Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2022–2023

36 348 Voorstel voor een verordening betreffende vooraf te verstrekken passagiersgegevens met het oog op de controles aan de buitengrenzen I Voorstel voor een verordening betreffende vooraf te verstrekken passagiersgegevens met het oog op het voorkomen van terroristische misdrijven en ernstige criminaliteit

C

BRIEF VAN LID KYRIAKIDES VAN DE EUROPESE COMMISSIE

Aan de voorzitter van de vaste commissie voor Justitie en Veiligheid

Cc: Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Brussel, 7 augustus 2023

De Europese Commissie dankt de Eerste Kamer voor haar advies over het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de verzameling en de doorgifte van vooraf te verstrekken passagiersgegeven (API) met het oog op het versterken en vergemakkelijken van de controles aan de buitengrenzen, tot wijziging van Verordening (EU) 2019/817 en Verordening (EU) 2018/1726, en tot intrekking van Richtlijn 2004/82/EG van de Raad (COM(2022) 729 final) en het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de verzameling en de doorgifte van vooraf te verstrekken passagiersgegevens met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, en tot wijziging van Verordening (EU) 2019/818 (COM(2022) 731 final).

De Commissie heeft alle punten die de Eerste Kamer in haar advies aan de orde stelt, zorgvuldig bestudeerd en wenst de volgende verduidelijkingen onder de aandacht te brengen.

Noodzaak en toegevoegde waarde van de voorstellen

Voortbouwend op de bevindingen van een in 2020 afgeronde evaluatie[1] van de API- richtlijn[2] heeft de Commissie in de gedetailleerde effectbeoor-

[1] Europese Commissie, Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive) (Evaluatie van Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven (API- richtlijn)), 8 september 2020, SWD(2020) 174 (alleen in het Engels beschikbaar).

[2] Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven (hierna «API-richtlijn» genoemd).

kst-36348-C
ISSN 0921 - 7371
's-Gravenhage 2023

deling bij de voorstellen[3] zorgvuldig de noodzaak en de meerwaarde beoordeeld van de in de beide API- voorstellen opgenomen maatregelen.

Grenscontroles

Uit de effectbeoordeling is gebleken dat de wijze waarop de API-richtlijn door de lidstaten wordt uitgevoerd, sterk verschilt. De lidstaten maken onvoldoende gebruik van de huidige API-regels, die slechts op 65% van de vluchten naar het Schengengebied worden toegepast. Zelfs wanneer API-gegevens door de lidstaten worden verzameld, maken nationale autoriteiten geen consistent gebruik van API-gegevens op een wijze die een doeltreffend beheer van de buitengrenzen overeenkomstig de doelstelling van de Schengengrenscode waarborgt[4].

Daarnaast zijn in de API-richtlijn beperkte criteria vastgesteld voor de verzameling, doorgifte en verwerking van API-gegevens. Zo bevat de richtlijn een verplichte maar niet-uitputtende lijst van API-gegevens, met de mogelijkheid voor de lidstaten om aanvullende gegevensvelden op te vragen. De toenemende praktijk van online check-ins heeft ertoe geleid dat de API-gegevens in reisdocumenten steeds vaker handmatig worden ingevoerd door de passagier zelf, wat kan leiden tot onvolledige of onjuiste gegevens die aan de nationale autoriteiten worden doorgegeven. Aangezien API- gegevens in hun huidige vorm minder betrouwbaar worden, hebben de lidstaten minder reden om gebruik te maken van dit voor het overige noodzakelijke instrument.

Bijgevolg wordt niet elke persoon die een buitengrens van het Schengengebied overschrijdt, vooraf aan de hand van API-gegevens gecontroleerd. Dit leidt tot een situatie waarin personen die controles willen omzeilen, routes vermijden waar API- gegevens consequent worden verzameld en in plaats daarvan het Schengengebied proberen binnen te komen via vliegroutes waar API-gegevens minder of niet worden gebruikt.

