



Brussel, 15.1.2024
COM(2024) 7 final

**VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE
RAAD**

**over de eerste evaluatie van de adequaatheidsbesluiten die zijn vastgesteld op grond van
artikel 25, lid 6, van Richtlijn 95/46/EG**

{SWD(2024) 3 final}

1. DE EERSTE EVALUATIE — ACHTERGROND EN CONTEXT

Dit verslag bevat de bevindingen van de Commissie over de eerste evaluatie van de adequaatheidsbesluiten die zijn vastgesteld op grond van artikel 25, lid 6, van Richtlijn 95/46/EG¹ (gegevensbeschermingsrichtlijn).

In deze besluiten heeft de Commissie vastgesteld dat elf landen of gebieden een passend beschermingsniveau waarborgen voor persoonsgegevens die vanuit de Europese Unie (EU) worden doorgegeven²: Andorra³, Argentinië⁴, Canada (voor commerciële exploitanten)⁵, de Faeröer⁶, Guernsey⁷, Man⁸, Israël⁹, Jersey¹⁰, Nieuw-Zeeland¹¹, Zwitserland¹², en Uruguay¹³. Als gevolg hiervan zijn er voor de doorgifte van gegevens vanuit de EU naar deze landen of gebieden geen aanvullende eisen nodig.

Met de inwerkingtreding van Verordening (EU) 2016/679¹⁴ (AVG) op 25 mei 2018 bleven de adequaatheidsbesluiten die krachtens de gegevensbeschermingsrichtlijn waren vastgesteld, van

¹ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281 van 23.11.1995, blz. 31).

² Sinds de opname ervan in de Overeenkomst betreffende de Europese Economische Ruimte (EER-overeenkomst) is de AVG ook van toepassing op Noorwegen, IJsland en Liechtenstein. Verwijzingen naar de EU in dit verslag moeten worden begrepen als verwijzingen die ook de EER-staten bestrijken.

³ Besluit 2010/625/EU van de Commissie van 19 oktober 2010 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, over de passende bescherming van persoonsgegevens in Andorra (PB L 277 van 21.10.2010, blz. 27).

⁴ Beschikking 2003/490/EG van de Commissie van 30 juni 2003 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de passende bescherming van persoonsgegevens in Argentinië (PB L 168 van 5.7.2003, blz. 19).

⁵ Beschikking 2002/2/EG van de Commissie van 20 december 2001 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming van persoonsgegevens geboden door de Canadese Personal Information Protection and Electronic Documents Act (PB L 2 van 4.1.2002, blz. 13).

⁶ Besluit 2010/146/EU van de Commissie van 5 maart 2010 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, over de gepastheid van de door de Faeröerse wet betreffende de verwerking van persoonsgegevens geboden bescherming (PB L 58 van 9.3.2010, blz. 17).

⁷ Beschikking 2003/821/EG van de Commissie van 21 november 2003 over de passende bescherming van persoonsgegevens op Guernsey (PB L 308 van 25.11.2003, blz. 27).

⁸ Beschikking 2004/411/EG van de Commissie van 28 april 2004 over de passende bescherming van persoonsgegevens op het eiland Man (PB L 151 van 30.4.2004, blz. 48).

⁹ Besluit 2011/61/EU van de Commissie van 31 januari 2011 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, over de passende bescherming van persoonsgegevens door de staat Israël wat de geautomatiseerde verwerking van persoonsgegevens betreft (PB L 27 van 1.2.2011, blz. 39).

¹⁰ Beschikking 2008/393/EG van de Commissie van 8 mei 2008 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de passende bescherming van persoonsgegevens in Argentinië (PB L 138 van 28.5.2008, blz. 21).

¹¹ Uitvoeringsbesluit 2013/65/EU van de Commissie van 19 december 2012 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, over de passende bescherming van persoonsgegevens in Nieuw-Zeeland (PB L 28 van 30.1.2013, blz. 12).

¹² Beschikking 2000/518/EG van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de passende bescherming van persoonsgegevens in Zwitserland (PB L 215 van 25.08.2000, blz. 1).

¹³ Uitvoeringsbesluit 2012/484/EU van de Commissie van 21 augustus 2012 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, over de passende bescherming van persoonsgegevens door de Republiek ten oosten van de Uruguay wat de geautomatiseerde verwerking van persoonsgegevens betreft (PB L 227 van 23.8.2012, blz. 11).

¹⁴ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het

kracht¹⁵. Tegelijkertijd heeft de AVG verduidelijkt dat adequaatheidsbesluiten “levende instrumenten” zijn, en bepaald dat de Commissie doorlopend toezicht moet houden op ontwikkelingen in derde landen die mogelijk gevolgen hebben voor het functioneren van bestaande adequaatheidsbesluiten¹⁶. Bovendien vereist artikel 97 AVG dat de Commissie deze besluiten om de vier jaar evalueert om te bepalen of de landen en gebieden waarvoor een passend beschermingsniveau is vastgesteld, nog steeds een passend beschermingsniveau voor persoonsgegevens waarborgen.

Deze eerste evaluatie van de adequaatheidsbesluiten die zijn vastgesteld op grond van het vroegere EU-kader voor gegevensbescherming, is uitgevoerd in het kader van een bredere evaluatie van de toepassing en werking van de AVG, waarover de Commissie haar bevindingen heeft gepresenteerd in haar mededeling “Gegevensbescherming als pijler van zeggenschap van de burger en de EU-aanpak van de digitale transformatie — twee jaar toepassing van de algemene verordening gegevensbescherming”¹⁷. De afronding van dit aspect van de evaluatie werd echter uitgesteld om rekening te houden met het arrest van het Hof van Justitie in de zaak *Schrems II*¹⁸, waarin het Hof belangrijke verduidelijkingen over belangrijke elementen van de adequaatheidsnorm heeft gegeven, en met andere gerelateerde ontwikkelingen. Dit heeft op zijn beurt geleid tot gedetailleerde uitwisselingen met de betrokken landen en gebieden over relevante aspecten van hun rechtskader, toezichtmechanismen en handhavingssysteem¹⁹. In dit verslag wordt ten volle rekening gehouden met al deze ontwikkelingen, zowel in de EU als in de betrokken derde landen en gebieden.

