Ministerie van Justitie en Veiligheid

eEvidence Q&A certificaten

1. Hoe kan ik er zeker van zijn dat het rechtssysteem in EU lidstaten tot een legitieme vordering aan de dienstaanbieder leidt?

De EU is een eigen rechtsgemeenschap met een eigen rechtsstelsel; het zogenoemde EU Acquis. Dat omvat onder andere regels over de eisen waaraan de rechtssystemen van lidstaten moeten voldoen. Uitgangspunt is dat EU lidstaten daarom wederzijds op elkaar vertrouwen. Lidstaten zijn op het niet voldoen aan de EU regels en eisen door de Europese Commissie - en politiek ook in de Raad van Ministers - aan te spreken en zo nodig te beboeten. Op grond daarvan moet erop vertrouwd worden dat een vordering van een justitiële autoriteit uit eender welke EU lidstaat aan de juiste EU breed gedeelde juridische eisen voldoet.

2. Moet of mag de dienstaanbieder de eEvidence vordering juridisch toetsen?

Het Europees recht – inclusief de eEvidence verordening - is in dit opzicht verplichtend naar de dienstaanbieders. De dienstaanbieders hebben op grond van artikel 10 van de verordening de mogelijkheid om op grond van de in dat artikel (limitatief) aangegeven gronden aan de uitvaardigende autoriteit te laten weten dat zij het bevel niet kunnen uitvoeren. Het is vervolgens aan die autoriteit om te beoordelen of het bevel in stand blijft, wordt aangepast of wordt ingetrokken.

3. Op welke manier wordt gecontroleerd of het nieuwe gedecentraliseerde eEvidence systeem juist gebruikt wordt door de lidstaten?

De verordening bevat een opsomming van een hele reeks aan gegevens over het gebruik van het systeem die lidstaten moeten vast leggen en waarover de lidstaten jaarlijks aan de Europese Commissie moeten rapporteren. Eens per jaar brengt deze daarover een rapport uit. Daarnaast wordt de verordening en dus ook het IT-systeem en het gebruik daarvan uiterlijk op 18 augustus 2029 geëvalueerd.

4. Hoe moet een dienstaanbieder omgaan met een vordering waarin vrijwel alle op te vragen typen informatie worden gevorderd?

Omdat het om veel verschillende soorten te vorderen gegevens gaat is dat dan heel lastig te automatiseren. Dan wordt het handwerk.

5. Wordt de oorspronkelijke vordering die ten grondslag ligt aan de eEvidence vordering meegezonden aan de dienstaanbieder?

Nee, een verstrekkingsbevel / bewaringsbevel wordt doorgegeven via een certificaat voor verstrekking (een CEV) of voor bewaring (CEB) volgens artikel 9 van de Verordening en bevat de punten die zijn aangegeven in de artikelen 5, lid 5, punten a) tot en met h) en 6, lid 4, punten a) tot en met f).

6. Voldoe ik wel aan de verplichtingen die de AVG mij stelt als ik een eEvidence vordering beantwoord?

Ja. De eEvidence verordening en de AVG zijn onderdeel van het EU acquis. In de wetgevingsprocedure is het een op het ander afgestemd op basis van adviezen van onder andere de dataprotectie autoriteiten. Artikel 32 van de Verordening formaliseert dat

7. Mag een dienstaanbieder eerder leveren dan de 10 dagen waarin een notificatie beoordeeld moet worden door de tenuitvoerleggende autoriteit?

Nee. De dienstaanbieder moet de tenuitvoerleggende autoriteit tot die 10 dagen de tijd geven om te kunnen interveniëren. Bij uitblijven van een interventie moet de dienstaanbieder na het verstrijken van de 10 dagen meteen leveren.

8. Wat gebeurt er als de tenuitvoerleggende autoriteit op grond van een notificatie weigert?

Dan wordt de dienstaanbieder hierover geïnformeerd. Daarnaast neemt de tenuitvoerleggende autoriteit contact op met de uitvaardigende autoriteit van de andere lidstaat via het decentrale IT-systeem om de weigering door te geven, voorzien van motivatie. De dienstaanbieder hoeft dan niets te doen anders dan het voorkomen van levering van de gevorderde gegevens.

