

Toepasselijke wet- en regelgeving

[]

Versie: 18 | Definitief
2025 11 01 | PUBLIEK

it starts
with a
personal
touch

www.previder.nl

it starts here | previder

Overzicht toepasselijke wet- en regelgeving

Telecommunicatiewet

Aanbieder versus openbaar aanbieder

- De wet maakt een onderscheid tussen een aanbieder van een communicatiedienst in de zin van artikel 126la Sv (hierna: een aanbieder van een communicatiedienst) en een aanbieder van een openbare telecommunicatiedienst of openbare telecommunicatienetwerk in de zin van de Telecommunicatiewet (hierna: een aanbieder van een openbare communicatiedienst of telecommunicatienetwerk).

Ingevolge artikel 126la Sv is een aanbieder van een communicatiedienst "de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst". Alle bevoegdheden die zijn opgenomen in artikel 126m tot en met 126nb Sv hebben betrekking op "aanbieders" – en derhalve niet alleen op "openbare aanbieders".

- Ingevolge artikel 1.1.ff van de Telecommunicatiewet is een openbaar telecommunicatiedienst een "voor het publiek beschikbare dienst die geheel of gedeeltelijk bestaat in het overbrengen van signalen via een elektronisch communicatienetwerk, voor zover deze dienst niet bestaat uit het verspreiden van programma's". Ingevolge artikel 1.1.ee Telecommunicatienetwerk is een openbaar telecommunicatienetwerk een "elektronisch communicatienetwerk dat geheel of gedeeltelijk wordt gebruikt om openbare telecommunicatiediensten aan te bieden, voor zover het netwerk niet gebruikt wordt voor het verspreiden van programma's".

Burgerlijk Wetboek

Aansprakelijkheid van hostingproviders

- Het uitgangspunt is 6:196c (lid 1 en 2) BW: Degene die diensten van de informatiemaatschappij verricht als bedoeld in artikel 15d lid 3 van Boek 3, bestaande uit het doorgeven van van een ander afkomstige informatie of het verschaffen van toegang tot een communicatienetwerk is niet aansprakelijk voor de doorgegeven informatie, indien:
 - ✧ 1) De hostingprovider weet niet en behoort niet te weten dat de informatie een onrechtmatig karakter heeft.
 - ✧ 2) Zodra de provider van het onrechtmatige karakter op de hoogte is, zal hij direct de informatie verwijderen of de toegang tot de website blokkeren.

Op grond van dit wetsartikel is een hosting provider niet aansprakelijk voor informatie die zij op verzoek van een gebruiker opslaat, tenzij zij wordt gewezen op het "onmiskenbaar onrechtmatige" karakter van de informatie én zij vervolgens niet prompt handelt om die informatie te blokkeren of ontoegankelijk te maken.

Gedragcode Notice-and-Take-Down 2018 inclusief addendum 1

Op grond van de E-commerce richtlijn zijn internettussenpersonen niet-aansprakelijk voor informatie door anderen opgeslagen. Dit niet-aansprakelijkheidsregime heeft geleid tot het hanteren van Notice-and-takedown (NTD) procedures.

De NTD code wordt met name gehanteerd door partijen die de mogelijkheid hebben om de evidente onrechtmatigheid van het internet te verwijderen, zoals service providers, hosters en andere aanbieders van online faciliteiten.

De NTD code respecteert de neutrale rol van Internet providers, omvat hoor en wederhoor van betrokkenen, zorgt voor snelheid van handelen. Zo kan evidente onrechtmatigheid snel worden geneutraliseerd en worden lange juridische trajecten voorkomen. Zij geeft daarbij online-dienstverleners duidelijkheid hoe ze kunnen optreden als zij zo'n verzoek binnen krijgen, en helpt degenen die meldingen doen om duidelijkheid te krijgen over hetgeen zij moeten en kunnen doen, en de afhandeling ervan bij de providers.

Zie NTD Code: https://noticeandtakedowncode.nl/wp-content/uploads/2018/12/ECP_01054-Gedragcode-notice-and-takedown-pdf-2.pdf

e-Commercerichtlijn

Artikelen 12-15 van e-commercerichtlijn zijn in Nederland geïmplementeerd in artikel 6:196c BW.

Wet Beveiliging Netwerk- en Informatiesystemen ("WBNI ") – NIS1

De WBNI blijft van kracht totdat de Nederlandse Cyberbeveiligingswet (Cbw) in werking treedt, die de WBNI zal vervangen (zie hierna).

