

V Bruseli 22. januára 2024
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Komu:	Thérèse BLANCHETOVÁ, generálna tajomníčka Rady Európskej únie
Č. dok. Kom.:	COM(2024) 7 final
Predmet:	SPRÁVA KOMISIE EURÓPSKEMU PARLAMENTU A RADE o prvom preskúmaní fungovania rozhodnutí o primeranosti prijatých podľa článku 25 ods. 6 smernice 95/46/ES

Delegáciám v prílohe zasielame dokument COM(2024) 7 final.

Príloha: COM(2024) 7 final



EURÓPSKA
KOMISIA

V Bruseli 15. 1. 2024
COM(2024) 7 final

SPRÁVA KOMISIE EURÓPSKEMU PARLAMENTU A RADE

**o prvom preskúmaní fungovania rozhodnutí o primeranosti prijatých podľa článku 25
ods. 6 smernice 95/46/ES**

{SWD(2024) 3 final}

1. PRVÉ PRESKÚMANIE – SÚVISLOSTI A KONTEXT

Táto správa obsahuje zistenia Komisie týkajúce sa prvého preskúmania rozhodnutí o primeranosti, ktoré boli prijaté na základe článku 25 ods. 6 smernice 95/46/ES¹ (smernica o ochrane údajov).

V týchto rozhodnutiach Komisia stanovila, že jedenásť krajín alebo území zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných z Európskej únie (EÚ)²: Andorra³, Argentína⁴, Kanada (pre obchodných prevádzkovateľov)⁵, Faerské ostrovy⁶, Guernsey⁷, Ostrov Man⁸, Izrael⁹, Jersey¹⁰, Nový Zéland¹¹, Švajčiarsko¹² a Uruguaj¹³. Prenosy údajov z EÚ do týchto krajín alebo na tieto územia sa preto môžu uskutočňovať bez ukladania doplňujúcich požiadaviek.

Rozhodnutia o primeranosti prijaté podľa smernice o ochrane údajov zostali po nadobudnutí účinnosti nariadenia (EÚ) 2016/679¹⁴ (všeobecné nariadenie o ochrane údajov) 25. mája 2018 v platnosti¹⁵. Vo všeobecnom nariadení o ochrane údajov sa zároveň objasnilo, že závery o primeranosti sú „živé nástroje“, a stanovilo sa, že Komisia musí priebežne monitorovať vývoj v tretích krajinách, ktorý by mohol ovplyvniť fungovanie existujúcich rozhodnutí o primeranosti¹⁶. Okrem toho sa v článku 97 všeobecného nariadenia o ochrane údajov vyžaduje, aby Komisia každé

¹ Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 23.11.1995, s. 31).

² Po začlenení do dohody o Európskom hospodárskom priestore (EHP) sa všeobecné nariadenie o ochrane údajov uplatňuje aj na Nórsko, Island a Lichtenštajnsko. Odkazy na EÚ v tejto správe by sa mali chápať tak, že sa vzťahujú aj na štáty EHP.

³ Rozhodnutie Komisie 2010/625/EÚ z 19. októbra 2010 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranej ochrane osobných údajov v Andorre, Ú. v. EÚ L 277, 21.10.2010, s. 27.

⁴ Rozhodnutie Komisie 2003/490/ES z 30. júna 2003 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranej ochrane osobných údajov v Argentíne, Ú. v. EÚ L 168, 5.7.2003, s. 19.

⁵ Rozhodnutie Komisie 2002/2/ES z 20. decembra 2001 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o náležitej ochrane osobných údajov ustanovenej kanadským zákonom na ochranu osobných údajov a elektronických dokumentov, Ú. v. ES L 2, 4.1.2002, s. 13.

⁶ Rozhodnutie Komisie 2010/146/EÚ z 5. marca 2010 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranej ochrane osobných údajov poskytovanej faerským zákonom o spracovaní osobných údajov, Ú. v. EÚ L 58, 9.3.2010, s. 17.

⁷ Rozhodnutie Komisie 2003/821/ES z 21. novembra 2003 o primeranej ochrane osobných údajov na Guernsey, Ú. v. EÚ L 308, 25.11.2003, s. 27.

⁸ Rozhodnutie Komisie 2004/411/ES z 28. apríla 2004 o primeranej ochrane osobných údajov na ostrove Man, Ú. v. EÚ L 151, 30.4.2004, s. 48.

⁹ Rozhodnutie Komisie 2011/61/EÚ z 31. januára 2011 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranej ochrane osobných údajov Izraelským štátom, pokiaľ ide o automatizované spracovanie osobných údajov, Ú. v. EÚ L 27, 1.2.2011, s. 39.

¹⁰ Rozhodnutie Komisie 2008/393/ES z 8. mája 2008 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranej ochrane osobných údajov v Jersey, Ú. v. EÚ L 138, 28.5.2008, s. 21.

¹¹ Vykonávacie rozhodnutie Komisie 2013/65/EÚ z 19. decembra 2012 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranej ochrane osobných údajov Novým Zélandom, Ú. v. EÚ L 28, 30.1.2013, s. 12.

¹² Rozhodnutie Komisie 2000/518/ES z 26. júla 2000 podľa smernice Európskeho parlamentu a Rady 95/46/ES o primeranej ochrane osobných údajov poskytovaných vo Švajčiarsku, Ú. v. ES L 215, 25.8.2000, s. 1.

¹³ Vykonávacie rozhodnutie Komisie 2012/484/EÚ z 21. augusta 2012 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranej ochrane osobných údajov zo strany Uruguajskej východnej republiky, pokiaľ ide o automatizované spracovanie osobných údajov, Ú. v. EÚ L 227, 23.8.2012, s. 11.

¹⁴ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

¹⁵ Pozri článok 45 ods. 9 všeobecného nariadenia o ochrane údajov, v ktorom sa stanovuje, že rozhodnutia prijaté Komisiou na základe článku 25 ods. 6 smernice 95/46/ES zostávajú v platnosti, pokiaľ ich Komisia nezmení, nenahradi alebo nezruší rozhodnutím prijatým v súlade s článkom 45 ods. 3 alebo 5.

¹⁶ Článok 45 ods. 4 všeobecného nariadenia o ochrane údajov. Pozri aj rozsudok Súdneho dvora EÚ zo 6. októbra 2015 vo veci C-362/14, Maximillian Schrems/Data Protection Commissioner (Schrems I), ECLI:EU:C:2015:650, bod 76.

štyri roky pravidelne preskúmavala tieto rozhodnutia s cieľom určiť, či krajiny a územia, ktoré získali záver o primeranosti, naďalej poskytujú primeranú úroveň ochrany osobných údajov.

