
Beleid en procedures bij justitiële vorderingen tot verstrekking van gegevens gericht aan een Cloudbaanbieder

Auteur:



Elfahmi el Bouazati

Lawyer IT, Technology and Privacy

Stimmt B.V.



Inhoudsopgave

Introductie	3
Vorderen kan, geheimhouden moet	3
Vordering kan alleen bij een misdrijf	4
Eerste stappen bij een vordering	5
De ijzeren regels voor medewerkers van een Cloudaanbieder	6
Beroep je op geheimhouding en afgeleid verschoningsrecht	6
Verplichte of een vrijwillige medewerking?	6
Verstrek nooit zomaar gegevens	6
Laat ambtenaar altijd weten dat je niet bevoegd bent te beslissen	6
Vraag om schriftelijke vordering	6
Contacteer altijd directie	7
Nooit meer verstrekken dan gevorderd	7
Controle van de vordering	8
Altijd betrokkenheid en voorafgaande toestemming van de officier van justitie vereist	8
Welke gegevens kunnen worden gevorderd en onder welke voorwaarden?	8
Welke informatie moet een vordering bevatten?	9
Moet er een verdachte genoemd zijn?	9
De geheimhoudingsplicht en (afgeleid) verschoningsrecht	10

1 Introductie

Dit document bevat beleid en procedures over hoe om te gaan met vorderingen van politie en/of justitie. Er zijn verschillende digitale opsporingsbevoegdheden te onderscheiden, te weten:

- internetonderzoek: het zoeken van gegevens op publiek toegankelijke internetbronnen;
- in beslag nemen van gegevensdragers en onderzoek daaraan;
- doorzoeken ter vastlegging van gegevens: het onderzoek van gegevensdragers die niet in beslag zijn genomen;
- de bevoegdheid om (heimelijk) binnen te dringen in geautomatiseerde werken en daaraan onderzoek te doen met het oog op bepaalde handelingen;
- het vorderen tot verstrekking van opgeslagen gegevens.

Dit document gaat niet in op alle digitale opsporingsbevoegdheden van justitiële organen. Dit beleid ziet op enkel de vorderingen tot verstrekking van gegevens die een daartoe bevoegd orgaan kan doen bij een Cloudaanbieder. Dit beleid ziet niet toe op andere opsporingsbevoegdheden van opsporingsorganen, zoals onderzoek ter plaatse op kantoor, heimelijk onderzoek, hackbevoegdheid, d etc.

Dit document is bedoeld als een praktische handleiding hoe om te gaan met (mondelijke en schriftelijke) justitiële vorderingen tot verstrekking van gegevens die je als Cloudaanbieder kunt krijgen. Cloudaanbieders moeten bedachtzaam zijn over de te volgen stappen en dienen niet klakkeloos de gevorderde gegevens te verstrekken. Het advies is altijd een jurist te raadplegen voor advies en ondersteuning.

Buiten scope

Buiten scope van deze handleiding zijn onder meer:

- andere opsporingsbevoegdheden dan vordering tot verstrekking van gegevens door justitiële organen
- vorderingen door andere (handhavings- en toezichts)organen zoals bijvoorbeeld door Agentschap Telecom, ACM, AP
- vordering met schriftelijke machtiging van rechter-commissaris (controleer altijd met een jurist of een schriftelijke machtiging vereist is voor de vordering)
- de grondslagen waarop de vordering gebaseerd wordt (controleer dit altijd met een jurist)

Dit document wordt aangehaald als: “Beleid en procedures vorderingen politie en justitie Cloudaanbieder”

1.1 Vorderen kan, geheimhouden moet

De politie of justitie kan een Cloudaanbieder benaderen met het verzoek om gegevens te verstrekken. Echter alle gegevens die een Cloudaanbieder over een subject te weten komt, kunnen vallen onder de geheimhouding. In de eerste plaats heeft de Cloudaanbieder te maken met de contractuele geheimhouding die tussen hem en zijn of haar klant geldt. Daarnaast kan ook geheimhouding voortvloeien uit feit dat een dienst onderdeel is van klant met een wettelijke beroepsgeheim en daardoor kan het hieraan gekoppelde afgeleid verschoningsrecht voor een Cloudaanbieder gelden. Ook (rechts)personen die diensten verlenen aan klanten met een wettelijk beroepsgeheim (artsen, advocaten, notarissen accounts enz.) hebben kunnen aldus een afgeleid verschoningsrecht, zoals een Cloudaanbieder. Alsdan kan dan gelden dat het verschoningsrecht van de verschoningsgerechtigde ook doorwerkt naar Cloudaanbieders die voor of namens

verschoningsgerechtigde gegevens verwerken. Daarom kunnen dienstverleners zich beroepen op een afgeleid verschoningsrecht.