Belangrijk is dat deze eerste evaluatie plaatsvindt tegen de achtergrond van de exponentiële ontwikkeling van digitale technologieën. In de afgelopen decennia is het belang van adequaatheidsbesluiten aanzienlijk toegenomen, omdat gegevensstromen een integraal onderdeel zijn geworden van de digitale transformatie van de samenleving en de globalisering van de economie. De grensoverschrijdende overdracht van gegevens is onderdeel geworden van de dagelijkse activiteiten van Europese ondernemingen, groot en klein en in alle sectoren. Meer dan ooit is eerbiediging van de privacy een voorwaarde voor stabiele, veilige en concurrerende handelsstromen. In die context spelen adequaatheidsbesluiten op vele manieren een steeds belangrijker rol. Door te waarborgen dat de bescherming zich samen met de

vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

¹⁵ Zie artikel 45, lid 9, AVG, waarin wordt bepaald dat besluiten die de Commissie op grond van artikel 25, lid 6, van Richtlijn 95/46/EG heeft vastgesteld, van kracht blijven totdat zij worden gewijzigd, ingetrokken of vervangen bij een overeenkomstig artikel 45, lid 3 of lid 5 vastgesteld besluit van de Commissie.

¹⁶ Artikel 45, lid 4, AVG. Zie ook het arrest van het Hof van Justitie van de Europese Unie van 6 oktober 2015 in zaak C-362/14, Maximilian Schrems/Data Protection Commissioner (“*Schrems I*”), ECLI:EU:C:2015:650, punt 76.

¹⁷ De mededeling is gepubliceerd in juni 2020 en kan worden geraadpleegd op: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en

¹⁸ Arrest van het Hof van Justitie van de Europese Unie van 16 juli 2020 in zaak C-311/18, Data Protection Commissioner/Facebook Ireland Ltd en Maximilian Schrems (“*Schrems II*”), ECLI:EU:C:2020:559.

¹⁹ Het adequaatheidsbesluit betreffende Japan is vastgesteld op basis van de AVG en voorziet in een afzonderlijke periodieke evaluatie. De eerste evaluatie is in april 2023 afgerond met het verslag van de Commissie aan het Europees Parlement en de Raad over de eerste evaluatie van de werking van het adequaatheidsbesluit voor Japan (COM(2023) 275 final), dat kan worden geraadpleegd op <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=COM:2023:275:FIN>

gegevens verplaatst, maken ze veilige gegevensstromen mogelijk, waarbij de rechten van individuen worden geëerbiedigd in overeenstemming met de mensgerichte aanpak van de digitale transformatie door de Europese Unie. Door te erkennen dat het privacykader van een derde land een beschermingsniveau biedt dat in grote lijnen overeenkomt met dat van de EU, bevorderen ze de afstemming van privacysystemen die zijn gebaseerd op hoge beschermingsnormen. Bovendien zijn de adequaatheidsbesluiten, zoals in dit verslag wordt uitgelegd, niet zozeer een “eindpunt” als wel de basis voor nauwere samenwerking en verdere afstemming van de regelgeving tussen de EU en gelijkgestemde partners. Door het vrije verkeer van persoonsgegevens mogelijk te maken, hebben deze besluiten handelskanalen geopend voor EU-bedrijven, onder meer door de voordelen van handelsovereenkomsten aan te vullen en te versterken en de samenwerking met buitenlandse partners op een groot aantal regelgevingsgebieden te vergemakkelijken. Doordat deze besluiten een eenvoudige en allesomvattende oplossing bieden voor de doorgifte van gegevens zonder dat de gegevensexporteur verdere waarborgen hoeft te bieden of toestemming hoeft te verkrijgen, wordt het voor met name kleine en middelgrote ondernemingen gemakkelijker om de vereisten voor internationale doorgifte van de AVG na te leven. Tot slot zijn adequaatheidsbesluiten van de Europese Commissie dankzij hun “netwerkeffect” ook steeds relevanter buiten de EU, omdat ze niet alleen het vrije verkeer van gegevens met de dertig economieën van de EU mogelijk maken, maar ook met veel meer rechtsgebieden over de hele wereld²⁰ die landen waarvoor een adequaatheidsbesluit van de EU bestaat, erkennen als “veilige bestemmingen” onder hun eigen regels voor gegevensbescherming.

Om al deze redenen, zoals ook bevestigd door de intensieve en vruchtbare dialoog met de betrokken derde landen/gebieden die aan deze evaluatie ten grondslag ligt, zijn adequaatheidsbesluiten een strategisch onderdeel geworden van de algemene betrekkingen van de EU met deze buitenlandse partners en worden zij erkend als een belangrijke stimulans voor het verdiepen van de samenwerking op een groot aantal gebieden. Het is daarom bijzonder belangrijk dat deze besluiten de tand des tijds kunnen doorstaan en kunnen aanknopen bij nieuwe ontwikkelingen en uitdagingen.

2. VOORWERP EN METHODOLOGIE VAN DE EVALUATIE

De adequaatheidsbesluiten die het voorwerp uitmaken van deze evaluatie, zijn vastgesteld op grond van het EU-kader voor gegevensbescherming dat voorafging aan de AVG. Terwijl de meest recente besluiten dateren van ongeveer tien jaar geleden (bijvoorbeeld de besluiten over Nieuw-Zeeland en Uruguay, beide vastgesteld in 2012), zijn andere al meer dan twintig jaar van kracht (bijvoorbeeld Canada, vastgesteld in 2001, en Zwitserland, vastgesteld in 2000). Sindsdien zijn de kaders voor gegevensbescherming in alle elf landen en gebieden verder geëvolueerd, bijvoorbeeld als gevolg van hervormingen in de wet- en regelgeving, ontwikkelingen in de handhavingspraktijk van gegevensbeschermingsautoriteiten of rechtspraak.

Bij de uitvoering van haar evaluatie heeft de Commissie zich daarom gericht op de ontwikkelingen in het gegevensbeschermingskader van de betrokken landen en gebieden die

²⁰ Zoals Argentinië, Colombia, Israël, Marokko, Zwitserland en Uruguay.

hebben plaatsgevonden sinds de vaststelling van het adequaatheidsbesluit. Beoordeeld is hoe deze ontwikkelingen het gegevensbeschermingslandschap van het betreffende land of gebied verder hebben gevormd en of de verschillende stelsels in het licht van deze ontwikkelingen nog steeds een passend beschermingsniveau waarborgen.