Dankzij de nieuwe regels zullen API-gegevens over alle personen die per vliegtuig naar het Schengengebied reizen, op doeltreffende en efficiënte wijze aan de grenzen kunnen worden gecontroleerd overeenkomstig de Schengengrenscode.

Preventie, opsporing, onderzoek en vervolging van ernstige misdrijven en terrorisme

Er bestaat een wereldwijde consensus dat passagiersinformatie niet alleen essentiële informatie is voor een doeltreffend grensbeheer, maar ook een belangrijk instrument is om zware criminaliteit en terrorisme te

---

[3] Europese Commissie, alleen in het Engels beschikbaar werkdocument van de diensten van de Commissie, effectbeoordelingsverslag bij het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de verzameling en de doorgifte van vooraf te verstrekken passagiersgegevens (API) met het oog op het versterken en vergemakkelijken van de controles aan de buitengrenzen, tot wijziging van Verordening (EU) 2019/817 en Verordening (EU) 2018/1726, en tot intrekking van Richtlijn 2004/82/EG van de Raad (COM(2022) 729 final) en het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de verzameling en de doorgifte van vooraf te verstrekken passagiersgegevens met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, en tot wijziging van Verordening (EU) 2019/818, SWD(2022) 422.

[4] Verordening (EU) 2016/399 van het Europees Parlement en de Raad van 9 maart 2016 betreffende een Uniecode voor de overschrijding van de grenzen door personen (Schengengrenscode).

bestrijden[5]. De API-voorstellen houden rekening met zowel de internationale ontwikkelingen op het gebied van het gebruik van passagiersinformatie als het door de Unie aangenomen instrument, namelijk de PNR-richtlijn[6], en hebben tot doel de veiligheid van de Unie te verbeteren en de rechtshandhavingsinstanties te voorzien van passende instrumenten om zware criminaliteit en terrorisme te bestrijden.

Het huidige rechtskader van de EU regelt alleen de doorgifte van PNR-gegevens voor de bestrijding van zware criminaliteit en terrorisme, maar doet dit niet specifiek voor API- gegevens, die de lidstaten momenteel alleen kunnen opvragen voor vluchten vanuit derde landen. Dit leidt tot een veiligheidskloof op vluchten binnen de EU, aangezien de lidstaten luchtvaartmaatschappijen alleen kunnen verzoeken PNR-gegevens door te geven.

Alleen het gecombineerde gebruik van API-gegevens – wanneer deze via een geautomatiseerd procedé worden verzameld dat volledige, correcte en betrouwbare gegevens oplevert – en PNR-gegevens kan die leemte opvullen. Door deze combinatie wordt de analytische capaciteit van passagiersinformatie-eenheden (PIE's) vergroot om de identiteit van passagiers te bevestigen wanneer informatie wordt vergeleken met databanken of vooraf vastgestelde criteria, hetgeen de nauwkeurigheid en de algehele doeltreffendheid ervan bij de bestrijding van zware criminaliteit en terrorisme verbetert zonder gevolgen voor reizigersstromen of de privacy van passagiers. Het zou de autoriteiten in staat stellen te bevestigen wie op het vliegtuig reist, waardoor de kloof tussen de aankoop van een ticket en de daadwerkelijke aanwezigheid op een vlucht wordt gedicht. Het zou de autoriteiten ook in staat stellen de op het moment van de reservering verstrekte informatie (d.w.z. de door de reizigers zelf verstrekte PNR-gegevens) te verifiëren en te koppelen aan de informatie die wordt verstrekt bij het inchecken, via een geautomatiseerde en accurate methode, en bij het instappen (d.w.z. API-gegevens).

Gebruik van een router voor de doorgifte en doorzending van API-gegevens

Met de voorstellen zou één router worden opgezet als één toegangspunt op EU-niveau, dat zou worden ontwikkeld en beheerd door het Agentschap van de Europese Unie voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA) en onder toezicht zou staan van de Europese Toezichthouder voor gegevensbescherming (EDPS). Enerzijds zal de router aanzienlijke efficiëntiewinst opleveren voor luchtvaartmaatschappijen wat betreft hun verbindingen met de lidstaten (1 toegangspunt in plaats van 27). Anderzijds zal de router ook voordelen opleveren voor de lidstaten (1 verbinding met alle luchtvaartmaatschappijen die vluchten uitvoeren). De router zou in wezen fungeren als één enkel punt voor de ontvangst en verdere verspreiding van API-gegevens.