Toto prvé preskúmanie rozhodnutí o primeranosti prijatých podľa bývalého rámca ochrany údajov EÚ sa začalo v rámci širšieho hodnotenia uplatňovania a fungovania všeobecného nariadenia o ochrane údajov, v súvislosti s ktorým Komisia predstavila svoje zistenia v oznámení s názvom *Communication on Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation* (Ochrana údajov ako pilier posilnenia postavenia občanov a prístupu EÚ k digitálnej transformácii – dva roky uplatňovania všeobecného nariadenia o ochrane údajov)¹⁷. Záver v prípade tohto aspektu preskúmania bol však odložený, aby sa zohľadnil rozsudok Súdneho dvora vo veci Schrems II¹⁸, v ktorej Súdny dvor poskytol dôležité objasnenia kľúčových prvkov štandardov primeranosti, ako aj ďalšieho súvisiaceho vývoja. To zase viedlo k podrobným výmenám s dotknutými krajinami a územiami, pokiaľ ide o príslušné aspekty ich právneho rámca, mechanizmov dohľadu a systému presadzovania¹⁹. V tejto správe sa v plnej miere zohľadňuje všetok tento vývoj v EÚ, ako aj v dotknutých tretích krajinách a územiach.

Dôležité je, že toto prvé preskúmanie sa uskutočňuje v kontexte prudkého vývoja digitálnych technológií. V posledných desaťročiach sa význam rozhodnutí o primeranosti výrazne zvýšil, keďže sa toky údajov stali neoddeliteľnou súčasťou digitálnej transformácie spoločnosti a globalizácie hospodárstva. Cezhraničný prenos údajov sa stal súčasťou každodenných operácií európskych spoločností všetkých veľkostí naprieč všetkými odvetviami. Viac než kedykoľvek predtým predstavuje rešpektovanie súkromia podmienku stabilných, bezpečných a konkurenčných obchodných tokov. V tejto súvislosti zohrávajú rozhodnutia o primeranosti v mnohých smeroch čoraz kľúčovejšiu úlohu. Zabezpečujú ochranu údajov, čím umožňujú bezpečné toky údajov, ktorými sa dodržiavajú práva jednotlivcov v súlade s prístupom EÚ k digitálnej transformácii zameraným na človeka. Uznáva sa v nich rámec tretích krajín na ochranu ako zaisťujúci rovnocennú úroveň ochrany, ktorá v zásade zodpovedá úrovni, akú zaisťuje EÚ, čím presadzujú konvergenciu medzi systémami ochrany súkromia na základe prísnych noriem ochrany. Ako sa vysvetľuje v tejto správe, rozhodnutia o primeranosti navyše nepredstavujú „koncový bod“, ale prostredníctvom nich sa položil základ pre užšiu spoluprácu a ďalšiu regulačnú konvergenciu medzi EÚ a podobne zmýšľajúcimi partnermi. Zabezpečením voľného toku osobných údajov sa týmito rozhodnutiami otvorili obchodné kanály pre prevádzkovateľov z EÚ, a to aj doplnením a rozšírením výhod obchodných dohôd, a takisto sa uľahčila spolupráca so zahraničnými partnermi v širokej škále oblastí regulácie. Poskytnutím jednoduchého a komplexného riešenia prenosov údajov bez toho, aby vývozca údajov musel poskytnúť ďalšie záruky alebo získať akékoľvek povolenie, uľahčujú plnenie požiadaviek na medzinárodný prenos stanovených vo všeobecnom

¹⁷ Oznámenie bolo uverejnené v júni 2020 a je k dispozícii na tomto odkaze: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en.

¹⁸ Rozsudok Súdneho dvora EÚ zo 16. júla 2020 vo veci C-311/18, Data Protection Commissioner/Facebook Ireland Ltd a Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559.

¹⁹ Rozhodnutie o primeranosti týkajúce sa Japonska bolo prijaté na základe všeobecného nariadenia o ochrane údajov a uvádza sa v ňom samostatné pravidelné preskúmanie. Prvé preskúmanie sa ukončilo v apríli 2023 správou Komisie Európskemu parlamentu a Rade o prvom preskúmaní fungovania rozhodnutia o primeranosti pre Japonsko [COM(2023) 275 final], ktorá je k dispozícii na tomto odkaze <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=COM:2023:275:FIN>.

nariadení o ochrane údajov, a to najmä zo strany malých a stredných podnikov. Napokon vďaka svojmu „sieťovému účinku“ sú rozhodnutia o primeranosti prijaté Európskou komisiou čoraz relevantnejšie aj mimo EÚ, keďže umožňujú nielen voľný tok údajov s 30 hospodárstvami EÚ, ale aj s mnohými ďalšími jurisdikciami na celom svete²⁰ uznávacími krajiny, ktoré sú v existujúcich rozhodnutiach o primeranosti EÚ označené ako „bezpečné destinácie“ podľa ich vlastných pravidiel ochrany údajov.

Na základe všetkých týchto dôvodov sa rozhodnutia o primeranosti stali strategickou zložkou celkového vzťahu EÚ s týmito zahraničnými partnermi a sú považované za hlavný faktor umožňujúci prehĺbenie spolupráce v širokej škále oblastí, čo sa potvrdilo aj intenzívnym a plodným dialógom s dotknutými tretími krajinami/územia, ktoré tvoria základ tohto preskúmania. Preto je obzvlášť dôležité, aby tieto rozhodnutia obstáli v skúške času a aby sa nimi riešil nový vývoj a nové výzvy.

2. CIEĽ A METODIKA PRESKÚMANIA

Rozhodnutia o primeranosti, ktoré sú predmetom tohto preskúmania, boli prijaté na základe rámca ochrany údajov EÚ, ktorý predchádzal všeobecnému nariadeniu o ochrane údajov. Hoci najnovšie rozhodnutia pochádzajú približne spreď desaťročia (napr. rozhodnutia týkajúce sa Nového Zélandu a Uruguaju, obe boli prijaté v roku 2012), iné sú platné viac ako 20 rokov (napr. rozhodnutie týkajúce sa Kanady, ktoré bolo prijaté v roku 2001 a rozhodnutie týkajúce sa Švajčiarska, ktoré bolo prijaté v roku 2000). Odvtedy sa rámce ochrany údajov vo všetkých jedenástich krajinách a územiach vyvíjali, napríklad prostredníctvom legislatívnych a regulačných reforiem, vývoja praxe orgánov pre ochranu osobných údajov v oblasti presadzovania alebo vývoja judikatúry.

Komisia sa preto pri vykonávaní svojho hodnotenia zamerala na vývoj rámcov ochrany údajov príslušných krajín a území, ktoré vznikli po prijatí rozhodnutia o primeranosti. Posúdila, ako tento vývoj ďalej formoval podmienky ochrany údajov príslušnej krajiny alebo územia a či rôzne režimy vzhľadom na tento vývoj ďalej zabezpečovali primeranú úroveň ochrany.