Daartoe is ten volle rekening gehouden met de ontwikkeling van het eigen stelsel voor gegevensbescherming van de EU, in het bijzonder met de inwerkingtreding van de AVG. Met name sinds de vaststelling van deze adequaatheidsbesluiten zijn de wettelijke norm die van toepassing is op dergelijke besluiten en de elementen die relevant zijn om te beoordelen of een buitenlands systeem een passend beschermingsniveau waarborgt, verder verduidelijkt door de rechtspraak van het Hof van Justitie en de richtsnoeren die zijn vastgesteld door de Groep gegevensbescherming artikel 29 en zijn opvolger, het Europees Comité voor gegevensbescherming²¹ (EDPB).

Met name heeft het Hof van Justitie in zijn arrest van 6 oktober 2015 in de zaak *Schrems I* vastgesteld dat weliswaar niet kan worden verlangd dat een derde land waarborgen voor hetzelfde beschermingsniveau als dat binnen de Unie biedt, maar dat de adequaatheidstoets zo moet worden opgevat dat die een beschermingsniveau vereist dat “in grote lijnen overeenkomt” met dat van de Unie²². Met name kunnen de middelen waarmee het derde land in kwestie voor de bescherming van de persoonsgegevens kan zorgen, anders zijn dan de middelen die binnen de Unie worden ingezet, zolang zij in de praktijk doeltreffend genoeg blijken om een passend beschermingsniveau te waarborgen²³. De adequaatheidstoets vereist daarom een alomvattende beoordeling van het systeem van het derde land als geheel, met inbegrip van de inhoud van de privacybescherming, de doeltreffende uitvoering en handhaving ervan.

Bovendien verduidelijkte het Hof dat de beoordeling van de Commissie niet beperkt mag blijven tot het algemene gegevensbeschermingskader van het derde land, maar ook betrekking moet hebben op de regels inzake de toegang tot persoonsgegevens door overheidsinstanties, met name voor doeleinden van rechtshandhaving en nationale veiligheid²⁴. Met het Handvest van de grondrechten als maatstaf heeft het Hof verschillende vereisten vastgesteld waarmee deze regels in overeenstemming moeten zijn om aan de norm van “wezenlijke overeenkomst” te voldoen. Een regeling op dit gebied moet bijvoorbeeld duidelijke en precieze regels betreffende de draagwijdte en de toepassing van een maatregel bevatten en minimale vereisten opleggen, zodat de personen van wie de persoonsgegevens aan de orde zijn, over voldoende garanties beschikken dat hun gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens²⁵. Een dergelijke regeling moet ook voorzien in een beroepsmogelijkheid voor

²¹ Het Europees Comité voor gegevensbescherming bestaat uit de toezichthoudende autoriteiten voor gegevensbescherming in de lidstaten en de Europese Toezichthouder voor gegevensbescherming.

²² *Schrems I*, punten 73, 74 en 96. Zie ook overweging 104 van Verordening (EU) 2016/679, waarin wordt verwezen naar de norm van wezenlijke overeenkomst.

²³ *Schrems I*, punt 74.

²⁴ *Schrems I*, punt 90.

²⁵ *Schrems I*, punt 91.

justitiabelen om toegang te krijgen tot de persoonsgegevens die op hen betrekking hebben, of om die gegevens te laten rectificeren of verwijderen²⁶.

In de AVG is voortgebouwd op de verduidelijkingen van het Hof van Justitie door de opnemings van een gedetailleerde catalogus van elementen waarmee de Commissie bij een adequaatheidsbeoordeling rekening moet houden²⁷. Bovendien heeft het Hof van Justitie in het *Schrems II*-arrest van 16 juli 2020 de norm van “wezenlijke overeenkomst” verder uitgewerkt, in het bijzonder met betrekking tot de regels inzake de toegang tot persoonsgegevens door overheidsinstanties voor doeleinden van rechtshandhaving en nationale veiligheid. Het Hof heeft met name verduidelijkt dat de norm van “wezenlijke overeenkomst” vereist dat de relevante rechtskaders die bindend zijn voor overheidsinstanties in de betrokken derde landen en gebieden, minimale eisen opleggen die waarborgen dat die instanties geen toegang tot gegevens kunnen krijgen die verder gaat dan wat noodzakelijk en evenredig is voor het nastreven van legitieme doelstellingen, en dat betrokkenen effectieve en afdwingbare rechten hebben tegen die instanties²⁸.

De ontwikkeling van de adequaatheidsnorm komt ook tot uiting in het richtsnoer dat oorspronkelijk door de Groep gegevensbescherming artikel 29 is vastgesteld en vervolgens door de EDPB is bekrachtigd²⁹. Dit richtsnoer, en met name de zogenaamde “adequaatheidsreferentie”, verduidelijkt verder met welke elementen de Commissie rekening moet houden bij het uitvoeren van een adequaatheidsbeoordeling, mede door het verschaffen van een overzicht van “essentiële garanties” voor de toegang tot persoonsgegevens door overheidsinstanties. Dat laatste bouwt met name voort op de rechtspraak van het Europees Hof voor de Rechten van de Mens en is door de EDPB geactualiseerd om rekening te houden met de verduidelijkingen van het Hof van Justitie in het *Schrems II*-arrest³⁰. Belangrijk is dat in de adequaatheidsreferentie ook wordt erkend dat de norm van “wezenlijke overeenkomst” geen puntsgewijze replicatie (“fotokopie”) van de EU-regels inhoudt, aangezien de middelen die zorgen voor een vergelijkbaar beschermingsniveau per privacysysteem kunnen verschillen en vaak een afspiegeling zijn van uiteenlopende rechtstradities.

Daarom heeft de Commissie, om te bepalen of de elf adequaatheidsbesluiten die op grond van de oude regels zijn genomen nog steeds voldoen aan de AVG-norm, niet alleen rekening gehouden met de ontwikkeling van het gegevensbeschermingskader in de betrokken landen en gebieden, maar ook met de ontwikkeling van de Unierechtelijke interpretatie van de adequaatheidsnorm zelf. Dit omvat ook een beoordeling van het rechtskader voor de toegang tot en het gebruik van persoonsgegevens die vanuit de EU worden doorgegeven door

²⁶ *Schrems I*, punt 95.

²⁷ Artikel 45, lid 2, AVG.

²⁸ *Schrems II*, punten 180-182.