9. Wat zijn de gevolgen voor een dienstaanbieder als deze niet in staat is om vast te stellen of een klant onder de weigeringsgrond voor immuniteiten valt?

Als een dienstaanbieder vanuit de eigen bedrijfsvoering niet over informatie beschikt op grond waarvan blijkt dat de gevorderde gegevens een immuniteit betreft dan kan het deze niet aangerekend worden als het hier onverhoopt toch de gegevens van bijvoorbeeld een verschoningsgerechtigde betreft (artikel 15, lid 2 van de Verordening). Er staat dan niets in de weg om de gegevens te verstrekken.

10. Als een uitvaardigende lidstaat niet over een vergoedingsregeling beschikt krijgt een dienstaanbieder dan op een andere manier de kosten vergoed?

Nee. Er vindt dan net zoals voor de dienstaanbieders in het betreffende nationale stelsel geen vergoeding van de kosten plaats

11. Hoe weet je of een uitvaardigende autoriteit wel bevoegd is om de gevraagde gegevens te vorderen?

Artikel 4 van de verordening geeft een limitatieve opsomming van wie waartoe bevoegd is. Op grond van artikel 31 van de verordening verstrekt iedere lidstaat aan de Commissie de informatie wie in de desbetreffende lidstaat de autoriteiten als bedoeld in artikel 4. In het gedecentraliseerd IT systeem worden die gevens via een zogenoemde bibliotheek ontsloten. Daarbij wordt dan een koppeling gemaakt met de justitiële atlas van het Europees Justitieel Netwerk (EJN) van Eurojust.

12. Hoe worden de passages in de certificaten uit de bijlagen van de verordening tot een logisch werkende boomstructuur of workflow uitgewerkt?

De gegevens en de workflow worden in het gedecentraliseerd IT-systeem verwerkt in een gebruikersinterface.

13. In het weigeringscertificaat moeten de persoonsgegevens van een medewerker van een dienstaanbieder worden vermeld. Het is onwenselijk wanneer dit wordt ingevuld door de uitvoerende medewerker. Hoe hier mee om te gaan?

Een dienstaanbieder kan net als voor de ondertekening van formele brieven e.d. hiervoor een vaste contactpersoon of niet persoonsgebonden authenticatie gebruiken.

14. Komt er een door alle lidstaten te raadplegen naslagwerk bij het gedecentraliseerde IT-systeem om veel voorkomende vragen aan dienstaanbieders over de geleverde of te leveren gegevens af te vangen?

Nee. De bij elke dienstaanbieder te vorderen typen gegevens en de interpretatie daarvan is bedrijfsvertrouwelijke informatie. Het kan vanuit een pragmatisch oogpunt wenselijk kan zijn dat deze informatie centraal beschikbaar is voor alle uitvaardigende autoriteiten. Vanuit beveiligingsoverwegingen is dat echter niet verantwoord. De decentrale opzet van het IT-systeem moet mede daarom borgen dat deze gevoelige gegevens alléén tussen de uitvaardigende autoriteit en de dienstaanbieder uitgewisseld wordt.

15. Moet de dienstaanbieder wachten op een bevestiging van de tenuitvoerleggende autoriteit?	Nee, de verordening kent geen verplichting daartoe.
16. Moet een dienstaanbieder elke lidstaat apart gaan factureren voor de vergoeding van de kosten?	Ja. Als een lidstaat voor het eigen land over een vergoedingsregeling voor lawful disclosure of data beschikt dan kan de dienstaanbieder deze lidstaat factureren volgens die regeling. Er wordt nog uitgezocht op welke manier de dienstaanbieder het best geïnformeerd kan worden over de procedure en factureringsgegevens per lidstaat.
17. Welke consequenties hebben de vergoedingsregelingen in lidstaten voor de implementatie door de dienstaanbieder?	De implementatiekosten van dienstaanbieders om zich voor 2026 voor te bereiden op eEvidence vorderingen worden niet vergoed.
18. Wat moet de dienstaanbieder doen als deze waarneemt dat er slachtofferinformatie van bijvoorbeeld een hack wordt gevorderd?	Deze informatie kan in een open tekstveld meegeleverd worden. De gevorderde informatie moet wel geleverd worden.