Na tento účel sa v plnej miere zohľadnil vývoj vlastného režimu ochrany údajov EÚ, najmä v súvislosti so začiatkom uplatňovania všeobecného nariadenia o ochrane údajov. Od prijatia týchto rozhodnutí o primeranosti sa právna norma uplatniteľná na takéto rozhodnutia, ako aj prvky príslušné pre posúdenie toho, či zahraničný systém zabezpečuje primeranú úroveň ochrany, predovšetkým ďalej objasnili prostredníctvom judikatúry Súdneho dvora a usmernení prijatých pracovnou skupinou zriadenou podľa článku 29 a Európskym výborom pre ochranu údajov²¹ ako jej nástupcom.

Súdny dvor konkrétne vo svojom rozsudku zo 6. októbra 2015 vo veci Schrems I konštatoval, že nemožno požadovať, aby tretia krajina zaistovala rovnakú úroveň ochrany ako tú, ktorú zaistuje EÚ, ale test primeranosti sa musí chápať ako požadujúci tzv. v zásade rovnocennú úroveň ochrany²². Súdny dvor predovšetkým objasnili prostriedky, ktoré dotknutá tretia krajina

²⁰ Patria sem napríklad Argentína, Izrael, Kolumbia, Maroko, Švajčiarsko a Uruguaj.

²¹ Európsky výbor pre ochranu údajov zahŕňa dozorné orgány pre ochranu údajov v členských štátoch a európskeho dozorného úradníka pre ochranu údajov.

²² Vec Schrems I, body 73, 74 a 96. Pozri aj odôvodnenie 104 nariadenia (EÚ) 2016/679, v ktorom sa odkazuje na štandard zásadnej rovnocennosti.

používa na ochranu osobných údajov, pričom sa môžu líšiť od prostriedkov, ktoré sa používajú v Únii, pokiaľ sa v praxi ukážu ako účinné na zabezpečenie primeranej úrovne ochrany²³. Test primeranosti si preto vyžaduje komplexné posúdenie systému tretej krajiny ako celku vrátane podstaty ochrany súkromia, jej účinného vykonávania a presadzovania.

Súdny dvor okrem toho objasnil, že posúdenie Komisie by sa nemalo obmedzovať na všeobecný rámec ochrany údajov tretej krajiny, ale malo by zahŕňať aj pravidlá upravujúce prístup orgánov verejnej moci k osobným údajom, najmä na účely presadzovania práva a národnej bezpečnosti²⁴. Súdny dvor použil ako kritérium Chartu základných práv a určil niekoľko požiadaviek, s ktorými by tieto pravidlá mali byť v súlade, aby spĺňali štandard „zásadnej rovnocennosti“. Napríklad v právnych predpisoch v tejto oblasti by sa mali stanoviť jasné a presné pravidlá upravujúce rozsah a uplatnenie opatrenia a stanovujúce minimálne požiadavky spôsobom, aby osoby, ktorých osobné údaje boli dotknuté, mali dostatočné záruky, ktoré umožnia účinne chrániť ich údaje pred rizikami zneužitia, ako aj pred akýmkoľvek nezákonným prístupom a akýmkoľvek nezákonným použitím týchto údajov²⁵. Jednotlivcom by sa takisto mala poskytnúť možnosť uplatniť právne prostriedky nápravy s cieľom získať prístup k osobným údajom, ktoré sa ich týkajú, alebo dosiahnuť opravu či vymazanie takýchto údajov²⁶.

Všeobecné nariadenie o ochrane údajov vychádza z objasnení poskytnutých Súdnym dvorom a stanovuje sa v ňom podrobný katalóg prvkov, ktoré musí Komisia pri posudzovaní primeranosti zohľadniť²⁷. Okrem toho Súdny dvor vo svojom rozsudku vo veci Schrems II zo 16. júla 2020 ďalej rozpracoval štandard „zásadnej rovnocennosti“, najmä pokiaľ ide o pravidlá prístupu orgánov verejnej moci k osobným údajom na účely presadzovania práva a národnej bezpečnosti. Konkrétne sa v ňom objasnilo, že štandardom „zásadnej rovnocennosti“ sa vyžaduje, aby príslušné právne rámce záväzné pre orgány verejnej moci v rámci dotknutých tretích krajín a území zahŕňali minimálne záruky, ktorými sa zabezpečí, aby takéto orgány nemali prístup k údajom nad rámec toho, čo je nevyhnutné a primerané na dosiahnutie legitímnych cieľov, a aby dotknuté osoby mali voči takýmto orgánom účinné a vymáhateľné práva²⁸.

Vývoj štandardu primeranosti sa takisto odzrkadľuje v usmerneniach, ktoré pôvodne prijala pracovná skupina zriadená podľa článku 29 a následne ich schválil Európsky výbor pre ochranu údajov²⁹. Týmto usmerneniami, a najmä takzvaným referenčným kritériom primeranosti, sa ďalej objasňujú prvky, ktoré musí Komisia zohľadniť pri vykonávaní posúdenia primeranosti, a to aj poskytnutím prehľadu „základných záruk“ prístupu orgánov verejnej moci k osobným údajom. Uvedené kritérium vychádza najmä z judikatúry Európskeho súdu pre ľudské práva a aktualizoval ho Európsky výbor pre ochranu údajov s cieľom zohľadniť vysvetlenia

²³ Vec Schrems I, bod 74.

²⁴ Vec Schrems I, bod 90.

²⁵ Vec Schrems I, bod 91.

²⁶ Vec Schrems I, bod 95.

²⁷ Článok 45 ods. 2 všeobecného nariadenia o ochrane údajov.

²⁸ Schrems II, body 180 – 182.

²⁹ Referenčné kritérium primeranosti, WP 254 rev. 01, 6. februára 2018 (dostupné na adrese: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

poskytnuté Súdny dvorom v rozsudku vo veci Schrems II³⁰. Dôležité je, že referenčným kritériom primeranosti sa takisto uznáva, že v súvislosti so štandardom „zásadnej rovnocennosti“ nejde o to, aby do detailu zodpovedal (ako „fotokópia“) pravidlám EÚ, keďže prostriedky na zabezpečenie porovnateľnej úrovne ochrany sa môžu medzi rôznymi systémami ochrany súkromia líšiť, čo často odráža rôzne právne tradície.