²⁹ Adequacy Referential, WP 254 rev. 01, 6 februari 2018 (beschikbaar op: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

³⁰ Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen (beschikbaar op: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_nl).

overheidsinstanties van de landen of gebieden waarvan op basis van artikel 25, lid 6, van de gegevensbeschermingsrichtlijn is vastgesteld dat zij een passend beschermingsniveau bieden.

3. EVALUATIEPROCES

Zoals hierboven beschreven, heeft de evaluatie van de bestaande adequaatheidsbesluiten voor elk van de betrokken landen of gebieden betrekking op het gegevensbeschermingskader en alle ontwikkelingen in verband met dat rechtskader sinds de vaststelling van het adequaatheidsbesluit, alsook op de regels inzake de toegang van de overheid tot gegevens — met name voor doeleinden van rechtshandhaving en nationale veiligheid. De afgelopen jaren hebben de diensten van de Commissie verschillende stappen ondernomen om deze beoordeling uit te voeren, waarbij zij nauw hebben samengewerkt met elk van de betrokken landen of gebieden.

Om de Commissie te helpen bij haar toezichtverplichtingen, heeft elk van de elf landen of gebieden de Commissie uitgebreide informatie verstrekt over de ontwikkelingen in zijn stelsel voor gegevensbescherming sinds de vaststelling van het adequaatheidsbesluit. Bovendien heeft de Commissie van elk van de elf landen of gebieden gedetailleerde informatie gevraagd over de in het betrokken land of gebied geldende regels inzake toegang van de overheid tot persoonsgegevens, met name voor doeleinden van rechtshandhaving en nationale veiligheid. De Commissie heeft ook informatie uit openbare bronnen en van toezichts- en handhavingsautoriteiten en lokale deskundigen over de werking van de besluiten en relevante ontwikkelingen in de wetgeving en praktijk van elk van de betrokken landen en gebieden vergaard, zowel wat betreft de regels inzake gegevensbescherming die gelden voor particuliere exploitanten als met betrekking tot de toegang van de overheid. Tot slot is, waar relevant, terdege rekening gehouden met de internationale verplichtingen die deze landen/gebieden zijn aangegaan in het kader van regionale of universele instrumenten.

Op basis daarvan is de Commissie een intensieve dialoog aangegaan met elk van de betrokken landen en gebieden. In de context van deze dialoog hebben veel van de genoemde landen en gebieden hun privacywetgeving gemoderniseerd en versterkt door middel van alomvattende of gedeeltelijke hervormingen (bv. Andorra, Canada, Faeröer, Zwitserland en Nieuw-Zeeland), onder andere om te beantwoorden aan de noodzaak om de continuïteit van de adequaatheidsbesluiten te waarborgen. Sommige van deze landen hebben verordeningen en/of richtsnoeren van hun gegevensbeschermingsautoriteiten aangenomen om nieuwe eisen op het gebied van gegevensbescherming in te voeren (bv. Israël, Uruguay) of om bepaalde privacyregels te verduidelijken (bv. Argentinië, Canada, Guernsey, Jersey, Man, Israël, Nieuw-Zeeland), voortbordurend op handhavingspraktijken of rechtspraak. Om relevante verschillen in het beschermingsniveau aan te pakken, zijn met sommige van de betrokken landen en gebieden bovendien — waar dit nodig was om de continuïteit van de adequaatheidsbesluiten te waarborgen — na onderhandelingen aanvullende waarborgen overeengekomen voor persoonsgegevens die vanuit Europa worden doorgegeven. Zo heeft de Canadese regering het recht op toegang tot en correctie van door de overheid verwerkte persoonsgegevens uitgebreid tot alle justitiabelen, ongeacht hun nationaliteit of verblijfplaats (terwijl deze rechten in het verleden alleen golden voor Canadese burgers, permanente ingezetenen of personen die in

Canada aanwezig waren)³¹. Een ander voorbeeld is de invoering door de Israëlische regering van specifieke waarborgen ter versterking van de bescherming van persoonsgegevens die vanuit de Europese Economische Ruimte worden doorgegeven, die met name nieuwe verplichtingen opleggen op het gebied van de nauwkeurigheid en de bewaring van gegevens, het recht op informatie en op verwijdering van gegevens versterken en aanvullende categorieën gevoelige gegevens invoeren³².

Tegelijkertijd hebben de diensten van de Commissie de standpunten verzameld van en regelmatig informatie verstrekt aan het Europees Parlement (Commissie burgerlijke vrijheden, justitie en binnenlandse zaken)³³, de Raad (via de Groep gegevensbescherming)³⁴, de EDPB³⁵ en de AVG-deskundigengroep met meerdere belanghebbenden³⁶ (waarin vertegenwoordigers van het maatschappelijk middenveld, het bedrijfsleven, de academische wereld en beoefenaars van juridische beroepen zitting hebben) over de voortgang van de evaluatie.

Dit verslag en het bijbehorende werkdokument van de diensten van de Commissie (SWD) zijn dan ook het resultaat van nauwe samenwerking met elk van de betrokken landen en gebieden en van overleg met en feedback van de relevante EU-instellingen en -organen. Ze zijn gebaseerd op verschillende bronnen, waaronder wetgeving, regelgevingsbesluiten, rechtspraak, besluiten en richtsnoeren van gegevensbeschermingsautoriteiten, verslagen van (onafhankelijke) toezichthoudende instanties en input van belanghebbenden. Voorafgaand aan de vaststelling van dit verslag zijn alle genoemde landen en gebieden in de gelegenheid gesteld om de feitelijke juistheid van de informatie over hun stelsel in het SWD te verifiëren.

4. BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

Uit de eerste evaluatie is gebleken dat het gegevensbeschermingskader in elk van de elf landen of gebieden sinds de vaststelling van de adequaatheidsbesluiten verder naar het EU-kader is toegegroeid. Wat de toegang van de overheid tot persoonsgegevens betreft, is uit de eerste evaluatie bovendien gebleken dat de wetgeving van deze landen of gebieden passende eisen en beperkingen oplegt en voorziet in toezicht- en verhaalmechanismen op dit gebied.

³¹ Section 12 van de Privacy Act, Privacy Act Extension Order, No. 1 en de Privacy Act Extension Order, No. 2.

³² Verordening 5783-2023 inzake de bescherming van de persoonlijke levenssfeer (instructies voor gegevens die naar Israël worden doorgegeven vanuit de Europese Economische Ruimte), gepubliceerd in het Israëlische Staatsblad (*Reshumut*) op 7 mei 2023.

