinden. Denk hierbij bijvoorbeeld aan cameratoezicht, opslag van videobeelden, registratie van toegangspassen, pincodegebruik en de toegang tot de patchkasten door wie, wanneer en waarom.

IV Beheer van communicatie- en bedieningsprocessen

Status en categorie van informatie en gegevens

Bij het beheer van de communicatie is het belangrijk dat de **status/categorie** van de informatie en gegevens (bijv. staatsgeheim of vertrouwelijk) altijd kenbaar is. Zorg daarom als organisatie dat je intern werkafspraken maakt over hoe deze categorisatie plaatsvindt en dat dit proces consistent wordt toegepast en gecontroleerd. Ook wordt sterk aangeraden dat in het geval van eventuele (onbedoelde) nalatigheid hiervan, het normaal is dat men hier elkaar op aanspreekt.

Reproductie

De reproductie van de informatie of gegevens is alléén toegestaan door geautoriseerde personen. Daaropvolgend mag reproductie alleen als dat nodig is voor de goede uitvoering van de bijzondere last (het verstrekken van de gegevens aan de bevoegde autoriteiten). ***Tip: Zorg actief voor dataminimalisatie, tenzij het niet anders kan om de vordering uit te voeren.***

Eventuele verplaatsing

Zorg dat de informatie of de gegevens niet buiten de normale (beveiligde) ruimte worden gebracht, tenzij dat voor de goede voortgang van de werkzaamheden noodzakelijk is. In dat geval wordt de verblijfplaats van de informatie of gegevens geregistreerd.

Verwijdering en vernietiging van informatie en gegevens

De verwijdering en vernietiging van de informatie en gegevens moet zo zijn ingeregeld dat dit proces niet kan worden teruggedraaid. Zorg ervoor dat je een rapport opmaakt van de verwijdering en vernietiging. Het rapport moet je in afschrift verzenden aan de bevoegde autoriteit of naar een door deze aangewezen instantie.

V Toegangsbeveiliging van geautomatiseerde informatiesystemen

De toegang tot geautomatiseerde informatiesystemen waarin de informatie en gegevens worden verwerkt is goed beveiligd, onder meer door middel van **persoonsgebonden authenticatie**. Ook moet de beveiliging zo zijn ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en tijdige interventie plaatsvindt.

Belangrijk is ook dat het **aantal foutieve inlogpogingen** is **beperkt tot drie.** Overschrijding van het aantal foutieve inlogpogingen leidt tot definitieve blokkering. Ook de mogelijk mislukte toegangspogingen moeten geregistreerd worden en daarop moet worden geacteerd. De definitieve blokkering kan alleen worden opgeheven door de benoemde functionaris (zie maatregel I, 'Beveiligingseis algemeen'). Dit is niet van toepassing op de systeembeheerder op de voorwaarde dat bij drie foutieve inlogpogingen een hernieuwde inlogpoging slechts kan plaatsvinden via een voor noodsituaties ingericht account en persoonsgebonden authenticatie voor het gebruik. De functionaris moet hiervoor toestemming verlenen.

Het geautomatiseerde systeem, waarin de gegevens en informatie worden verwerkt, wordt niet eerder verlaten dan nadat een (**handmatig of automatisch**) **toegangsbeveiligingsmechanisme** in werking is gesteld. ***Tip: zorg als organisatie ervoor dat dit proces staat gedocumenteerd.***

Zorg er ook voor dat alle handelingen met betrekking tot de verwerking van de informatie en de gegevens in het geautomatiseerde informatiesysteem persoonsgebonden zijn vastgelegd om (eventueel) onderzoek ernaar mogelijk te maken. Daarnaast moet je als organisatie hebben vastgelegd dat alléén geautoriseerd personeel toegang heeft tot het geautomatiseerde informatiesysteem en de autorisaties van alle gebruikers worden vastgelegd.

De toegangsrechten voor het personeel moet volgens de wet ook periodiek worden geëvalueerd. Tip: houd een schema bij waarin staat wie er toegang heeft, waarom deze persoon toegang heeft en de meest recente updates op datum staan vermeld.

VI – Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen

Deze sectie gaat specifiek in op de ontwikkeling, het onderhoud en eventuele reparaties van het geautomatiseerde informatiesystemen.

Zorg als organisatie ervoor dat **alle wijzigingen in apparatuur, software of procedures** die de beveiliging van de gegevens en informatie kunnen beïnvloeden controleerbaar zijn. ***Tip: Maak een overzichtsdocument waarin alle wijzigingen zijn gedocumenteerd en als aanvaardbaar zijn beoordeeld.***

Het **onderhouden van geautomatiseerde informatiesystemen**, voor zover deze nog toegang verschaffen tot gegevens en informatie, vindt **op locatie plaats**. ***Tip: maak een schema/agenda waarin je vastlegt wanneer onderhoud heeft plaatsgevonden.***

Het op afstand onderhouden van geautomatiseerde informatiesystemen is slechts toegestaan, als dit wordt uitgevoerd door geautoriseerde personen en alleen op tijdstippen waarvoor de functionaris toestemming heeft verleend. Daarnaast moet ook worden aangetoond dat er voldoende veiligheidsgaranties bestaan voor het handhaven van het beveiligingsniveau van de gegevens en informatie.