V záujme určenia, či jedenásť rozhodnutí o primeranosti prijatých podľa predchádzajúcich pravidiel naďalej spĺňa štandard stanovený vo všeobecnom nariadení o ochrane údajov, Komisia preto zohľadnila nielen vývoj rámcov ochrany údajov v dotknutých krajinách a na dotknutých územiach, ale aj vývoj vo výklade samotného štandardu primeranosti podľa práva EÚ. Zahŕňa to aj posúdenie právneho rámca upravujúceho prístup k osobným údajom, ktoré sú prenášané z EÚ orgánmi verejnej moci krajín alebo území, o ktorých sa zistilo, že poskytujú primeranú úroveň ochrany na základe článku 25 ods. 6 smernice o ochrane údajov, a používanie týchto osobných údajov.

3. PROCES PRESKÚMANIA

Ako bolo uvedené, v prípade každej z dotknutých krajín alebo území sa hodnotenie existujúcich rozhodnutí o primeranosti vzťahuje na rámec ochrany údajov a akýkoľvek vývoj vzhľadom na tento právny rámec, a to od prijatia záveru o primeranosti, ako aj na pravidlá upravujúce prístup vlády k údajom – najmä na účely presadzovania práva a národnej bezpečnosti. V posledných rokoch podnikli útvary Komisie niekoľko krokov na vykonanie tohto posúdenia v úzkej spolupráci s každou príslušnou krajinou alebo územím.

Každá z jedenástich krajín alebo území poskytla Komisii od prijatia rozhodnutia o primeranosti komplexné informácie o vývoji svojho režimu ochrany údajov s cieľom pomôcť Komisii pri plnení si povinností v oblasti monitorovania. Okrem toho Komisia požadovala od každej z jedenástich krajín a území podrobné informácie o pravidlách pre prístup vlády k osobným údajom, najmä na účely presadzovania práva a národnej bezpečnosti, ktoré sa uplatňujú v rámci príslušnej krajiny alebo územia. Komisia si takisto vyžiadala informácie z verejných zdrojov, od orgánov dohľadu a orgánov presadzovania práva, ako aj od miestnych odborníkov o fungovaní rozhodnutí a príslušnom vývoji práva a praxe v každej dotknutej krajine a území, a to pokiaľ ide o pravidlá ochrany údajov uplatňované na súkromných prevádzkovateľov, aj pokiaľ ide o prístup vlády k týmto údajom. V relevantných prípadoch sa náležite zohľadnili medzinárodné záväzky, ktoré tieto krajiny/územia prijali v rámci regionálnych alebo univerzálnych nástrojov.

Na tomto základe sa Komisia zapojila do intenzívneho dialógu s každou z dotknutých krajín a území. V kontexte tohto dialógu mnohé z uvedených krajín a území zmodernizovali a posilnili svoje právne predpisy v oblasti ochrany súkromia prostredníctvom komplexných alebo čiastočných reforiem (napr. Andorra, Kanada, Faerské ostrovy, Švajčiarsko, Nový Zéland), čo okrem iného vyvolala potreba zabezpečiť kontinuitu rozhodnutí o primeranosti. Niektoré z týchto krajín prijali právne predpisy a/alebo usmernenia svojho orgánu pre ochranu osobných údajov s cieľom zaviesť

³⁰ Odporúčania č. 02/2020 o európskych základných zárukách týkajúcich sa opatrení sledovania (dostupné na adrese: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en).

nové požiadavky na ochranu údajov (napr. Izrael, Uruguaj) alebo objasniť určité pravidlá ochrany súkromia (napr. Argentína, Kanada, Guernsey, Jersey, Ostrov Man, Izrael, Nový Zéland), a to na základe praxe v oblasti presadzovania práva alebo judikatúry. Okrem toho sa v záujme riešenia príslušných rozdielov v úrovni ochrany s niektorými dotknutými krajinami a územiami rokovalo o dodatočných zárukách v prípade osobných údajov prenášaných z Európy, ak to bolo potrebné na zabezpečenie kontinuity rozhodnutia o primeranosti, a na týchto dodatočných zárukách sa dohodlo. Napríklad kanadská vláda rozšírila práva na prístup k osobným údajom spracúvaným verejným sektorom a na ich opravu na všetkých jednotlivcov bez ohľadu na ich štátnu príslušnosť alebo miesto pobytu (keďže tieto práva boli v minulosti prístupné len kanadským občanom, osobám s trvalým pobytom alebo jednotlivcom zdržiavajúcim sa v Kanade)³¹. Ďalším príkladom je, že izraelská vláda zaviedla osobitné záruky na posilnenie ochrany osobných údajov prenášaných z Európskeho hospodárskeho priestoru, ktorými sa vytvárajú predovšetkým nové povinnosti v oblasti presnosti údajov a ich uchovávaní, posilňujú práva na informácie a vymazanie a zavádzajú dodatočné kategórie citlivých údajov³².

Útvary Komisie zároveň zhromaždili názory Európskeho parlamentu (Výbor pre občianske slobody, spravodlivosť a vnútorné veci)³³, Rady (prostredníctvom pracovnej skupiny pre ochranu údajov)³⁴, Európskeho výboru pre ochranu údajov³⁵ a expertnej skupiny viacerých zainteresovaných strán pre všeobecné nariadenie o ochrane údajov³⁶ (ktorá zahŕňa zástupcov občianskej spoločnosti, priemyslu, akademickej obce a odborníkov pracujúcich v oblasti práva) a pravidelne ich informovali o pokroku v hodnotení.

Táto správa a sprievodný pracovný dokument útvarov Komisie sú preto výsledkom úzkej spolupráce s každou z dotknutých krajín a území, ako aj konzultácií s príslušnými inštitúciami a orgánmi EÚ a spätnej väzby od nich. Opierajú sa o rôzne zdroje vrátane právnych predpisov, regulačných aktov, judikatúry, rozhodnutí a usmernení od orgánov pre ochranu osobných údajov, správ od (nezávislých) orgánov dohľadu a príspevkov zainteresovaných strán. Pred prijatím tejto správy mali všetky uvedené krajiny a územia možnosť overiť vecnú správnosť informácií o svojom systéme uvedených v pracovnom dokumente útvarov Komisie.

³¹ Paragraf 12 zákona o ochrane osobných údajov, nariadenie o rozšírení zákona o ochrane osobných údajov č. 1 a nariadenie o rozšírení zákona o ochrane osobných údajov č. 2.

³² Právne predpisy o ochrane súkromia (pokyny pre údaje, ktoré boli prenesené do Izraela z Európskeho hospodárskeho priestoru), 5783 – 2023, uverejnené v úradnom vestníku Izraela (Reshumut) 7. mája 2023.

³³ Pozri napr. uznesenie Európskeho parlamentu z 25. marca 2021 o hodnotiacej správe Komisie o vykonávaní všeobecného nariadenia o ochrane údajov po dvoch rokoch od jeho uplatňovania [2020/2717(RSP)], ktoré je k dispozícii na tomto odkaze: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EN.html.