³³ Zie bijvoorbeeld de resolutie van het Europees Parlement van 25 maart 2021 over het evaluatieverslag van de Commissie over de toepassing van de algemene verordening gegevensbescherming, twee jaar na de inwerkingtreding (2020/2717(RSP)), beschikbaar op: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_NL.html

³⁴ Zie bijvoorbeeld het standpunt van de Raad en bevindingen over de toepassing van de algemene verordening gegevensbescherming (AVG), goedgekeurd op 19 december 2019, beschikbaar op: <https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/nl/pdf>

³⁵ Zie bijvoorbeeld de bijdrage van de EDPB aan de evaluatie van de AVG uit hoofde van artikel 97, vastgesteld op 18 februari 2020, beschikbaar op: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf

³⁶ Zie bijvoorbeeld het verslag van de deskundigengroep met meerdere belanghebbenden over de evaluatie van de AVG, beschikbaar op: <https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=nl&do=groupDetail.groupMeeting&meetingId=21356>

De gedetailleerde bevindingen voor elk van de elf landen of gebieden worden gepresenteerd in het SWD van de Commissie dat bij dit verslag is gevoegd. Op basis van deze bevindingen concludeert de Commissie dat elk van de elf landen en gebieden nog steeds een passend beschermingsniveau waarborgt voor persoonsgegevens die vanuit de Europese Unie worden doorgegeven in de zin van de AVG, zoals uitgelegd door het Hof van Justitie. De bevindingen voor elk van de landen en gebieden met een passend beschermingsniveau worden hieronder samengevat.

4.1. Andorra

De Commissie is verheugd over de ontwikkelingen in het Andorrese rechtskader sinds de vaststelling van het adequaatheidsbesluit, met inbegrip van wetswijzigingen en activiteiten van toezichthoudende instanties. Met name de goedkeuring van de gekwalificeerde wet 29/2021 inzake de bescherming van persoonsgegevens, die in mei 2022 in werking is getreden, heeft bijgedragen aan een hoger niveau van gegevensbescherming, aangezien de wet qua structuur en belangrijkste onderdelen nauw aansluit bij de AVG.

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties in Andorra duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven, kunnen raadplegen en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende rechtskader en internationale verplichtingen, met name de grondwet van Andorra, het Europees Verdrag tot bescherming van de rechten van de mens (EVRM) en het Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108 en het wijzigingsprotocol waardoor het gemoderniseerde Verdrag 108+ is ontstaan), alsook uit specifieke voorschriften inzake gegevensbescherming die van toepassing zijn op de verwerking van persoonsgegevens in het kader van de rechtshandhaving en die in wezen zijn overgenomen van de kernelementen van Richtlijn (EU) 2016/680³⁷. Daarnaast legt het Andorrese recht een aantal specifieke voorwaarden en beperkingen op voor de toegang tot en het gebruik van persoonsgegevens door overheidsinstanties en voorziet het in toezicht- en verhaalmechanismen op dit gebied.

Op basis van de algemene bevindingen in het SWD concludeert de Commissie dat Andorra een passend beschermingsniveau blijft waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven.

Wat betreft de specifieke gegevensbeschermingsregels die momenteel van toepassing zijn op de verwerking van gegevens door rechtshandavingsinstanties, is de Commissie verheugd over het voornemen van de Andorrese wetgever om deze regels te vervangen door een meer

³⁷ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

alomvattende regeling die nog meer in overeenstemming zal zijn met de regels die in de EU gelden. De Commissie zal de toekomstige ontwikkelingen op dit terrein nauwlettend volgen.

4.2. Argentinië

De Commissie is verheugd over de ontwikkelingen in het Argentijnse rechtskader sinds de vaststelling van het adequaatheidsbesluit, waaronder wetswijzigingen, rechtspraak en activiteiten van toezichthoudende instanties, die hebben bijgedragen tot een hoger niveau van gegevensbescherming. Met name is de onafhankelijkheid van de Argentijnse toezichthoudende autoriteit voor gegevensbescherming aanzienlijk versterkt bij decreet nr. 746/17, waarbij de *Agencia de Acceso a la Información Pública* (agentschap voor de toegang tot openbare informatie, AAIP) werd belast met het toezicht op de naleving van de wetgeving inzake gegevensbescherming. Daarnaast heeft de AAIP een aantal bindende verordeningen en adviezen uitgevaardigd die verduidelijken hoe het kader voor gegevensbescherming in de praktijk moet worden geïnterpreteerd en toegepast, waardoor de wetgeving inzake gegevensbescherming up-to-date blijft. Argentinië heeft ook zijn internationale verplichtingen op het gebied van gegevensbescherming versterkt doordat het in 2019 is toegetreden tot het Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens en het aanvullend protocol daarbij, en doordat het in 2023 het wijzigingsprotocol waardoor het gemoderniseerde Verdrag 108+ is ontstaan, heeft geratificeerd.

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties in Argentinië duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven, kunnen raadplegen en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende rechtskader en internationale verplichtingen, met name de Argentijnse grondwet, het Amerikaanse Verdrag tot bescherming van de rechten van de mens, Verdrag 108 en Verdrag 108+, en uit de Argentijnse gegevensbeschermingsregels (Wet nr. 25.326 van 4 oktober 2000 inzake de bescherming van persoonsgegevens) die ook van toepassing zijn op de verwerking van persoonsgegevens door Argentijnse overheidsinstanties, onder meer voor doeleinden van rechtshandhaving en nationale veiligheid. Daarnaast legt het Argentijnse recht een aantal specifieke voorwaarden en beperkingen op voor de toegang tot en het gebruik van persoonsgegevens voor de handhaving van het strafrecht en de nationale veiligheid en voorziet het in toezicht- en verhaalmechanismen op dit gebied.

Op basis van de algemene bevindingen in het SWD concludeert de Commissie dat Argentinië een passend beschermingsniveau blijft waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven.

Tegelijkertijd beveelt de Commissie aan om de beschermingseisen die op het niveau van secundaire regelgeving zijn ontwikkeld, in wetgeving vast te leggen om de rechtszekerheid te vergroten en deze eisen te consolideren. De ontwerpwet inzake gegevensbescherming die onlangs in het Argentijnse Congres is ingediend, kan een kans bieden om dergelijke

ontwikkelingen te codificeren en zo het Argentijnse privacykader verder te versterken. De Commissie zal de toekomstige ontwikkelingen op dit terrein nauwlettend volgen.