---

[5] Sinds 2014 hebben de internationale gemeenschap en de resoluties van de Veiligheidsraad van de Verenigde Naties herhaaldelijk opgeroepen tot het gebruik van zowel voorafgaande passagiersgegevens als persoonsgegevens van passagiers (PNR-gegevens) voor veiligheidsdoeleinden. Zie Resoluties 2178(2014), 2309(2016), 2396(2017) en 2482(2019) van de VN-Veiligheidsraad, alsmede Besluit 6/16 van de ministerraad van de OVSE van 9 december 2016 over een intensiever gebruik van op voorhand af te geven passagiersgegevens.

[6] Richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit (PNR-richtlijn).

De «ontvangst» van de gegevens door de router en de doorzending aan de nationale autoriteiten zouden een beperkte verwerking zijn, die in de voorstellen gedetailleerd wordt geregeld, waarbij de gegevens alleen via de router – zonder dat deze toegang heeft tot persoonsgegevens – passeren totdat zij de databanken in de lidstaten bereiken.

Zodra de doorzending van de gegevens is voltooid, worden de gegevens onmiddellijk en automatisch gewist. In de praktijk is het een kwestie van seconden vanaf het moment dat de router gegevens uit de databanken van luchtvaartmaatschappijen ontvangt en deze doorstuurt naar de databanken van de autoriteiten van de lidstaten. Voor het gegevensverkeer via de router zal er geen gebruik worden gemaakt van instrumenten voor artificiële intelligentie, in overeenstemming met de taak van de router om de naar de nationale autoriteiten doorgezonden reeksen API-gegevens niet te wijzigen.

Voor de ontwikkeling van de router door eu-LISA zou worden voortgebouwd op ervaring die eu-LISA heeft opgedaan bij de bouw van centrale componenten en op delen van de technische infrastructuur die het Agentschap heeft ontwikkeld voor andere EU-systemen, namelijk het inreis-uitreissysteem (EES) en het Europees reisinformatie- en -autorisatiesysteem (Etias). Deze systemen voorzien in een webdienst voor vervoerders (toegangsportaal voor vervoerders), met inbegrip van luchtvaartmaatschappijen, waarmee deze laatste verbinding zouden moeten maken. Voor die systemen heeft eu-LISA de hoogste normen op het gebied van IT-beveiliging toegepast en heeft het voorzien in een uitgebreide reeks beveiligingsmaatregelen, waaronder EU-normen voor cyberbeveiliging die vereist zijn om certificaten voor vervoerders in te voeren in plaats van een vooraf gedeelde sleutel, teneinde de meest strikte toegangsregeling tot stand te brengen en voortaan het risico op cyberaanvallen aanzienlijk te verminderen. Wat het inreis-uitreissysteem en de toegangspoorten van het Europees reisinformatie- en -autorisatiesysteem betreft, zouden specifieke beveiligingsvereisten voor de API-router nader worden uitgewerkt in de overeenkomstige gedelegeerde handelingen met betrekking tot de doorgifte en doorzending van API-gegevens via de router.

Daarnaast omvatten de voorstellen van de Commissie een volledige reeks monitoringmaatregelen om de belangrijkste belanghebbenden te ondersteunen bij het beoordelen van de doeltreffendheid van de verzameling van API-gegevens: verslagen en statistieken zullen worden verstrekt aan de grens- en rechtshandhavingsautoriteiten van de lidstaten, het Europees Parlement, de Raad, de Commissie, eu-LISA, Frontex en de EDPS, met een passend niveau van granulariteit, vertrouwelijkheid en regelmatigheid. De statistieken zouden met name voortbouwen op het bij de interoperabiliteitsverordeningen ingevoerde gemeenschappelijk register voor verslagen en statistieken[7].