De **reparaties aan het geautomatiseerde informatiesysteem**, waarin de informatie en gegevens worden verwerkt, vindt **op locatie plaats**. Alleen wanneer de informatie en gegevens zijn verwijderd en niet te achterhalen zijn, kan hiervan worden afgeweken.

Uitbesteding werkzaamheden aan derden

Een belangrijk artikel binnen het Bbgt is artikel 8. Dit artikel beschrijft wat je als aanbieder hebt gedaan om de uitbesteding van de werkzaamheden veilig en volgens de wetgeving te borgen. Dit geldt bijvoorbeeld wanneer je deze werkzaamheden hebt uitbesteed bij NBIP.

Binnen dit artikel wordt expliciet benadrukt dat je zelf als aanbieder verantwoordelijk ervoor blijft dat een derde partij die je hiervoor inschakelt, de verplichtingen nakomt.

Om welke verplichtingen gaat het?

Als aanbieder draag je zorg ervoor dat een derde partij zich verplicht:

- De opgevraagde gegevens en informatie te beveiligen waardoor deze niet door onbevoegden kan worden ingezien.
- Zich te houden aan de geheimhoudingsplicht over de opgevraagde gegevens en informatie.
- De maatregelen uit het Bbgt na te leven.
- Alle informatie te verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is.

Let op: de verplichtingen moeten zijn opgenomen in een schriftelijke overeenkomst tussen jou en de derde partij. Ook moet er inzage worden gegeven in de overeenkomst wanneer een bevoegde autoriteit expliciet hiernaar verzoekt.

Wat te doen bij een inbreuk op gegevens?

In artikel 6 van het Bbgt is de **meldplicht van beveiligingsincidenten** vastgelegd. Gebeurt er bij jou als aanbieder van een beveiligingsincident, waarbij er ongeoorloofde inbreuk is gemaakt op gegevens of informatie? Of is er een probleem met de geplaatste livetap? Meld dit dan als aanbieder zo snel mogelijk bij de bevoegde autoriteiten. Het gaat hierbij om de volgende autoriteiten (artikel 1, Bbgt):

- de officier van justitie of de door de korpschef voor zijn korps, dan wel door het hoofd van een andere opsporingsdienst voor zijn dienst aangewezen opsporingsambtenaar;
- het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), of de door hem aangewezen ambtenaar;
- het hoofd van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), of de door hem aangewezen ambtenaar.

Als aanbieder geef je door:

- om welke informatie of gegevens het gaat;
- de wijze waarop de inbreuk heeft plaatsgevonden;
- welke maatregelen zijn genomen om verdere verspreiding van de bedoelde informatie of gegevens tegen te gaan en herhaling te voorkomen.

Nieuwe wetgeving voor aanbieders

Het is in eerste plaats belangrijk voor aanbieders om aan de Telecommunicatiewet en het Bbgt te voldoen. Op korte termijn treedt ook aanvullende wetgeving in werking.

eEvidence

Onder het eEvidence pakket kunnen bevoegde instanties uit andere Europese lidstaten rechtstreeks elektronisch bewijsmateriaal opvragen bij aanbieders van digitale diensten in andere Europese lidstaten.

Wie moet hieraan voldoen?

Aanbieders van:

- elektronische communicatiediensten
- internetdomeinnamen en IP-nummering
- communicatie-, opslag- en verwerkingsdiensten

Als aanbieder die valt onder eEvidence moet je geregistreerd staan bij de Autoriteit Consument en Markt (ACM). De ACM geldt als toezichthouder van eEvidence en zien erop toe dat bedrijven zich tijdig inschrijven in de Court Database (CDB) van de Europese Commissie.

Let op: Wanneer dit niet wordt gedaan, kan de ACM het bestuursrecht toepassen om te handhaven wanneer je je niet (tijdig) inschrijft of je gegevens niet up-to-date houdt.

Vanaf wanneer?

Per 18 augustus 2026 moeten aanbieders voldoen aan eEvidence. Je leest hier meer over op de website van NBIP.

Cyberbeveiligingswet (Cbw)

De Cyberbeveiligingswet (Cbw) is de nationale implementatiewet van de Europese NIS2-richtlijn. Deze richtlijn heeft als doel om een hoog gemeenschappelijk niveau van cyberbeveiliging in Europa te bereiken, en om de werking van de interne markt te verbeteren.