³⁴ Pozri napr. stanovisko a zistenia Rady týkajúce sa uplatňovania všeobecného nariadenia o ochrane údajov (GDPR), prijaté 19. decembra 2019, ktoré sú k dispozícii na tomto odkaze: <https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf>.

³⁵ Pozri napr. príspevok Európskeho výboru pre ochranu údajov k hodnoteniu všeobecného nariadenia o ochrane údajov podľa článku 97, prijatý 18. februára 2020, ktorý je k dispozícii na tomto odkaze: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

³⁶ Pozri napr. správu expertnej skupiny viacerých zainteresovaných strán o hodnotení všeobecného nariadenia o ochrane údajov, ktorá je k dispozícii na tomto odkaze: <https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&do=groupDetail.groupMeeting&meetingId=21356>.

4. HLAVNÉ ZISTENIA A ZÁVERY

V prvom preskúmaní sa ukázalo, že od prijatia rozhodnutí o primeranosti sa rámce ochrany údajov zavedené v každej z jedenástich krajín alebo území ďalej zblížovali s rámcom EÚ. Pokiaľ ide o prístup vlády k osobným údajom, z prvého preskúmania navyše vyplynulo, že právom v rámci týchto krajín alebo území sa ukladajú primerané záruky a obmedzenia, pričom poskytuje mechanizmy dohľadu a nápravy v tejto oblasti.

Podrobné zistenia týkajúce sa každej z jedenástich krajín alebo území sú uvedené v pracovnom dokumente útvarov Komisie, ktorý je pripojený k tejto správe. Na základe týchto zistení Komisia dospela k záveru, že každá z jedenástich krajín a území naďalej zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných z Európskej únie v zmysle všeobecného nariadenia o ochrane údajov podľa výkladu Súdneho dvora. Zistenia v prípade každej z jedenástich krajín a území sú zhrnuté ďalej v texte.

4.1. *Andorra*

Komisia víta vývoj andorrského právneho rámca od prijatia rozhodnutia o primeranosti vrátane legislatívnych zmien a činností dozorných orgánov. Konkrétne prijatie kvalifikovaného zákona č. 29/2021 o ochrane osobných údajov, ktorý nadobudol účinnosť v máji 2022, prispelo k zvýšeniu úrovne ochrany údajov, keďže zákon je vzhľadom na svoju štruktúru a hlavné zložky úzko zosúladený so všeobecným nariadením o ochrane údajov.

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci v Andorre sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho právneho rámca a z medzinárodných záväzkov, najmä z andorrskej ústavy, Európskeho dohovoru o ľudských právach a z Dohovoru Rady Európy o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Dohovor č. 108 a pozmeňujúci protokol, ktorým sa vytvára modernizovaný Dohovor č. 108+), ako aj z osobitných pravidiel ochrany údajov, ktoré sa vzťahujú na spracúvanie osobných údajov v kontexte presadzovania práva, pričom v podstate kopírujú základné prvky smernice (EÚ) 2016/680³⁷. Okrem toho andorrské právo stanovuje niekoľko osobitných podmienok a obmedzení týkajúcich sa prístupu orgánov verejnej moci k osobným údajom a ich používania, pričom poskytuje mechanizmy dohľadu a nápravy v tejto oblasti.

Komisia na základe celkových zistení uvedených v pracovnom dokumente útvarov Komisie dospela k záveru, že Andorra naďalej poskytuje primeranú úroveň ochrany osobných údajov prenášaných z EÚ.

Pokiaľ ide o osobitné pravidlá ochrany údajov, ktoré sa v súčasnosti uplatňujú na spracúvanie údajov orgánmi presadzovania práva, Komisia víta zámer andorrského zákonodarcu nahradiť

³⁷ Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV.

tieto pravidlá komplexnejším režimom, ktorý sa ešte viac zosúladi s pravidlami, ktoré sa uplatňujú v EÚ. Komisia bude budúci vývoj v tejto oblasti pozorne monitorovať.

4.2. *Argentína*

Komisia víta vývoj argentínskeho právneho rámca od prijatia rozhodnutia o primeranosti vrátane legislatívnych zmien, judikatúry a činností orgánov dohľadu, ktoré prispeli k zvýšeniu úrovne ochrany údajov. Nezávislosť argentínskeho dozorného orgánu na ochranu údajov bola predovšetkým výrazne posilnená dekrétom č. 746/17, ktorým sa *Agencia de Acceso a la Información Pública* (AAIP) poverila dohľadom nad dodržiavaním zákona o ochrane údajov. Okrem toho AAIP vydala niekoľko záväzných predpisov a stanovísk, ktorými sa objasňuje, ako sa má rámec ochrany údajov vykladať a uplatňovať v praxi, čím pomáha udržiavať aktuálnosť právnych predpisov o ochrane údajov. Argentína takisto posilnila svoje medzinárodné záväzky v oblasti ochrany údajov tým, že sa pripojila k Dohovoru Rady Európy o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov a k jeho dodatkovému protokolu v roku 2019 a ratifikovala pozmeňujúci protokol, ktorým sa vytvára modernizovaný Dohovor č. 108+ v roku 2023.

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci v Argentíne sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho právneho rámca a z medzinárodných záväzkov, najmä z argentínskej ústavy, Amerického dohovoru o ľudských právach, z Dohovoru č. 108 a Dohovoru č. 108+, ako aj z argentínskych pravidiel ochrany údajov (zákon 25.326 o ochrane osobných údajov zo 4. októbra 2000), ktoré sa vzťahujú aj na spracúvanie osobných údajov argentínskymi orgánmi verejnej moci, a to aj na účely presadzovania práva a národnej bezpečnosti. Okrem toho argentínske právo stanovuje niekoľko osobitných podmienok a obmedzení týkajúcich sa prístupu k osobným údajom a ich používania na účely presadzovania práva v trestných veciach a národnej bezpečnosti, pričom poskytuje mechanizmy dohľadu a nápravy v tejto oblasti.

Komisia na základe celkových zistení uvedených v pracovnom dokumente útvarov Komisie dospela k záveru, že Argentína naďalej poskytuje primeranú úroveň ochrany osobných údajov prenášaných z EÚ.

Komisia zároveň odporúča zakotviť ochranu, ktorá bola vytvorená na nižšej ako legislatívnej úrovni, v právnych predpisoch s cieľom zvýšiť právnu istotu a konsolidovať tieto požiadavky. Návrh zákona o ochrane údajov, ktorý bol nedávno predstavený na argentínskom kongrese, by mohol poskytnúť príležitosť kodifikovať takýto vývoj, a tým ďalej posilniť argentínsky rámec ochrany súkromia. Komisia bude budúci vývoj v tejto oblasti pozorne monitorovať.