Op grond van deze wet heeft Previder als DSP een meldplicht bij het NCSC. Daarnaast bevat de wet een zorgplicht. Partijen die onder de wet vallen moeten maatregelen nemen om de kansen en gevolgen van digitale incidenten te verkleinen.

Cyberbeveiligingswet ("Cbw ") – NIS2

De WBNI blijft van kracht totdat de Nederlandse Cyberbeveiligingswet (Cbw) in werking treedt, die de WBNI zal vervangen (zie hierna).

Gericht op verbetering van de cyberveiligheid in essentiële sectoren door striktere beveiligingsvereisten voor bedrijven en overheidsinstanties.

Data Act

Gericht op eerlijke toegang tot en gebruik van (vooral niet-persoonlijke) data, tussen bedrijven en overheden, wat innovatie stimuleert. De Data Act gaat in op het voorkomen van Provider lock in en regelt daarvoor de kostenstructuur die een provider in rekening mag brengen bij het overstappen naar een andere Provider. Tot drie jaar na de inwerkingtreding van de Data Act mogen providers overstapkosten in rekening brengen die niet hoger mogen zijn dan de directe kosten die de provider maakt voor het overstapproces. Voorbeelden van gebruikelijke overstapkosten zijn kosten voor de doorgifte van gegevens van de ene aanbieder naar de andere.

AI Act

Gericht op systemen door risico's te beoordelen van 'minimaal risico' tot 'onaanvaardbaar risico'. Met name strenge regels voor hoog-risico toepassingen zoals gezichtsherkenning en medische apparaten.

Wet op de inlichtingen- en veiligheidsdiensten 2017 ("WIV 2017")

Ter achtergrondinformatie: een verleende bevoegdheid strekt altijd tot het bereiken van een bepaald doel. Het uitgangspunt van de wet is dat de voorwaarden waaronder bevoegdheden mogen worden ingezet, nauwkeurig zijn omschreven en afgebakend. Bevoegdheden mogen niet worden gebruikt om in werkelijkheid een ander doel te bereiken dan waartoe de wettelijke bevoegdheid strekt. Dit neemt niet weg dat tegelijkertijd meerdere bevoegdheden kunnen worden toegepast en dat toepassing van de ene bevoegdheid kan uitmonden in toepassing van een andere, meer verstrekkende bevoegdheid. Dit laatste geldt bijvoorbeeld in het geval dat opsporingsambtenaren tijdens het maken van een forensic image constateren dat de bestanden te groot zijn en dat tot inbeslagneming van één of meer servers moet worden overgegaan. De opsporingsambtenaren zijn daartoe (in beginsel) bevoegd, indien de inbeslagneming dient om de waarheid aan de dag te brengen en ook overigens aan de voorwaarden waaronder inbeslagneming kan plaatsvinden wordt voldaan.

Enkele belangrijke artikelen:

- Artikel 42 WIV 2017 is de AIVD/MIVD bevoegd om, al dan niet met behulp van een technisch hulpmiddel, besloten plaatsen en gesloten voorwerpen te doorzoeken.
- Vorderen van verkeersgegevens door AIVD/MIVD. De vordering kan worden gericht aan aanbieders van communicatiediensten.
- Vorderen van identificerende gegevens door AIVD/MIVD
- Art. 45 WIV 2017: binnendringen van een geautomatiseerd werk, al dan niet in combinatie met opdracht tot decryptie door AIVD/MIVD
- Art. 54 WIV 2017: vorderen opgeslagen gegevens door AIVD/MIVD
- Art. 58 WIV 2017: toegang tot plaatsen door AIVD/MIVD
- Op grond van art 135 WIV 2017 is een ieder die betrokken is bij de uitvoering van de WIV 2017 tot geheimhouding verplicht, behalve voor zover enig wettelijk voorschrift hem tot bekendmaking verplicht

Algemene Wet Bestuursrecht ("Awb")

- Op grond van art. 5:17 Awb zijn toezichthouders (vervolgens) bevoegd om inzage in zakelijke gegevens en bescheiden te 'vorderen', voor zover dat redelijkerwijs nodig is voor de vervulling van hun taak (art. 5:13 Awb). Degene die zo'n vordering krijgt, is verplicht daaraan medewerking te geven (art. 5:20 Awb).
- Opzettelijke weigering van medewerking levert een strafbaar feit op in de zin van art. 184 Sr (het niet opvolgen ambtelijk bevel). Alleen verschoningsgerechtigden (zoals advocaten) kunnen de medewerking weigeren (art. 5:20 Awb).

