

Bruselj, 22. januar 2024
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Prejemnik:	Thérèse BLANCHET, generalna sekretarka Sveta Evropske unije
Št. dok. Kom.:	COM(2024) 7 final
Zadeva:	POROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU o prvem pregledu izvajanja sklepov o ustreznosti, sprejetih na podlagi člena 25(6) Direktive 95/46/ES

Delegacije prejmejo priloženi dokument COM(2024) 7 final.

Priloga: COM(2024) 7 final



EVROPSKA
KOMISIJA

Bruselj, 15.1.2024
COM(2024) 7 final

POROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

**o prvem pregledu izvajanja sklepov o ustreznosti, sprejetih na podlagi člena 25(6)
Direktive 95/46/ES**

{SWD(2024) 3 final}

1. PRVI PREGLED – OZADJE IN OKVIR

To poročilo vsebuje ugotovitve Komisije o prvem pregledu sklepov o ustreznosti, ki so bili sprejeti na podlagi člena 25(6) Direktive 95/46/ES¹ (Direktiva o varstvu podatkov).

Komisija je v teh sklepih ugotovila, da ustrezno raven varstva osebnih podatkov, prenesenih iz Evropske unije (EU), zagotavlja 11 držav oziroma ozemelj²: Andora³, Argentina⁴, Kanada (za gospodarske subjekte)⁵, Ferski otoki⁶, Guernsey⁷, Otok Man⁸, Izrael⁹, Jersey¹⁰, Nova Zelandija¹¹, Švica¹² in Urugvaj¹³. Zato za prenose podatkov iz EU v te države oziroma ozemlja niso potrebne dodatne zahteve.

Sklepi o ustreznosti, sprejeti na podlagi Direktive o varstvu podatkov, so kljub začetku uporabe Uredbe (EU) 2016/679¹⁴ (v nadaljnjem besedilu: splošna uredba o varstvu podatkov) 25. maja 2018 ostali veljavni¹⁵. Hkrati je v splošni uredbi o varstvu podatkov pojasnjeno, da so ugotovitve o ustreznosti „živi instrumenti“, pri čemer je določeno, da mora Komisija redno spremljati razvoj dogodkov v tretjih državah, ki bi lahko vplival na izvajanje obstoječih sklepov

¹ Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).

² Splošna uredba o varstvu podatkov se po vključitvi v Sporazum o Evropskem gospodarskem prostoru uporablja tudi za Norveško, Islandijo in Lihtenštajn. Sklice na EU v tem poročilu bi bilo treba razumeti tako, da zajemajo tudi države EGP.

³ Sklep Komisije 2010/625/EU z dne 19. oktobra 2010 v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES o ustreznem varstvu osebnih podatkov v Andori (UL L 277, 21.10.2010, str. 27).

⁴ Odločba Komisije 2003/490/ES z dne 30. junija 2003 v skladu z Direktivo 95/46/ES Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov v Argentini (UL L 168, 5.7.2003, str. 19).

⁵ Odločba Komisije 2002/2/ES z dne 20. decembra 2001 na podlagi Direktive 95/46/ES Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja kanadski Zakon o varstvu osebnih podatkov in elektronskih dokumentih (UL L 2, 4.1.2002, str. 13).

⁶ Sklep Komisije 2010/146/EU z dne 5. marca 2010 v skladu z Direktivo 95/46/ES Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja ferski zakon o obdelavi osebnih podatkov (UL L 58, 9.3.2010, str. 17).

⁷ Odločba Komisije 2003/821/ES z dne 21. novembra 2003 o primernem varstvu osebnih podatkov na Guernseyju (UL L 308, 25.11.2003, str. 27).

⁸ Odločba Komisije 2004/411/ES z dne 28. aprila 2004 o ustreznem varstvu osebnih podatkov na otoku Man (UL L 151, 30.4.2004, str. 48).

⁹ Sklep Komisije 2011/61/EU z dne 31. januarja 2011 o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Država Izrael pri avtomatizirani obdelavi osebnih podatkov, v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES (UL L 27, 1.2.2011, str. 39).

¹⁰ Odločba Komisije 2008/393/ES z dne 8. maja 2008 v skladu z Direktivo 95/46/ES Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov na otoku Jersey (UL L 138, 28.5.2008, str. 21).

¹¹ Izvedbeni sklep Komisije 2013/65/EU z dne 19. decembra 2012 v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Nova Zelandija (UL L 28, 30.1.2013, str. 12).

¹² Odločba Komisije 2000/518/ES z dne 26. julija 2000 po Direktivi 95/46/ES Evropskega parlamenta in Sveta o primernosti zaščite osebnih podatkov v Švici (UL L 215, 25.8.2000, str. 1).

¹³ Izvedbeni sklep Komisije 2012/484/EU z dne 21. avgusta 2012 o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Vzhodna republika Urugvaj pri avtomatizirani obdelavi osebnih podatkov, v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES (UL L 227, 23.8.2012, str. 11).