[7] Verordening (EU) 2019/817 van het Europees Parlement en de Raad van 20 mei 2019 tot vaststelling van een kader voor interoperabiliteit tussen de Unie-informatiesystemen op het gebied van grenzen en visa en tot wijziging van Verordeningen (EG) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 en (EU) 2018/1861 van het Europees Parlement en de Raad, Beschikking 2004/512/EG van de Raad en Besluit 2008/633/JBZ van de Raad; en Verordening (EU) 2019/818 van het Europees Parlement en de Raad van 20 mei 2019 tot vaststelling van een kader voor interoperabiliteit tussen de Unie-informatiesystemen op het gebied van politiële en justitiële samenwerking, asiel en migratie en tot wijziging van Verordeningen (EU) 2018/1726, (EU) 2018/1862 en (EU) 2019/816.

Impact op het recht op bescherming van persoonsgegevens

De API-voorstellen van de Commissie bevatten strenge beperkingen en waarborgen op het gebied van de bescherming van persoonsgegevens, die het resultaat zijn van een grondige beoordeling van de gevolgen voor de reizigers.

De opslag van gegevens door luchtvaartmaatschappijen en bevoegde autoriteiten verschilt in de beide voorstellen op basis van het doel van de verzameling van de gegevens. Voor grensbeheerdoeleinden werd de opslag van de gegevens bepaald op basis van de bestaande regels voor opslag in de API-richtlijn en de analyse van de operationele behoeften van de nationale autoriteiten, alsook de gevolgen voor het recht op bescherming van persoonsgegevens. De API-gegevens die de PIE's uit hoofde van het rechtshandhavingsvoorstel ontvangen, zouden door de PIE's worden verwerkt overeenkomstig de desbetreffende bepalingen van de PNR-richtlijn, die de uitlegging van die regels door het Hof van Justitie omvat.

Verenigbaarheid met ander recht

In zijn arrest in zaak C-817/19[8] bevestigde het Hof van Justitie de geldigheid van alle bepalingen van de PNR-richtlijn. Het Hof achtte geen daarvan onverenigbaar met het primaire recht van de Unie en bijgevolg is er geen juridische noodzaak voor de medewetgever om een stuk wetgeving te wijzigen dat van toepassing blijft.

Tegelijkertijd heeft het Hof een uitlegging gegeven van de vereisten waaraan de lidstaten moeten voldoen voor de doorgifte en verwerking van PNR-gegevens. De Commissie volgt nauwlettend de wijze waarop de lidstaten hun PNR-systemen en, in voorkomend geval, hun nationale omzettingswetgeving aanpassen aan de uitlegging van het Hof van de PNR-richtlijn.

Het voorgestelde API-rechtshandhavingsinstrument is uitsluitend gericht op de verzameling en de doorgifte van API-gegevens door luchtvaartmaatschappijen, met als doel de verzameling van API-gegevens aan te vullen om het gebruik van PNR-gegevens in het kader van de PNR-richtlijn te versterken. Bijgevolg blijven alle aspecten die door de PNR-richtlijn worden geregeld, ongewijzigd, met inbegrip van de regels inzake de verwerking van PNR-gegevens en API-gegevens door de PIE's van de lidstaten.

De voorstellen van de Commissie brengen derhalve geen wijzigingen in de PNR-richtlijn aan en vormen in plaats daarvan een specifieke aanvulling op de regels inzake de doorgifte van API-gegevens. Bijgevolg zouden de autoriteiten van de lidstaten (PIE's) geen systematische API-gegevens ontvangen voor alle vluchten binnen de EU, tenzij zij de noodzaak van de verzameling van dergelijke gegevens kunnen rechtvaardigen (deze noodzaak moet regelmatig worden herzien, zoals vereist door het Hof). De router zou ervoor zorgen dat de doorzending van API-gegevens aan de PIE's voldoet aan de vereisten van het Hof, en tegelijkertijd tegemoetkomen aan de operationele behoeften van de lidstaten en het recht van luchtvaartmaatschappijen om te ondernemen. De doorzending via de router naar de PIE's is opgezet als een technische oplossing om de doorzending van API-gegevens naar passagiersinformatie-eenheden te beperken tot geselecteerde vluchten,

[8] Arrest van het Hof van Justitie van 21 juni 2022, Ligue des droits humains ASBL tegen ministerraad, C- 817/19, ECLI:EU:C:2022:491.

zonder dat vertrouwelijke informatie wordt bekendgemaakt over welke vluchten binnen de EU zijn geselecteerd.