Bij een vordering tot verstrekking door justitiële organen dient als hoofdregel te gelden dat Cloudaanbieders niet zomaar informatie over subject aan de politie of justitie verstrekken en dienen zich beraden over hoe legitiem een vordering is en daarbij zich in eerste instantie te beroepen op hun (contractuele) geheimhoudingsplicht of -indien het geval- op het afgeleid verschoningsrecht.

1.2 Vordering kan alleen bij een misdrijf

De bevoegdheden tot het vorderen van gegevens kan alleen worden toegepast in geval van verdenking van een misdrijf of van het beramen of plegen van misdrijven in georganiseerd verband die een ernstige inbreuk op de rechtsorde opleveren. Vordering kan dus niet geschieden bij een overtreding, maar uitsluitend bij misdrijven.

Van de verstrekking van de gegevens wordt een proces verbaal opgemaakt opdat rechterlijke controle achteraf mogelijk is.

2 Eerste stappen bij een vordering

- I. Controleer altijd de (schriftelijke) vordering. Indien de vordering mondeling geschiedt verzoek dan de bevoegde persoon/orgaan de vordering op schrift te zetten. Controleer daarna de schriftelijke vordering, Is de vordering afkomstig van een bevoegd orgaan? In het bijgevoegde gekwalificeerd certificaat voor de elektronische handtekening in de elektronische vordering kunt u de identiteit controleren van de persoon die vordering stelt of namens een bevoegd orgaan wordt gesteld. Zie hiermee informatie over de controleerbaarheid de gekwalificeerde elektronische handtekening: <https://www.om.nl/onderwerpen/elektronische-handtekening>
- II. Maak de politie en/of justitie duidelijk dat ze te maken met wat voor een organisatie/bedrijf ze te maken hebben en vraag in hoeverre ze niet op andere minder vergaande wijze voor de Cloudbaanbieder aan de gegevens kunnen komen.
- III. Wijs ze op de (contractuele) geheimhouding en/of op het feit dat er sprake is van (afgeleid) beroepsgeheim en verschoningsrecht. Maak dus altijd schriftelijk bezwaar tegen de vordering.
- IV. Bij telefonische verzoeken van politie en/of justitie: bel terug ter verificatie van de instantie en de vordering en vraag altijd naar de namen van de betreffende ambtenaar die het verzoek doet (al dan niet namens een officier van justitie).
- V. Verzoek altijd politie en/of justitie om haar verzoek conform de wet gericht en schriftelijk te stellen. Een vordering mag nimmer onbepaald zijn.
- VI. Vraag naar één contactpersoon en een vast telefoonnummer bij politie en/of justitie als aanspreekpunt.
- VII. Maak bij politie en/of justitie bekend wie de contactpersoon is binnen de organisatie een Cloudbaanbieder.

3 De ijzeren regels voor medewerkers van een Cloudbaanbieder

3.1 Beroep je op geheimhouding en afgeleid verschoningsrecht

Wijs de opsporingsambtenaar altijd op de verwevenheid met geheimhouding en eventueel het van toepassing zijnde stringente beroepsgeheim en verschoningsrecht. Een Cloudbaanbieder heeft altijd een (buiten)contractuele geheimhoudingsplicht jegens zijn klanten. Bij een vordering wordt dus impliciet die geheimhoudingsplicht te schenden, met het risico op aansprakelijkheid als Cloudbaanbieder bij een eventuele verstrekking. Dus als uitgangspunt dient te gelden dat gewezen wordt op de (buiten)contractuele geheimhouding.

3.2 Verplichte of een vrijwillige medewerking?

Gaat het om een verplichte of een vrijwillige medewerking aan een vordering tot verstrekking van gegevens. In een vordering waarin *niet* wordt gewezen op het verplichte karakter en de geheimhoudingsplicht, geldt als een vordering waar u vrijwillig aan meewerkt. Wees dus daarvan bewust. Bij medewerking aan een vrijwillige vordering tot verstrekking bent u jegens uw klant makkelijker aansprakelijk omdat u niet wettelijk verplicht was om mee te werken aan de vordering. Bij vordering waarbij u wettelijk verplicht bent mee te werken, kunt u als Cloudbaanbieder bij aansprakelijkstelling eventueel een beroep doen op het verplichte karakter van de vordering, met dien verstande dat altijd de vordering gecontroleerd dient te zijn en de opsporingsambtenaar verzocht wordt om voor Cloudbaanbieder minder ingrijpende wijzen tot verkrijging van gegevens aan te wenden.