4.3. *Canada*

De Commissie is verheugd over de ontwikkelingen in het Canadese rechtskader sinds de vaststelling van het adequaatheidsbesluit, met inbegrip van diverse wetswijzigingen, rechtspraak en activiteiten van toezichthoudende instanties, die hebben bijgedragen tot een hoger niveau van gegevensbescherming. In het bijzonder is de Personal Information Protection and Electronic Documents Act (Pipeda) verder versterkt door middel van verschillende wijzigingen (bv. inzake de voorwaarden voor geldige toestemming en meldingen van inbreuken in verband met persoonsgegevens), terwijl belangrijke vereisten voor gegevensbescherming (bv. inzake de verwerking van gevoelige gegevens) verder zijn verduidelijkt door middel van rechtspraak en richtlijnen van de Canadese federale autoriteit voor gegevensbescherming, het Office of the Privacy Commissioner. Tegelijkertijd beveelt de Commissie aan om een aantal beschermingseisen die op het niveau van secundaire regelgeving zijn ontwikkeld, in wetgeving vast te leggen om de rechtszekerheid te vergroten en deze eisen te consolideren. De lopende hervorming van de Pipeda zou met name een kans kunnen zijn om dergelijke ontwikkelingen te codificeren en zo het Canadese privacykader verder te versterken. De Commissie zal de toekomstige ontwikkelingen op dit terrein nauwlettend volgen.

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties in Canada duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven, kunnen raadplegen en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende grondwettelijke kader (het Canadese Handvest van rechten en vrijheden), rechtspraak, specifieke wetgeving die de toegang tot gegevens regelt, en gegevensbeschermingsregels (d.w.z. de Privacy Act en soortgelijke wetten op provinciaal niveau) die ook van toepassing zijn op de verwerking van persoonsgegevens door Canadese overheidsinstanties, onder meer voor doeleinden van rechtshandhaving en nationale veiligheid. Daarnaast biedt het Canadese rechtssysteem effectieve toezicht- en verhaalmechanismen op dit gebied, onder andere door een recente uitbreiding van de rechten van betrokkenen en verhaalsmogelijkheden voor niet-Canadese onderdanen of inwoners.

Op basis van de algemene bevindingen in het SWD concludeert de Commissie dat Canada een passend beschermingsniveau blijft waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven aan ontvangers die onder de Pipeda vallen. Zoals hierboven vermeld, wordt de Pipeda momenteel hervormd, waardoor de privacybescherming nog verder kan worden versterkt, ook op gebieden die relevant zijn voor de vaststelling van de adequaatheid.

4.4. *Faeröer*

De Commissie is verheugd over de ontwikkelingen in het rechtskader van de Faeröer sinds de vaststelling van het adequaatheidsbesluit, waaronder wetswijzigingen, rechtspraak en activiteiten van toezichthoudende instanties, die hebben bijgedragen tot een hoger niveau van

gegevensbescherming. De Faeröer hebben met name hun gegevensbeschermingskader aanzienlijk gemoderniseerd door de goedkeuring van de Data Protection Act, die in 2021 in werking is getreden en het Faeröerse stelsel nauw heeft afgestemd op de AVG.

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties in de Faeröer duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven, kunnen raadplegen en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende rechtskader en internationale verplichtingen, met name het grondwettelijke kader en het EVRM, alsook uit specifieke wetten die de toegang van de overheid tot gegevens regelen en de gegevensbeschermingsregels die van toepassing zijn op de verwerking van persoonsgegevens voor de handhaving van het strafrecht (de wet betreffende de verwerking van persoonsgegevens door rechtshandavingsinstanties die in 2022 op de Faeröer in werking is getreden en die de wetgeving omzet die door Denemarken is vastgesteld ter uitvoering van Richtlijn (EU) 2016/680 op de Faeröer) en van de nationale veiligheid (vervat in de Act on the Security and Intelligence Service). Bovendien zijn er op dit gebied effectieve toezicht- en verhaalmechanismen beschikbaar.

Op basis van de algemene bevindingen in het SWD concludeert de Commissie dat de Faeröer een passend beschermingsniveau blijven waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven.

4.5. Guernsey

De Commissie is verheugd over de ontwikkelingen in het rechtskader van Guernsey sinds de vaststelling van het adequaatheidsbesluit, waaronder wetswijzigingen en activiteiten van toezichthoudende instanties, die hebben bijgedragen tot een hoger niveau van gegevensbescherming. Guernsey heeft met name zijn gegevensbeschermingskader aanzienlijk gemoderniseerd door de Data Protection (Bailiwick of Guernsey) Law 2017 aan te nemen, die sinds 2019 van toepassing is en het stelsel van Guernsey nauw afstemt op de AVG.

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties in Guernsey duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven, kunnen raadplegen en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende rechtskader en internationale verplichtingen, met name het EVRM en Verdrag 108, alsook uit de gegevensbeschermingsregels van Guernsey, met inbegrip van de specifieke bepalingen voor de verwerking van persoonsgegevens in het kader van de rechtshandhaving die zijn vastgesteld in de Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018. Daarnaast legt het recht van Guernsey een aantal specifieke voorwaarden en beperkingen op voor de toegang tot en het gebruik van persoonsgegevens voor de handhaving van het strafrecht en de nationale veiligheid en voorziet het in toezicht- en verhaalmechanismen op dit gebied.

Op basis van de algemene bevindingen in het SWD concludeert de Commissie dat Guernsey een passend beschermingsniveau blijft waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven.

4.6. Man

De Commissie is verheugd over de ontwikkelingen in het rechtskader van het eiland Man sinds de vaststelling van het adequaatheidsbesluit, waaronder wetswijzigingen en activiteiten van toezichthoudende instanties, die hebben bijgedragen tot een hoger niveau van gegevensbescherming. Het eiland Man heeft met name in 2018 nieuwe wetgeving aangenomen (de Data Protection Act 2018, aangevuld met de Data Protection (Application of GDPR) Order 2018) die de meeste bepalingen van het gegevensbeschermingskader van de EU in de rechtsorde van het eiland Man opneemt en slechts kleine aanpassingen aanbrengt op specifieke punten, met name om het kader aan de lokale context aan te passen.