Zoals bevestigd in het advies van de EDPS bestaat er geen andere oplossing die ervoor kan zorgen dat alleen API-gegevens van geselecteerde vluchten binnen de EU door de PIE's worden ontvangen en verder worden verwerkt, waarbij die vertrouwelijkheid wordt gewaarborgd en geen onevenredige operationele lasten voor luchtvaartmaatschappijen worden gecreëerd[9].

Selectiecriteria voor vluchten binnen de EU

Het Hof van Justitie heeft in dezelfde zaak C-817/19 geoordeeld dat lidstaten die besloten hebben PNR-gegevens te verzamelen over vluchten binnen de EU, zoals bepaald in artikel 2 van de PNR-richtlijn, dit alleen mogen doen voor zover dat strikt noodzakelijk is voor de verwezenlijking van de doelstellingen van die richtlijn.

Het Hof oordeelde dat PNR-gegevens alleen mogen worden doorgegeven en verwerkt voor alle vluchten binnen de EU indien uit een beoordeling van de lidstaat blijkt dat er sprake is van een werkelijke en actuele of voorzienbare terroristische dreiging. Bij gebreke van een dergelijke bedreiging is de doorgifte van PNR-gegevens aan de PIE's en de daaropvolgende verwerking van dergelijke gegevens alleen gerechtvaardigd voor bepaalde vluchten binnen de EU die door de lidstaten moeten worden geselecteerd op basis van hun dreigingsevaluaties. In beide gevallen heeft het Hof vereist dat het resultaat van de beoordeling, en dus van de selectie van de vluchten, regelmatig wordt herzien. Het Hof heeft geen richtsnoeren verstrekt over de criteria voor een dergelijke dreigingsevaluatie. Het heeft de lidstaten met deze belangrijke taak belast, waarvan de correcte uitvoering onderworpen blijft aan het toezicht van de bevoegde nationale gegevensbeschermingsautoriteiten.

De regels voor de verzameling en de doorgifte van API-gegevens over vluchten binnen de EU die zijn vastgesteld in het voorstel van de Commissie voor de verzameling en de doorgifte van API-gegevens voor zware criminaliteit en terrorisme, zijn gebaseerd op de nationale dreigingsevaluatie voor de selectie van vluchten binnen de EU die lidstaten moeten uitvoeren, als onderdeel van de uitvoering van artikel 2 van de PNR-richtlijn en in overeenstemming met de vereisten van het arrest van het Hof.

Bijgevolg, en als gevolg van de dreigingsevaluatie en de selectie van vluchten binnen de EU die door de nationale autoriteiten moet worden uitgevoerd, zou de router de opdracht krijgen om API-gegevens door te geven aan de bevoegde autoriteiten van de lidstaten indien een vlucht wordt geselecteerd, of om API-gegevens over niet- geselecteerde vluchten binnen de EU onmiddellijk en automatisch te wissen.

---

[9] Europese Toezichthouder voor gegevensbescherming, Opinion 6/2023 on the Proposals for Regulations on the collection and transfer of advance passenger information (API) (Advies 6/2023 over de voorstellen voor verordeningen betreffende de verzameling en de doorgifte van vooraf te verstrekken passagiersgegevens (API)), 8 februari 2023, punten 20–21 (alleen in het Engels beschikbaar).

De Europese Commissie hoopt dat zij met de toelichting in dit antwoord voldoende is ingegaan op de door de Eerste Kamer aan de orde gestelde punten en zij kijkt ernaar uit de politieke dialoog in de toekomst voort te zetten.