4.3. *Kanada*

Komisia víta vývoj kanadského právneho rámca od prijatia rozhodnutia o primeranosti vrátane niekoľkých legislatívnych zmien, judikatúry a činností orgánov dohľadu, ktoré prispeli k zvýšeniu úrovne ochrany údajov. Konkrétne bol zákon o ochrane osobných informácií a elektronických dokumentoch (PIPEDA) ďalej posilnený rôznymi zmenami (napr. pokiaľ ide

o podmienky platného súhlasu a oznámenia o porušení ochrany údajov), zatiaľ čo kľúčové požiadavky na ochranu údajov (napr. týkajúce sa spracúvania citlivých údajov) boli ďalej objasnené prostredníctvom judikatúry, ako aj usmernení vydaných kanadským federálnym orgánom na ochranu osobných údajov, úradom komisára pre ochranu súkromia. Komisia zároveň odporúča zakotviť určitú ochranu, ktorá bola vytvorená na nižšej ako legislatívnej úrovni, v právnych predpisoch s cieľom zvýšiť právnu istotu a konsolidovať tieto požiadavky. Prebiehajúca legislatívna reforma PIPEDA by mohla ponúknuť najmä príležitosť kodifikovať takýto vývoj, a tým ďalej posilniť kanadský rámec ochrany súkromia. Komisia bude budúci vývoj v tejto oblasti pozorne monitorovať.

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci v Kanade sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho ústavného rámca (kanadská Charta práv a slobôd), z judikatúry, osobitných právnych predpisov upravujúcich prístup k údajom, ako aj pravidiel ochrany údajov (t. j. zo zákona o ochrane osobných údajov a podobných zákonov na provinčnej úrovni), ktoré sa vzťahujú aj na spracúvanie osobných údajov kanadskými orgánmi verejnej moci, a to aj na účely presadzovania práva a národnej bezpečnosti. Kanadský právny systém okrem toho poskytuje účinné mechanizmy dohľadu a nápravy v tejto oblasti, a to aj prostredníctvom nedávneho rozšírenia práv dotknutých osôb a možností nápravy pre cudzích štátnych príslušníkov alebo osoby s pobytom v Kanade.

Komisia na základe celkových zistení uvedených v pracovnom dokumente útvarov Komisie dospela k záveru, že Kanada naďalej poskytuje primeranú úroveň ochrany osobných údajov prenášaných z EÚ príjemcom, na ktorých sa vzťahuje PIPEDA. Ako už bolo uvedené, PIPEDA v súčasnosti podlieha legislatívnej reforme, ktorá by mohla ďalej posilniť ochranu súkromia aj v oblastiach, ktoré sú relevantné pre záver o primeranosti.

4.4. Faerské ostrovy

Komisia víta vývoj právneho rámca Faerských ostrovov od prijatia rozhodnutia o primeranosti vrátane legislatívnych zmien, judikatúry a činností orgánov dohľadu, ktoré prispeli k zvýšeniu úrovne ochrany údajov. Faerské ostrovy predovšetkým výrazne zmodernizovali svoj rámec ochrany údajov prijatím zákona o ochrane údajov, ktorý nadobudol účinnosť v roku 2021 a ktorým sa úzko zosúladiť faerský režim so všeobecným nariadením o ochrane údajov.

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci na Faerských ostrovoch sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho právneho rámca a z medzinárodných záväzkov, najmä z ústavného rámca a Európskeho dohovoru o ľudských právach, ako aj z osobitných zákonov upravujúcich prístup vlády k údajom a pravidlá ochrany údajov, ktoré sa vzťahujú na spracúvanie osobných údajov na účely presadzovania práva v trestných veciach [zákon o spracúvaní osobných údajov orgánmi presadzovania práva, ktorý nadobudol účinnosť na

Faerských ostrovoch v roku 2022 a ktorým sa transponujú právne predpisy, ktoré Dánsko prijalo na účely vykonávania smernice (EÚ) 2016/680 na Faerských ostrovoch] a na účely národnej bezpečnosti (obsiahnuté v zákone o bezpečnostnej a spravodajskej službe). Okrem toho sú v tejto oblasti k dispozícii účinné mechanizmy dohľadu a nápravy.

Komisia na základe celkových zistení uvedených v pracovnom dokumente útvarov Komisie dospela k záveru, že Faerské ostrovy naďalej poskytujú primeranú úroveň ochrany osobných údajov prenášaných z EÚ.

4.5. *Guernsey*

Komisia víta vývoj guernseyského právneho rámca od prijatia rozhodnutia o primeranosti vrátane legislatívnych zmien a činností orgánov dohľadu, ktoré prispeli k zvýšeniu úrovne ochrany údajov. Na Guernsey sa predovšetkým výrazne zmodernizoval rámec ochrany údajov prijatím zákona o ochrane údajov (Bailiwick Guernsey) z roku 2017, ktorý sa uplatňuje od roku 2019 a ktorým sa úzko zosúladuje guernseyský režim so všeobecným nariadením o ochrane údajov.

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci na Guernsey sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho právneho rámca a z medzinárodných záväzkov, najmä z Európskeho dohovoru o ľudských právach a z Dohovoru č. 108, ako aj z guernseyských pravidiel ochrany údajov vrátane osobitných ustanovení o spracúvaní osobných údajov v kontexte presadzovania práva stanovených v zákone o ochrane údajov (presadzovanie práva a súvisiace záležitosti) (Bailiwick Guernsey) z roku 2018. Okrem toho guernseyské právo stanovuje niekoľko osobitných podmienok a obmedzení týkajúcich sa prístupu k osobným údajom a ich používania na účely presadzovania práva v trestných veciach a národnej bezpečnosti, pričom poskytuje mechanizmy dohľadu a nápravy v tejto oblasti.

Komisia na základe celkových zistení uvedených v pracovnom dokumente útvarov Komisie dospela k záveru, že Guernsey naďalej poskytuje primeranú úroveň ochrany osobných údajov prenášaných z EÚ.

4.6. *Ostrov Man*

Komisia víta vývoj právneho rámca Ostrova Man od prijatia rozhodnutia o primeranosti vrátane legislatívnych zmien a činností orgánov dohľadu, ktoré prispeli k zvýšeniu úrovne ochrany údajov. Ostrov Man konkrétne prijal nové právne predpisy v roku 2018 [zákon o ochrane údajov z roku 2018 doplnený nariadením o ochrane údajov (uplatňovanie všeobecného nariadenia o ochrane údajov) z roku 2018], ktorými sa začleňuje väčšina ustanovení rámca EÚ na ochranu údajov do právneho poriadku Ostrova Man a zároveň sa vykonávajú iba menšie úpravy konkrétnych aspektov, najmä s cieľom prispôbiť rámec miestnemu kontextu.