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties op het eiland Man duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende rechtskader en internationale verplichtingen, met name het EVRM en Verdrag 108, alsook uit de gegevensbeschermingsregels van het eiland Man, met inbegrip van de specifieke bepalingen voor de verwerking van persoonsgegevens in het kader van de rechtshandhaving die zijn vastgesteld in de Data Protection (Application of LED) Order 2018 en de LED Implementing Regulations 2018. Daarnaast legt het recht van het eiland Man een aantal specifieke voorwaarden en beperkingen op voor de toegang tot en het gebruik van persoonsgegevens voor de handhaving van het strafrecht en de nationale veiligheid en voorziet het in toezicht- en verhaalmechanismen op dit gebied.

Op basis van de algemene bevindingen in het SWD concludeert de Commissie dat het eiland Man een passend beschermingsniveau blijft waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven.

4.7. Israël

De Commissie is verheugd over de ontwikkelingen in het Israëlische rechtskader sinds de vaststelling van het adequaatheidsbesluit, waaronder wetswijzigingen, rechtspraak en activiteiten van toezichthoudende instanties, die hebben bijgedragen tot een hoger niveau van gegevensbescherming. Israël heeft met name specifieke eisen opgelegd ter versterking van de bescherming van persoonsgegevens die vanuit de Europese Economische Ruimte worden doorgegeven, door de goedkeuring van Verordening 5783-2023 inzake de bescherming van de persoonlijke levenssfeer (instructies voor gegevens die naar Israël worden doorgegeven vanuit de Europese Economische Ruimte). Israël versterkte ook de eisen voor gegevensbeveiliging door de goedkeuring van Verordening 5777-2017 inzake de bescherming van de persoonlijke levenssfeer (gegevensbeveiliging) en consolideerde de onafhankelijkheid van zijn toezichthoudende autoriteit voor gegevensbescherming in een bindende regeringsresolutie.

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties in Israël duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven, kunnen raadplegen en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende rechtskader, met name de Israëlische basiswet, alsook uit Wet 5741-1981 inzake de bescherming van de persoonlijke levenssfeer en de op grond daarvan vastgestelde verordeningen, die van toepassing zijn op de verwerking van persoonsgegevens door Israëlische overheidsinstanties, onder meer voor doeleinden van rechtshandhaving en nationale veiligheid. Daarnaast legt het Israëlische recht een aantal specifieke voorwaarden en beperkingen op voor de toegang tot en het gebruik van persoonsgegevens voor de handhaving van het strafrecht en de nationale veiligheid en voorziet het in toezicht- en verhaalmechanismen op dit gebied.

Op basis van de algemene bevindingen in het SWD concludeert de Commissie dat Israël een passend beschermingsniveau blijft waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven.

Tegelijkertijd beveelt de Commissie aan om een aantal beschermingseisen die op het niveau van secundaire regelgeving en in de rechtspraak zijn ontwikkeld, in wetgeving vast te leggen om de rechtszekerheid te vergroten en deze eisen te consolideren. Wet 5722-2022 inzake de bescherming van de persoonlijke levenssfeer (amendment nr. 14), die onlangs in het Israëlische parlement is ingediend, biedt een belangrijke kans om dergelijke ontwikkelingen te consolideren en te codificeren, en daarmee het Israëlische privacykader verder te versterken. De Commissie zal de toekomstige ontwikkelingen op dit terrein nauwlettend volgen.

4.8. Jersey

De Commissie is verheugd over de ontwikkelingen in het rechtskader van Jersey sinds de vaststelling van het adequaatheidsbesluit, waaronder wetswijzigingen, rechtspraak en activiteiten van toezichthoudende instanties, die hebben bijgedragen tot een hoger niveau van gegevensbescherming. Jersey heeft met name zijn gegevensbeschermingskader aanzienlijk gemoderniseerd door de Data Protection (Jersey) Law 2018 en de Data Protection Authority (Jersey) Law 2018 aan te nemen, die in 2018 in werking zijn getreden en het stelsel van Jersey nauw afstemmen op de AVG.

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties in Jersey duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven, kunnen raadplegen en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende rechtskader en internationale verplichtingen, met name het EVRM en Verdrag 108, alsook uit de gegevensbeschermingsregels van Jersey, met inbegrip van de specifieke bepalingen voor de verwerking van persoonsgegevens in het kader van de rechtshandhaving die zijn vastgesteld in de Data Protection (Jersey) Law 2018, zoals gewijzigd bij Schedule 1 bij die wet. Daarnaast legt het recht van Jersey een aantal specifieke voorwaarden

en beperkingen op voor de toegang tot en het gebruik van persoonsgegevens voor de handhaving van het strafrecht en de nationale veiligheid en voorziet het in toezicht- en verhaalmechanismen op dit gebied.

Op basis van de algemene bevindingen in het SWD concludeert de Commissie dat Jersey een passend beschermingsniveau blijft waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven.

4.9. Nieuw-Zeeland

De Commissie is verheugd over de ontwikkelingen in het rechtskader van Nieuw-Zeeland sinds de vaststelling van het adequaatheidsbesluit, waaronder wetswijzigingen, rechtspraak en activiteiten van toezichthoudende instanties, die hebben bijgedragen tot een hoger niveau van gegevensbescherming. Het stelsel voor gegevensbescherming onderging met name een ingrijpende hervorming met de goedkeuring van de Privacy Act 2020, die de convergentie met het gegevensbeschermingskader van de EU verder versterkte, met name wat betreft de regels voor internationale doorgiften van persoonsgegevens en de bevoegdheden van de gegevensbeschermingsautoriteit (het Office of the Privacy Commissioner).

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties in Nieuw-Zeeland duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven, kunnen raadplegen en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende grondwettelijke kader (bv. de Bill of Rights Act) en uit rechtspraak, evenals uit specifieke wetten die de toegang van de overheid tot gegevens regelen en bepalingen van de Privacy Act die ook van toepassing zijn op de verwerking van persoonsgegevens door strafrechtelijke handhavingsinstanties en nationale veiligheidsdiensten. Bovendien voorziet het Nieuw-Zeelandse rechtssysteem in verschillende toezicht- en verhaalmechanismen op dit gebied.