3.3 Verstrek nooit zomaar gegevens

Medewerkers mogen nimmer uit eigen beweging gegevens verstrekken aan opsporingsambtenaren en evenmin aan gebruikers over wie gegevens zijn gevorderd. Verstrekking is altijd een kwestie van controleren en afwegen.

3.4 Laat ambtenaar altijd weten dat je niet bevoegd bent te beslissen

Medewerkers die geconfronteerd worden met een vordering dienen in voorkomende gevallen te laten weten dat zij niet bevoegd zijn een dergelijke verzoek te behandelen en verwijzen altijd door naar het hoogst mogelijk niveau (directie).

3.5 Vraag om schriftelijke vordering

Vraag altijd om een adequate schriftelijke vordering waarin het wetsartikel is vermeld waarop de vordering is gebaseerd en zo concreet mogelijk de gegevens die worden gevorderd. Vraag altijd naar de identificatie van degene die de gegevens vraagt/vordert. De vordering moet ook ondertekend zijn door een ambtenaar die de vordering mag en kan ondertekenen. In digitale context is dat een

gekwalificeerde elektronische handtekening. Valideer de gekwalificeerde elektronische handtekening. Zie hiervoor: <https://www.om.nl/onderwerpen/elektronische-handtekening>

3.6 Contacteer altijd directie

Contacteer altijd degene die binnen het bedrijf bevoegd is tot afdoening van vragen van politie en/of justitie, in dit geval de directie. Directie bepaalt of legal dient te worden geraadpleegd.

3.7 Nooit meer verstrekken dan gevorderd

Verstrek -indien daartoe besloten door directie (die eventueel legal heeft geraadpleegd)- nooit meer gegevens dan gevorderd worden. Vraag ook altijd de wijze waarop de gegevens beveiligd kunnen worden verstrekt.

3.8 Leg vast welke stukken worden gevorderd

Maak waar mogelijk kopieën van essentiële stukken die verstrekt zijn maak een lijst van alle verstrekte gegevens. Laat deze als ontvangstbewijs tekenen/bevestigen door de betreffende ambtenaar waarbij ook is opgenomen dat da t de gegevens onder protest zijn verstrekt. .

4 Controle van de vordering¹

4.1 Altijd betrokkenheid en voorafgaande toestemming van de officier van justitie vereist

Hieronder (paragraaf 4.2) is aangegeven bij welke categorie gegevens wiens bevel nodig is. Gebruikersgegevens kunnen worden gevorderd door een opsporingsambtenaar. Voor andere categorie gegevens geldt dat dit enkel kan op bevel van officier van justitie of zelfs met machtiging van de rechter-commissaris. Voor het verkrijgen van gegevens met betrekking tot informatie/gegevens waarbij een partij is met een wettelijk beroepsgeheim betrokken, is altijd de voorafgaande toestemming van de officier van justitie vereist, ook wanneer de wet dat niet voorschrijft. Dat betekent dat ook voor het vorderen van identificerende gegevens (artikel 126nc/uc Sv) en het bevel opgave te doen van gegevens in het kader van een strafrechtelijk financieel onderzoek (artikel 126a Sv) telkens de toestemming van de officier van justitie of zelfs de rechter-commissaris nodig is. Een verzoek die niet door of namens de officier van justitie is gedaan neemt een Cloudaanbieder in behandeling en communiceert terug dat het verzoek niet is gedaan door een daartoe bevoegd orgaan.

Zie hieronder een overzicht van de vordering tot verstrekking van gegevens en de juridische voorwaarden die daaraan zijn verbonden. In geval van Gebruikersgegevens (zie hieronder) geldt dat een opsporingsambtenaar die ook kan vorderen. Voor de overige type gegevens geldt dat een officier van justitie het bevel moet geven. In sommige gevallen en bij inhoudelijke gegevens is er een rechterlijke machtiging nodig.

4.2 Welke gegevens kunnen worden gevorderd en onder welke voorwaarden?

Voor het vorderen van gegevens kunnen de volgende relevante categorieën worden onderscheiden: (1) gebruikersgegevens, (2) verkeersgegevens, (3) andere gegevens en (4) inhoudelijke gegevens.

De tabel verschaft een overzicht van de juridische basis voor de vordering bevoegdheden van gegevens bij een Cloudaanbieder.