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci na Ostrove Man sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä

na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho právneho rámca a z medzinárodných záväzkov, najmä z Európskeho dohovoru o ľudských právach a z Dohovoru č. 108, ako aj z pravidiel Ostrova Man v oblasti ochrany údajov vrátane osobitných ustanovení o spracúvaní osobných údajov v kontexte presadzovania práva stanovených v zákone o ochrane údajov (uplatňovanie smernice o presadzovaní práva) z roku 2018 a v právnych predpisoch o vykonávaní smernice o presadzovaní práva z roku 2018. Okrem toho právo Ostrova Man stanovuje niekoľko osobitných obmedzení týkajúcich sa prístupu k osobným údajom a ich používania na účely presadzovania práva v trestných veciach a národnej bezpečnosti, pričom poskytuje mechanizmy dohľadu a nápravy v tejto oblasti.

Komisia na základe celkových zistení uvedených v pracovnom dokumente útvarov Komisie dospela k záveru, že Ostrov Man naďalej poskytuje primeranú úroveň ochrany osobných údajov prenášaných z EÚ.

4.7. *Izrael*

Komisia víta vývoj izraelského právneho rámca od prijatia rozhodnutia o primeranosti vrátane legislatívnych zmien, judikatúry a činností orgánov dohľadu, ktoré prispeli k zvýšeniu úrovne ochrany údajov. Izrael konkrétne zaviedol záruky na posilnenie ochrany osobných údajov prenášaných z Európskeho hospodárskeho priestoru prijatím právnych predpisov o ochrane súkromia (pokyny pre údaje, ktoré boli prenesené do Izraela z Európskeho hospodárskeho priestoru), 5783 – 2023. Izrael takisto posilnil požiadavky na bezpečnosť údajov prijatím právnych predpisov o ochrane súkromia (bezpečnosť údajov), 5777 – 2017, pričom upevnil nezávislosť svojho dozorného orgánu pre ochranu údajov v záväznom uznesení vlády.

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci v Izraeli sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho právneho rámca, najmä zo základného izraelského zákona, ako aj zo zákona o ochrane súkromia *Protection of Privacy Law 5741-1981* a z právnych predpisov prijatých na jeho základe, ktoré sa vzťahujú na spracúvanie osobných údajov izraelskými orgánmi verejnej moci, a to aj na účely presadzovania práva a národnej bezpečnosti. Okrem toho izraelské právo stanovuje niekoľko osobitných obmedzení týkajúcich sa prístupu k osobným údajom a ich používania na účely presadzovania práva v trestných veciach a národnej bezpečnosti, pričom poskytuje mechanizmy dohľadu a nápravy v tejto oblasti.

Komisia na základe celkových zistení uvedených v pracovnom dokumente útvarov Komisie dospela k záveru, že Izrael naďalej poskytuje primeranú úroveň ochrany osobných údajov prenášaných z EÚ.

Komisia zároveň odporúča, aby sa do právnych predpisov zakotvila ochrana, ktorá bola vytvorená na nižšej ako legislatívnej úrovni a v rámci judikatúry, s cieľom zvýšiť právnu istotu a upevniť tieto požiadavky. Zákon o ochrane súkromia (pozmeňujúci návrh č. 14), 5722 – 2022, ktorý bol nedávno predložený izraelskému parlamentu, ponúka významnú príležitosť na konsolidáciu a kodifikáciu

takéhoto vývoja, a tým aj na ďalšie posilnenie izraelského rámca ochrany súkromia. Komisia bude budúci vývoj v tejto oblasti pozorne monitorovať.

4.8. Jersey

Komisia víta vývoj jerseyškého právneho rámca od prijatia rozhodnutia o primeranosti vrátane legislatívnych zmien, judikatúry a činností orgánov dohľadu, ktoré prispeli k zvýšeniu úrovne ochrany údajov. Na Jersey sa predovšetkým výrazne zmodernizoval rámec ochrany údajov prijatím zákona o ochrane údajov (Jersey) z roku 2018 a zákona o orgáne pre ochranu osobných údajov (Jersey) z roku 2018, ktoré nadobudli účinnosť v roku 2018 a ktorými sa úzko zosúladiť jerseyšký režim so všeobecným nariadením o ochrane údajov.

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci v Jersey sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho právneho rámca a z medzinárodných záväzkov, najmä z Európskeho dohovoru o ľudských právach a z Dohovoru č. 108, ako aj z jerseyšských pravidiel ochrany údajov vrátane osobitných ustanovení o spracúvaní osobných údajov v kontexte presadzovania práva stanovených v zákone o ochrane údajov (Jersey) z roku 2018 zmenenom dodatkom 1 k uvedenému zákonu. Okrem toho jerseyské právo stanovuje niekoľko osobitných obmedzení týkajúcich sa prístupu k osobným údajom a ich používania na účely presadzovania práva v trestných veciach a národnej bezpečnosti, pričom poskytuje mechanizmy dohľadu a nápravy v tejto oblasti.

Komisia na základe celkových zistení uvedených v pracovnom dokumente útvarov Komisie dospela k záveru, že Jersey naďalej poskytuje primeranú úroveň ochrany osobných údajov prenášaných z EÚ.

4.9. Nový Zéland

Komisia víta vývoj novozélandského právneho rámca od prijatia rozhodnutia o primeranosti vrátane legislatívnych zmien, judikatúry a činností orgánov dohľadu, ktoré prispeli k zvýšeniu úrovne ochrany údajov. Režim ochrany údajov prešiel najmä komplexnou reformou prijatím zákona o ochrane osobných údajov z roku 2020, ktorým sa ešte viac zvýšila konvergencia s rámcom EÚ na ochranu údajov, najmä pokiaľ ide o pravidlá medzinárodných prenosov osobných údajov a o právomoci orgánu pre ochranu osobných údajov (úrad komisára pre ochranu súkromia).

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci na Novom Zélande sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho ústavného rámca (napr. z Listiny práv) a z judikatúry, ako aj z osobitných zákonov upravujúcich prístup vlády k údajom a z ustanovení zákona o ochrane osobných údajov, ktoré sa vzťahujú aj na spracúvanie osobných údajov orgánmi

činnými v trestnom konaní a národnými bezpečnostnými orgánmi. V právnom systéme Nového Zélandu sa okrem toho stanovujú rôzne mechanizmy dohľadu a nápravy v tejto oblasti.