Lid van de Commissie,
Stella Kyriakides

Bijlage

De Commissie heeft alle aanvullende vragen van de Eerste Kamer zorgvuldig bestudeerd en wenst de volgende verduidelijkingen onder de aandacht te brengen.

1) De Commissie houdt rekening met de inbreng van alle relevante belanghebbenden en adviesorganen. De standpunten die naar voren zijn gebracht in het gezamenlijk advies van het Europees Comité voor gegevensbescherming (EDPB)/de Europese Toezichthouder voor gegevensbescherming (EDPS) en in het advies van de Juridische Dienst van de Raad, zijn aan de orde gesteld in de documenten die de diensten van de Commissie op respectievelijk 8 februari 2023 en 17 mei 2023 aan het secretariaat van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement hebben toegezonden. Het is nu in de eerste plaats aan het Europees Parlement en de Raad, als medewetgevers van de EU, om het voorstel te bespreken en hun standpunt te bepalen.

2) Veeleer dan het begrip «benaderen van kinderen» (ook wel «grooming» genoemd) te definiëren verwijst het voorstel naar de definitie in Richtlijn 2011/93/EU ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie[10]. Artikel 6 van de richtlijn verplicht de lidstaten tot het strafbaar stellen van «het doen van een voorstel door middel van informatie- en communicatietechnologie, door een volwassene aan een kind dat nog niet seksueel meerderjarig is, tot ontmoeting met het oogmerk om [met dat kind seksuele handelingen aan te gaan of materiaal betreffende seksueel misbruik van kinderen te vervaardigen] voor zover dit voorstel is gevolgd door materiële handelingen die tot een dergelijke ontmoeting leiden», alsook van elke «poging door middel van informatie- en communicatietechnologie om [materiaal betreffende seksueel misbruik van kinderen te verwerven, in bezit te hebben of zich toegang tot dergelijk materiaal te verschaffen], door een volwassene die een kind benadert dat nog niet seksueel meerderjarig is met het oogmerk [materiaal betreffende seksueel misbruik van kinderen] te verschaffen waarin dat kind wordt afgebeeld».

De in artikel 6 van de richtlijn omschreven strafbare feiten vormen een voor alle lidstaten geldende bindende minimumnorm op het gebied van de strafbaarstelling van grooming in de Europese Unie. Aangezien in het voorstel naar deze minimumnorm wordt verwezen, kan de definitie van grooming in het kader van het voorstel niet ruimer zijn dan die welke is vastgelegd in de nationale rechtsstelsels, met inbegrip van het Nederlandse.

3) Bijgevolg is de Commissie van mening dat er in de hele EU een duidelijke en uniforme minimumnorm bestaat met betrekking tot de definitie van grooming. Hierbij dient te worden opgemerkt dat het voorstel aanbieders niet verplicht om te bepalen of een bepaalde gedraging volgens artikel 6 van Richtlijn 2011/93/EU neerkomt op grooming. De taak om dat te beoordelen is en blijft voorbehouden aan de rechtshandhavingsinstanties in het kader van onderzoeken en, in laatste instantie, aan de rechterlijke macht in het kader van strafprocedures. Aanbieders moeten alleen – als zij daartoe door een rechter of een onafhankelijke administratieve autoriteit worden gelast – potentiële gevallen van grooming opsporen op basis van de uitputtende lijst van indicatoren die hun wordt verstrekt door het EU-centrum ter voorkoming en bestrijding van seksueel misbruik van kinderen (hierna «het

[10] https://eur-lex.europa.eu/eli/dir/2011/93

EU-centrum» genoemd). Met andere woorden: de bepalingen over de opsporing van grooming door aanbieders zijn bedoeld om ervoor te zorgen dat deze aanbieders, net als aanbieders van offlinediensten, verantwoordelijkheid nemen voor het kindveilig houden van hun diensten en het melden van mogelijke illegale activiteiten op hun diensten. Aanbieders worden niet verplicht de onwettigheid van de opgespoorde gedragingen te beoordelen. Het EU-centrum moet overigens als filter fungeren zodat de rechtshandhavingsinstanties niet worden overspoeld met kennelijk ongegronde meldingen.