Categorie van gegevens	Juridische basis	Type gegevens	Voorwaarden
Gebruikersgegevens	126na Sv	Naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst.	Bevel opsporingsambtenaar.
Verkeersgegevens	126n Sv	Tijd, duur, gebruikte apparatuur, afgenomen diensten en locatiegegevens.	Bevel officier van justitie, in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 Sv.
Andere gegevens	126nd Sv	O.a. betalingsgegevens en profielgegevens, niet zijnde gevoelige gegevens.	Bevel officier van justitie, in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 Sv.

¹ Dit hoofdstuk is vooral voor directie en legal bedoeld. Een gewone medewerker of leek zou de controle niet altijd juist kunnen uitvoeren / doen.

Inhoudelijke
gegevens

126ng lid 2 Sv

Opgeslagen e-mail gegevens. Mogelijk
andere inhoudelijke gegevens, zoals
opgeslagen documenten.

Bevel officier van justitie,
machtiging rechter-commissaris, indien
het onderzoek het dringend vordert en
de rechtsorde wordt geschaad, in
opsporingsonderzoeken naar
misdrijven zoals omschreven in art. 67
Sv.

4.3 Welke informatie moet een vordering bevatten?

De officier van justitie moet buiten de Gebruikersgegevens om altijd vooraf toestemming verlenen voor het vorderen van de andere gegevens, zie tabel hierboven

In de vordering dient - naast de specifieke informatie die op grond van de toepasselijke bepaling van het Wetboek van Strafvordering moet worden opgenomen (zie artikel 152 t/m 159 Sv en hiermee samenhangende richtlijnen en aanwijzingen voor vorderingen) - in ieder geval de volgende informatie te worden opgenomen:

- a) een zo nauwkeurig mogelijke **vermelding van de gegevens** die worden verlangd (zie bijvoorbeeld artikel 126nd lid 3 Sv). Daarbij moet zo duidelijk mogelijk worden aangegeven om welke gegevens het gaat. Protesteer altijd tegen breed geformuleerde vordering tot verstrekking van gegevens.
- b) indien bekend, een nauwkeurige **aanduiding van de persoon of personen** over wie de gegevens worden gevorderd;
- c) de **termijn** waarbinnen en de **wijze** waarop de gegevens dienen te worden verstrekt;
- d) een **verwijzing naar de wettelijke bepaling** op grond waarvan de gegevens worden gevorderd (de titel van de vordering);
- e) de mededeling dat een Cloudaanbieder verplicht is aan de vordering te voldoen. Dit maakt het verschil in een verplichte en vrijwillige medewerking. In een vordering waarin niet wordt gewezen op het verplichte karakter en een geheimhoudingsplicht, geldt als een vordering waar u vrijwillig aan meewerkt (doe evt. een beroep op geheimhouding en verschoningsrecht);
- f) de mededeling dat hij verplicht is om alle informatie omtrent de vordering geheim te houden (beroep geheimhouding en verschoningsrecht).

4.4 Moet er een verdachte genoemd zijn?

In de vordering hoeft niet te worden vermeld op welke verdachte (of veroordeelde) het onderzoek waarin de vordering wordt gedaan betrekking heeft.

De vordering hoeft geen betrekking te hebben op gegevens over de verdachte zelf. Er kunnen ook gegevens worden gevorderd over personen die geen verdachte zijn, zoals blijkt uit de bepalingen in het Wetboek van Strafvordering.

5 De geheimhoudingsplicht en (afgeleid) verschoningsrecht

Er zijn beroepsgroepen die (wettelijk) verplicht zijn tot geheimhouding ten aanzien van al hetgeen waarvan hij uit hoofde van zijn werkzaamheid als zodanig kennis neemt. Dezelfde geheimhoudingsplicht geldt voor de personen die onder zijn verantwoordelijkheid werkzaam zijn of werkzaamheden uitvoeren. In het Wetboek van Strafvordering is aan bepaalde beroepsgroepen op grond van zijn geheimhoudingsplicht een verschoningsrecht toegekend in het geval zij in zaak raken als getuige wordt gehoord. Dit verschoningsrecht werkt door in de toepassing van dwangmiddelen en opsporingsbevoegdheden. Een verschoningsgerechtigde is niet verplicht mee te werken als een vordering in strijd is met zijn geheimhoudingsplicht (artikel 96a lid 3 onder b Sv). Dit geldt ook voor het vorderen van gegevens (bijvoorbeeld artikel 126nd lid 2 Sv). Ook in de bepalingen voor doorzoeking wordt rekening gehouden met de bijzondere positie van partijen met een wettelijke beroepsgeheim op grond van zijn geheimhoudingsplicht (bijvoorbeeld artikel 98 lid 2 Sv). Het advies is: raadpleeg altijd juristen om de vordering te controleren en afwegingen te maken voor al dan niet verstrekking van gegevens.