19. Wat moet de dienstaanbieder doen als men per ongeluk de verkeerde gegevens heeft geleverd?	Direct de uitvaardigende autoriteit informeren.
20. Is het mogelijk om met lidstaten die de meeste vorderingen aan Nederlandse dienstaanbieders sturen bilaterale procesafspraken te maken over de manier waarop vorderingen worden aangeboden?	de bijhorende vorderingen in het decentrale IT-systeem worden geïmplementeerd zijn leidend.
21. Hoe kan op voorhand bekend zijn bij de uitvaardigende autoriteit welke bewaartermijnen een dienstaanbieder gebruikt voor diens eigen bedrijfsvoering?	Dat kan niet bekend zijn omdat er geen wettelijke bewaartermijn geldt en er ook geen centrale administratie zal worden bijgehouden van welke bewaartermijnen dienstaanbieders in het kader van hun bedrijfsvoering aanhouden.
22. Moet een dienstaanbieder als deze een vordering weigert maar kennis heeft van mogelijk relevante hieraan gerelateerde informatie die doorgeven aan de uitvaardigende autoriteit?	Nee, dat hoeft niet, maar dat mag wel. Een weigering moet gemotiveerd worden en dat tekstveld kan ook gebruikt worden om de uitvaardigende autoriteit verder op weg te helpen.

23. Wat als een vordering van toepassing is op een dienst die ik lever aan een klant die zelf een dienstaanbieder is, een zgn. reseller, en ik geen directe toegang heb tot de gevraagde informatie?

Dat kan afhankelijk van het soort dienst reden voor een weigering zijn waarbij in de toelichting kan worden aangegeven dat de uitvaardigende autoriteit zich tot de andere dienstaanbieder moet richten. Het zonder overleg met de uitvaardigende autoriteit zelf proactief benaderen van de reseller in kwestie kan om onderzoeksredenen onwenselijk zijn.

24. Welke soort boetes kent de eEvidence verordening en richtlijn en onder welke omstandigheden kunnen die door welke partij opgelegd worden?

De tenuitvoerleggende autoriteit kan in het eigen land in het kader van de eEvidence verordening vanuit het strafrecht een boete op leggen aan een dienstaanbieder of deze vervolgen wanneer deze in gebreke blijft. Dat is echter een ultimum remedium. Voordat een strafrechtelijke benadering wordt gekozen is eerst de toezichthouder (in Nederland: de ACM) op de eEvidence richtlijn aan zet. De toezichthouder kan wanneer deze uit een lidstaat een klacht ontvangt over een dienstaanbieder en na eigen onderzoek vanuit het bestuursrecht een boete opleggen.

25. Wat als een Nederlandse dienstaanbieder niet geregistreerd is bij de toezichthouder op de eEvidence richtlijn?

Dan kan een uitvaardigende autoriteit diens gegevens niet vinden in het gedecentraliseerde eEvidence IT-systeem. Deze zal zich vervolgens wenden tot de eigen nationale toezichthouder op de richtlijn die contact zal openen met de dito Nederlandse toezichthouder met het verzoek er voor te zorgen dat de betreffende Nederlandse dienstaanbieder zich alsnog registreert om een eEvidence vordering te kunnen ontvangen.

26. Wat gebeurt er als een vordering voor abonneegegevens gebaseerd is op een vergrijp dat in Nederland niet strafbaar is?

Deze weigeringsgrond kan niet door de dienstaanbieder worden ingeroepen in het geval er abonnee-gegevens of verkeersgegevens, enkel met het doel een persoon te identificeren, worden gevraagd. Alleen voor de vordering van verkeers- en inhoudsgegevens kan een tenuitvoerleggende autoriteit vaststellen of het onderliggende vergrijp in Nederland ook strafbaar is en, als dat niet zo, is de aanwezigheid van dubbele strafbaarstelling als weigeringsgrond inroepen.