Op basis van de algemene bevindingen in het SWD concludeert de Commissie dat Nieuw-Zeeland een passend beschermingsniveau blijft waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven. De Commissie is ook verheugd dat de Nieuw-Zeelandse regering onlangs een wetsvoorstel tot wijziging van de Privacy Act 2020 heeft ingediend bij het parlement om de bestaande transparantievereisten verder aan te scherpen. De Commissie zal de toekomstige ontwikkelingen op dit terrein nauwlettend volgen.

4.10. Zwitserland

De Commissie is verheugd over de ontwikkelingen in het Zwitserse rechtskader sinds de vaststelling van het adequaatheidsbesluit, waaronder wetswijzigingen, rechtspraak en activiteiten van toezichthoudende instanties, die hebben bijgedragen tot een hoger niveau van gegevensbescherming. Dit betreft in het bijzonder de gemoderniseerde federale gegevensbeschermingswet die de convergentie met het gegevensbeschermingskader van de EU verder heeft vergroot, met name wat betreft de bescherming van gevoelige gegevens en de

regels voor internationale doorgifte van gegevens. Zwitserland heeft ook zijn internationale verplichtingen op het gebied van gegevensbescherming versterkt door in september 2023 Verdrag 108+ te ratificeren.

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties in Zwitserland duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven, kunnen raadplegen en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende rechtskader en internationale verplichtingen, met name de Zwitserse federale grondwet, het EVRM en Verdrag 108+, alsook uit de Zwitserse regels inzake gegevensbescherming, waaronder de federale gegevensbeschermingswet en specifieke regels inzake gegevensbescherming die van toepassing zijn op de strafrechtelijke handhavingsinstanties (bv. het wetboek van strafvordering) en de nationale veiligheidsdiensten (bv. de wet op de inlichtingendienst). Daarnaast legt het Zwitserse recht een aantal specifieke voorwaarden en beperkingen op voor de toegang tot en het gebruik van persoonsgegevens voor de handhaving van het strafrecht en de nationale veiligheid en voorziet het in toezicht- en verhaalmechanismen op dit gebied.

Op basis van de algemene bevindingen in het SWD concludeert de Commissie dat Zwitserland een passend beschermingsniveau blijft waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven.

4.11. Uruguay

De Commissie is verheugd over de ontwikkelingen in het Uruguayaanse rechtskader sinds de vaststelling van het adequaatheidsbesluit, met inbegrip van diverse wetswijzigingen, rechtspraak en activiteiten van toezichthoudende instanties, die hebben bijgedragen tot een hoger niveau van gegevensbescherming. Uruguay heeft met name Ley n°. 18.333 de proteccion de datos personales y Acción de Habeas data (wet nr. 18.331 inzake de bescherming van persoonsgegevens en “Habeas data”-actie) van 2008 gemoderniseerd en versterkt door middel van wetswijzigingen in 2018 en 2020, die het territoriale toepassingsgebied van de wetgeving op het gebied van de gegevensbescherming uitbreidden, en zorgden voor nieuwe verantwoordingsvereisten (zoals effectbeoordelingen, gegevensbescherming door ontwerp en door standaardinstellingen, melding van inbreuken in verband met persoonsgegevens en de aanstelling van functionarissen voor gegevensbescherming) en aanvullende bescherming voor biometrische gegevens. Uruguay heeft ook zijn internationale verplichtingen op het gebied van gegevensbescherming versterkt door in 2019 toe te treden tot Verdrag 108 en in 2021 Verdrag 108+ te ratificeren.

Wat de toegang van de overheid tot persoonsgegevens betreft, gelden voor de overheidsinstanties in Uruguay duidelijke, nauwkeurige en toegankelijke regels op grond waarvan deze instanties gegevens die vanuit de EU worden doorgegeven, kunnen raadplegen en vervolgens kunnen gebruiken voor doeleinden van algemeen belang, met name voor de handhaving van het strafrecht en de nationale veiligheid. Deze beperkingen en eisen vloeien voort uit het overkoepelende rechtskader en internationale verplichtingen, met name de

Uruguyaanse grondwet, het Amerikaanse Verdrag tot bescherming van de rechten van de mens, Verdrag 108 en Verdrag 108+, en uit de gegevensbeschermingsregels in Wet nr. 18.331 inzake de bescherming van persoonsgegevens en de Habeas data-actie die van toepassing zijn op de verwerking van persoonsgegevens door Uruguyaanse overheidsinstanties, onder meer voor doeleinden van rechtshandhaving en nationale veiligheid. Daarnaast legt het Uruguyaanse recht een aantal specifieke voorwaarden en beperkingen op voor de toegang tot en het gebruik van persoonsgegevens door overheidsinstanties en voorziet het in toezicht- en verhaalmechanismen op dit gebied.

Op basis van de algemene bevindingen van deze eerste evaluatie concludeert de Commissie dat Uruguay een passend beschermingsniveau blijft waarborgen voor persoonsgegevens die vanuit de EU worden doorgegeven.

5. TOEKOMSTIGE MONITORING EN SAMENWERKING

De Commissie erkent de uitstekende samenwerking met de relevante autoriteiten in elk van de betrokken landen en gebieden bij de uitvoering van deze evaluatie en waardeert deze ten zeerste. De Commissie zal de ontwikkelingen in de beschermingskaders en de praktijk van de betrokken landen en gebieden nauwlettend blijven volgen. In het geval van ontwikkelingen in een land of gebied met een passend beschermingsniveau die een negatieve invloed zouden hebben op het vastgestelde passende niveau van gegevensbescherming, zal de Commissie, waar nodig, gebruikmaken van haar bevoegdheden op grond van artikel 45, lid 5, AVG om een adequaatheidsbesluit op te schorten, te wijzigen of in te trekken.

Deze evaluatie bevestigt dat de vaststelling van een adequaatheidsbesluit geen “eindpunt” is, maar een gelegenheid biedt om de dialoog en samenwerking met gelijkgestemde internationale partners over gegevensstromen en digitale aangelegenheden meer in het algemeen verder te intensiveren. In dit verband kijkt de Commissie uit naar toekomstige uitwisselingen met de relevante autoriteiten om de samenwerking op internationaal niveau bij de bevordering van veilige en vrije gegevensstromen verder te versterken, onder meer door versterkte samenwerking bij de handhaving. Om deze dialoog te intensiveren en de uitwisseling van informatie en ervaringen te bevorderen, is de Commissie van plan om in 2024 een bijeenkomst op hoog niveau te organiseren met vertegenwoordigers van de EU en alle landen die profiteren van een adequaatheidsbesluit.