Komisia na základe celkových zistení uvedených v pracovnom dokumente útvarov Komisie dospela k záveru, že Nový Zéland naďalej poskytuje primeranú úroveň ochrany osobných údajov prenášaných z EÚ. Komisia takisto víta skutočnosť, že novozélandská vláda nedávno predložila parlamentu pozmeňujúci návrh zákona o ochrane osobných údajov z roku 2020 s cieľom ďalej posilniť existujúce požiadavky na transparentnosť. Komisia bude budúci vývoj v tejto oblasti pozorne monitorovať.

4.10. Švajčiarsko

Komisia víta vývoj švajčiarskeho právneho rámca od prijatia rozhodnutia o primeranosti vrátane legislatívnych zmien, judikatúry a činností orgánov dohľadu, ktoré prispeli k zvýšeniu úrovne ochrany údajov. Ide predovšetkým o modernizovaný federálny zákon o ochrane údajov, ktorým sa ďalej zvýšila konvergencia s rámcom EÚ na ochranu údajov, najmä pokiaľ ide o ochranu citlivých údajov a pravidlá medzinárodných prenosov údajov. Švajčiarsko takisto posilnilo svoje medzinárodné záväzky v oblasti ochrany údajov tým, že v septembri 2023 ratifikovalo Dohovor č. 108+.

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci vo Švajčiarsku sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho právneho rámca a z medzinárodných záväzkov, najmä zo švajčiarskej federálnej ústavy, z Európskeho dohovoru o ľudských právach a z Dohovoru č. 108+, ako aj zo švajčiarskych pravidiel ochrany údajov vrátane federálneho zákona o ochrane údajov a osobitných pravidiel ochrany údajov, ktoré sa vzťahujú na presadzovanie práva v trestných veciach (napr. trestný poriadok) a národné bezpečnostné orgány (napr. zákon o spravodajských službách). Okrem toho švajčiarske právo stanovuje niekoľko osobitných obmedzení týkajúcich sa prístupu k osobným údajom a ich používania na účely presadzovania práva v trestných veciach a národnej bezpečnosti, pričom poskytuje mechanizmy dohľadu a nápravy v tejto oblasti.

Komisia na základe celkových zistení uvedených v pracovnom dokumente útvarov Komisie dospela k záveru, že Švajčiarsko naďalej poskytuje primeranú úroveň ochrany osobných údajov prenášaných z EÚ.

4.11. Uruguaj

Komisia víta vývoj uruguajského právneho rámca od prijatia rozhodnutia o primeranosti vrátane niekoľkých legislatívnych zmien, judikatúry a činností orgánov dohľadu, ktoré prispeli k zvýšeniu úrovne ochrany údajov. Uruguaj predovšetkým zmodernizoval a posilnil svoj zákon 18.331 o ochrane osobných údajov a opatrenie *habeas data* z roku 2008 prostredníctvom legislatívnych zmien v rokoch 2018 a 2020, ktorými sa rozšíril územný rozsah pôsobnosti právnych predpisov o ochrane údajov, vytvorili nové požiadavky na zodpovednosť (ako sú posúdenia vplyvu,

špecificky navrhnutá a štandardná ochrana údajov, oznámenie o porušení ochrany údajov a vymenovanie úradníkov pre ochranu údajov) a zaviedla dodatočná ochrana biometrických údajov. Uruguaj takisto posilnil svoje medzinárodné záväzky v oblasti ochrany údajov pristúpením k Dohovoru č. 108 v roku 2019 a ratifikáciou Dohovoru č. 108+ v roku 2021.

Pokiaľ ide o prístup vlády k osobným údajom, na orgány verejnej moci v Uruguaji sa vzťahujú jasné, presné a prístupné pravidlá, podľa ktorých môžu mať takéto orgány prístup k údajom prenášaným z EÚ a následne ich používať na ciele v oblasti verejného záujmu, najmä na účely presadzovania práva v trestných veciach a národnej bezpečnosti. Tieto obmedzenia a záruky vyplývajú zo zastrešujúceho právneho rámca a z medzinárodných záväzkov, najmä z uruguajskej ústavy, Amerického dohovoru o ľudských právach, z Dohovoru č. 108 a Dohovoru č. 108+, ako aj z pravidiel ochrany údajov v zákone 18.331 o ochrane osobných údajov a z opatrenia *habeas data*, ktoré sa vzťahujú na spracúvanie osobných údajov verejnými orgánmi v Uruguaji, najmä na účely presadzovania práva a národnej bezpečnosti. Okrem toho sa v uruguajskom práve stanovuje niekoľko osobitných podmienok a obmedzení týkajúcich sa prístupu k osobným údajom a ich používania orgánmi verejnej moci, pričom poskytuje mechanizmy dohľadu a nápravy v tejto oblasti.

Na základe celkových zistení v rámci tohto prvého preskúmania Komisia dospela k záveru, že Uruguaj naďalej poskytuje primeranú úroveň ochrany osobných údajov prenášaných z EÚ.

5. BUDÚCE MONITOROVANIE A SPOLUPRÁCA

Komisia uznáva a do veľkej miery oceňuje vynikajúcu spoluprácu s príslušnými orgánmi v každej z dotknutých krajín a území pri vykonávaní tohto preskúmania. Komisia bude naďalej pozorne monitorovať vývoj rámcov ochrany a skutočnú prax dotknutých krajín a území. Ak by vývoj v rámci krajiny alebo územia, kde sa zabezpečuje primeraná úroveň ochrany údajov, negatívne ovplyvnil zistenú primeranú úroveň ochrany údajov, Komisia v prípade potreby využije svoje právomoci podľa článku 45 ods. 5 všeobecného nariadenia o ochrane údajov na pozastavenie, zmenu alebo zrušenie rozhodnutia o primeranosti.

Týmto preskúmaním sa potvrdzuje, že prijatie rozhodnutia o primeranosti nie je „koncovým bodom“, ale poskytuje príležitosť na ďalšie zintenzívnenie dialógu a spolupráce s podobne zmýšľajúcimi medzinárodnými partnermi v oblasti tokov údajov a všeobecnejšie digitálnych záležitostí. V tejto súvislosti Komisia očakáva budúce výmeny s príslušnými orgánmi s cieľom ďalej posilniť spoluprácu na medzinárodnej úrovni v oblasti podpory bezpečných a voľných tokov údajov, a to aj prostredníctvom posilnenej spolupráce v oblasti presadzovania. S cieľom zintenzívniť tento dialóg a podporiť výmenu informácií a skúseností má Komisia v úmysle zorganizovať v roku 2024 zasadnutie na vysokej úrovni, na ktorom sa zúčastnia zástupcovia EÚ a všetkých krajín, ktoré majú prospech z rozhodnutia o primeranosti.