De Cbw bestaat uit de zorgplicht voor aanbieders van digitale infrastructuur en diensten waarin zij passende en evenredige technische, operationele en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen. Daarnaast is er een meldplicht vastgelegd waarbij aanbieders verplicht zijn te melden wanneer zij te maken hebben met grote ICT-incidenten, zoals bijvoorbeeld een grootschalig datalek.

Wanneer de Cbw in werking treedt, vervangt deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni).

Meer info over de Cbw?

Voor de Cbw heeft het NCSC een FAQ-pagina opgesteld met daarin aanvullende informatie over de toekomstige wet. Klik hier om deze te raadplegen.

Begrippenlijst

Aanbieder: Aanbieder van een telecommunicatienetwerk en/of -dienst, zoals vastgelegd in de Telecommunicatiewet, artikel 13.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD): Autoriteit Consument en Markt (ACM): registreert aanbieders die openbare elektronische communicatie-activiteiten aanbieden en welke volgens de Telecommunicatiewet bepaalde rechten en plichten hebben. De ACM let erop of deze aanbieders zich aan de regels houden.

Autoriteit Persoonsgegevens (AP): onafhankelijke toezichthouder op persoonsgegevens die mensen beschermt in een digitale wereld.

Bbgt: Besluit beveiliging gegevens telecommunicatie. Geldend van 01-05-2018 t/m heden.

Cyberbeveiligingswet (Cbw): is de nationale implementatiewet van de Europese NIS2-richtlijn. Deze NIS2-richtlijn heeft als doel om een hoog gemeenschappelijk niveau van cyberbeveiliging in Europa te bereiken, en om de werking van de interne markt te verbeteren. De wet gaat gelden voor aanbieders van digitale infrastructuur en diensten.

Gegevens: betreft de verkeers- en locatiegegevens, bedoeld in artikel 11.1, onderdeel b respectievelijk onderdeel d, alsmede de daarmee verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren. Artikel 2.1 van de Bbgt spreekt over gegevens welke in het kader van het verlenen van medewerking aan de uitvoering van een bevoegd gegeven bijzondere last dan wel een opdracht op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2017 tot het aftappen of opnemen van telecommunicatie door een bevoegde autoriteit aan de aanbieder zijn verstrekt.

Informatie: betreft de informatie welke door de aanbieder aan een bevoegde autoriteit is verstrekt op grond van de artikelen 13.2b en 13.4 van de wet alsmede de gegevens welke zijn vervat in het aan deze verstrekking ten grondslag liggende verzoek of in de aan deze verstrekking ten grondslag liggende vordering om informatie van de desbetreffende bevoegde autoriteit;

Lawful Disclosure (LD): het verstrekken van gegevens ten aanzien van klanten zoals NAW-gegevens

Lawful Interception (LI): het tappen van dataverkeer Militaire Inlichtingen- en Veiligheidsdienst (MIVD): dienst die de krijgsmacht ondersteunt met betrouwbare en actuele inlichtingen. Ook houdt de dienst dag en nacht zicht op dreigingen tegen Nederland, de krijgsmacht en bondgenoten. Onderdeel van het ministerie van Defensie.

Nationaal Cyber Security Centrum (NCSC): is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Fungeert als uitvoeringscoördinator, kennis- en expertisecentrum, nationaal en sectoraal Computer Security Incident Response Team (CSIRT).

Nationale Beheersorganisatie Internetproviders (NBIP): uitvoeringsinstituut voor tapvordering voor digitale infrastructuur en dienstenaanbieders. NBIP biedt gezamenlijke faciliteiten voor aanbieders van digitale infrastructuur en diensten zodat zij hun digitale weerbaarheid en naleving van wet- en regelgeving op orde hebben.

PGP-sleutel: bestand om veiligheidsinbreuken in elektronische vertrouwensdiensten (eIDAS) versleuteld te versturen. Wordt gebruikt voor Wbni-incidentmeldingen

Rijksinspectie Digitale Infrastructuur (RDI): is uitvoerder en toezichthouder van wet- en regelgeving op gebied van telecommunicatie. De RDI is onderdeel van het Ministerie van Economische Zaken. Opvolger Agentschap Telecom (sinds 1 januari 2023).

Verklaring Omtrent het Gedrag (VOG): is een verklaring waaruit blijkt dat het justitiële verleden van een persoon of rechtspersoon geen bezwaar vormt voor de functie of het doel waarvoor de VOG is aangevraagd. Justis (de screeningsautoriteit van het ministerie van Justitie en Veiligheid) is de enige instantie die de VOG-aanvragen behandelt en de VOG afgeeft.

Wet beveiliging netwerk- en informatiesystemen (Wbni): wet die sinds 9 november 2018 geldt en is er op gericht om de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en maatschappelijke ontwrichting te voorkomen. De Wbni verplicht aanbieders van essentiële diensten en digitale dienstverleners om maatregelen te nemen om hun ICT te beveiligen tegen incidenten.

nationale
beheersorganisatie
internet providers