4) Het begrip «waarschijnlijk» in artikel 7, lid 6, punt a), en lid 7, punt b), maakt het voor de bevoegde coördinerende autoriteit mogelijk om aan de hand van de voorwaarden van de voorgestelde verordening en in het licht van de specifieke kenmerken van de betrokken dienst geval per geval te bepalen of er een significant risico bestaat dat een dienst wordt gebruikt voor online seksueel misbruik van kinderen. Dit helpt om, mede in het licht van het voorafgaande risicobeoordelings- en risicobeperkingsproces, voor elk specifiek geval een evenredige en evenwichtige oplossing te vinden.

Hoe waarschijnlijk het is dat een dienst wordt gebruikt voor online seksueel misbruik van kinderen, hangt in de praktijk grotendeels af van de doeltreffendheid van de risicobeperkende maatregelen die zijn genomen om belemmeringen te creëren voor mogelijke plegers van online seksueel misbruik (bijvoorbeeld via functionaliteiten die contact tussen volwassenen en niet-verwante kinderen voorkomen) en om beschermingslagen te creëren rond kinderen die het doelwit van dergelijk misbruik kunnen zijn (bijvoorbeeld via bewustmakings- en educatieve instrumenten, instrumenten voor ouderlijk toezicht en beschermende afscherm- en filterfuncties). Indien dat passend en nuttig wordt geacht, is de Commissie bereid de medewetgever te helpen bij het nader omschrijven van de begrippen «waarschijnlijk» en/of «significant risico».

5) Het voorstel om het EU-centrum op te richten heeft precies tot doel de uitvoering van het voorstel door alle relevante actoren te vergemakkelijken. Dat het EU-centrum een faciliterende rol heeft, blijkt uit de taken van het centrum op het gebied van ondersteuning van de aanbieders gedurende het hele opsporings- en meldingsproces en op het gebied van overleg met de coördinerende autoriteiten. Het EU-centrum zal binnen dit wetgevingskader het personeel en de organisatievorm krijgen die het nodig heeft om alle meldingen te verwerken en zijn faciliterende taken uit te voeren.

Het voorstel verplicht de coördinerende autoriteiten niet om meldingen van seksueel misbruik van kinderen te verwerken. Deze autoriteiten krijgen passende termijnen om de risicobeoordeling en de risicobeperkende maatregelen te evalueren en te beslissen of ze om de uitvaardiging van opsporingsbevelen moeten verzoeken. Aangezien ze geen meldingen van mogelijk online seksueel misbruik van kinderen hoeven te verwerken, zijn hun activiteiten minder tijdgevoelig dan de meldingen van aanbieders en de verdere verwerking van de meldingen door het EU-centrum. Het aantal meldingen dat aanbieders naar aanleiding van hun opsporingsactiviteiten indienen bij het EU-centrum, heeft dan ook geen rechtstreeks effect op de coördinerende autoriteiten.

Aanbieders waartegen een opsporingsbevel is uitgevaardigd, zullen tijdens de betrokken periode voor hun opsporingswerk geautomatiseerde technologieën inzetten (met inachtneming van een reeks waarborgen) en gebruikmaken van de uitputtende lijst van indicatoren die hun door het EU-centrum wordt verstrekt. Voor het melden van mogelijk online

seksueel misbruik van kinderen op hun diensten moeten ze het model in bijlage III bij het voorstel gebruiken. De meeste handelingen voor het doen van meldingen worden dus onmiddellijk en voor een deel via geautomatiseerde instrumenten uitgevoerd, weliswaar met menselijk toezicht op de werking van die instrumenten en, waar nodig, met menselijke tussenkomst.

Gezien het bovenstaande acht de Commissie het onwaarschijnlijk dat vertraging zal ontstaan wegens problemen bij de behandeling van meldingen door de coördinerende autoriteiten, het EU-centrum of aanbieders.