Digital Operational Resilience Act ("DORA")

De essentie van DORA (Digital Operational Resilience Act) is het versterken van de digitale weerbaarheid van de financiële sector in de EU tegen cyberdreigingen. Dit wordt bereikt door het vergroten van de weerbaarheid door middel van eisen aan ICT-risicobeheer, incidentrapportage en -tests, en toezicht op ICT-leveranciers om de continuïteit van financiële diensten te waarborgen.

Wetboek van Strafvordering ("Sv")

Enkele belangrijke artikelen die van toepassing zijn:

- Artikel 96 Sv: inbeslagnemingsbevoegdheid en betredingsbevoegdheid: regelt een algemene inbeslagnemingsbevoegdheid. Als is voldaan aan de voorwaarden van het eerste lid, mag de opsporingsambtenaar aangetroffen, daarvoor vatbare voorwerpen in beslag nemen en mag hij daartoe ook elke plaats betreden
- Artikel 96a Sv: bevel tot uitlevering: regelt de bevoegdheid om van daarvoor vatbare voorwerpen de uitlevering te vorderen van een (rechts)persoon, niet zijnde een verdachte
- Artikel 96c Sv: doorzoeken van plaatsen ter inbeslagneming: regelt voor de (hulp)officier van justitie een bevoegdheid tot het doorzoeken van plaatsen ter inbeslagneming
- Artikel 125i/125j Sv: doorzoeken ter vastlegging van gegevens: regelt de bevoegdheid tot doorzoeking van een plaats ter vastlegging van gegevens en de bevoegdheid tot vastlegging van die gegevens. De doorzoeking kan zich uitstrekken tot identificerende gegevens, andere dan identificerende gegevens en gevoelige gegevens
- Artikel 125o Sv: ontoegankelijk maken van gegevens: Indien bij een doorzoeking in een geautomatiseerd werk gegevens worden aangetroffen waarmee of waardoor strafbare feiten zijn begaan, kan worden bepaald dat deze gegevens ontoegankelijk worden gemaakt voor derden en/of niet verder kunnen worden verspreid
- Artikel 126m Sv: opnemen vertrouwelijke communicatie met een technisch hulpmiddel ("tappen"): regelt de bevoegdheid om met een technisch hulpmiddel vertrouwelijke communicatie op te nemen. Het gaat hierbij om het kennis nemen van de inhoud van de communicatie
- Artikel 126n Sv: vordering verstrekking verkeersgegevens: regelt de bevoegdheid tot het vorderen van verkeersgegevens. De bevoegdheid tot het vorderen van verkeersgegevens ziet zowel op historische als toekomstige verkeersgegevens en omvat zowel gebruikersgegevens als locatiegegevens
- Op grond van art. 138g Sv wordt onder aanbieder van een communicatiedienst verstaan "de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst

Wetboek van Strafrecht ("Sr")

- Op grond van art. 184 Wetboek van Strafrecht (Sr), wettelijk verplichtingen om te voldoen aan: een (rechtmatig gegeven) bevel tot uitlevering van voorwerpen (zoals servers) of aan een (rechtmatig gedane) vordering tot het verstrekken van (bepaalde) gegevens, (wettelijk) verplicht is om de inbeslagneming van voorwerpen (zoals servers) door opsporingsambtenaren toe te staan.

Intellectueel eigendomsrecht

Intellectueel eigendomsrecht is de verzamelnaam voor rechten op intellectuele creaties. Denk aan o.m. muziek, merken, vormgeving, uitvindingen, teksten en foto's. Onder het IE recht vallen onder andere het auteursrecht, het merkenrecht, het handelsnaamrecht en het octrooirecht. Deze rechten zijn zowel in Nederlandse als internationale wetgeving vastgelegd.

Algemene Verordening Gegevensbescherming

Elke verwerking van persoonsgegevens moet rechtmatig, eerlijk en transparant zijn. In de AVG staat wat bedrijven en organisaties wel en niet mogen doen met persoonsgegevens van hun klanten, personeel en andere personen.

Uitvoeringswet AVG ("UAVG")

De AVG is rechtstreeks van toepassing in Nederland. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG).

Wet Bevordering Speur- en Ontwikkelingswerk ("WBSO")

De Wet bevordering speur- en ontwikkelingswerk is een fiscale regeling van het Nederlandse ministerie van Economische Zaken om Onderzoek & Ontwikkeling (R&D) te bevorderen.



it starts
with a
personal
touch

www.previder.nl

it starts here | **previder**