¹⁴ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

¹⁵ Glej člen 45(9) splošne uredbe o varstvu podatkov, ki določa, da odločitve, ki jih je Komisija sprejela na podlagi člena 25(6) Direktive 95/46/ES, ostanejo veljavne, dokler jih Komisija ne spremeni, nadomesti ali razveljavi s sklepom, sprejetim v skladu z odstavkom 3 ali 5 člena 45.

o ustreznosti¹⁶. Poleg tega mora v skladu s členom 97 splošne uredbe o varstvu podatkov te sklepe redno pregledovati vsaka štiri leta, da bi ugotovila, ali države in ozemlja, za katere je bila ugotovljena ustreznost, še naprej zagotavljajo ustrezno raven varstva osebnih podatkov.

Ta prvi pregled sklepov o ustreznosti, sprejetih na podlagi nekdanjega okvira EU za varstvo podatkov, se je začel v okviru širše ocene uporabe in izvajanja splošne uredbe o varstvu podatkov, ugotovitve v zvezi s katero je Komisija predstavila v Sporočilu o varstvu podatkov kot stebru krepitve vloge državljanov in pristopa EU k digitalnemu prehodu – dve leti uporabe splošne uredbe o varstvu podatkov¹⁷. Vendar je bil sklep o tem vidiku pregleda odložen, da bi se upoštevala sodba Sodišča v zadevi Schrems II¹⁸, v kateri je Sodišče podalo pomembna pojasnila o ključnih elementih standarda ustreznosti, in drug s tem povezan razvoj dogodkov. To pa je privedlo do podrobne izmenjave informacij z zadevnimi državami in ozemlji o pomembnih vidikih njihovega pravnega okvira, nadzornih mehanizmov in sistema izvrševanja¹⁹. V tem poročilu je v celoti upoštevan ves ta razvoj dogodkov v EU ter zadevnih tretjih državah in ozemljih.

Pomembno je, da ta prvi pregled poteka v razmerah eksponentnega razvoja digitalnih tehnologij. V zadnjih desetletjih se je pomen sklepov o ustreznosti znatno povečal, saj je pretok podatkov postal sestavni del digitalne preobrazbe družbe in globalizacije gospodarstva. Čezmejni prenos podatkov je postal del vsakodnevnega poslovanja evropskih podjetij vseh velikosti in v vseh sektorjih. Spoštovanje zasebnosti je bolj kot kdaj koli prej pogoj za stabilne, varne in konkurenčne trgovinske tokove. V tem okviru imajo sklepi o ustreznosti v mnogih pogledih vse bolj ključno vlogo. Z zagotavljanjem, da se ob prenosu podatkov ohrani njihovo varstvo, omogočajo varen pretok podatkov ob spoštovanju pravic posameznikov v skladu s pristopom EU k digitalni preobrazbi, ki je osredotočen na človeka. S tem, ko potrjujejo, da okvir za varstvo zasebnosti tretjih držav zagotavlja raven varstva, ki je v bistvu enaka ravni varstva v EU, spodbujajo zbliževanje sistemov varstva zasebnosti, ki temeljijo na visokih standardih varstva. Poleg tega, kot je pojasnjeno v tem poročilu, sklepi o ustreznosti niso „končni cilj“, temveč so podlaga za tesnejše sodelovanje in nadaljnje regulativno zbliževanje med EU in podobno mislečimi partnericami. Z omogočanjem prostega pretoka osebnih podatkov odpirajo poslovne poti za gospodarske subjekte EU, saj med drugim dopolnjujejo in še povečujejo koristi trgovinskih sporazumov, ter lajšajo sodelovanje s tujimi partnerji na številnih regulativnih področjih. Z zagotavljanjem preproste in celovite rešitve za prenose podatkov, ne da bi moral izvoznik podatkov zagotoviti dodatne zaščitne ukrepe ali pridobiti dovoljenje, zlasti malim in srednjim podjetjem olajšujejo izpolnjevanje zahtev za mednarodni prenos iz splošne uredbe o varstvu podatkov. Nazadnje, sklepi o ustreznosti, ki jih sprejme

¹⁶ Člen 45(4) splošne uredbe o varstvu podatkov. Glej tudi sodbo Sodišča Evropske unije z dne 6. oktobra 2015, Maximilian Schrems/Data Protection Commissioner (Schrems I), C-362/14, ECLI:EU:C:2015:650, točka 76.

¹⁷ Sporočilo je bilo objavljeno junija 2020 in je na voljo na naslednji povezavi: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en.

¹⁸ Sodba Sodišča Evropske unije z dne 16. julija 2020, Data Protection Commissioner/Facebook Ireland Ltd. in Maximilian Schrems (Schrems II), C-311/18, ECLI:EU:C:2020:559.

¹⁹ Sklep o ustreznosti v zvezi z Japonsko je bil sprejet na podlagi splošne uredbe o varstvu podatkov, v njem pa je določen ločen redni pregled. Prvi pregled je bil zaključen aprila 2023 s Poročilom Komisije Evropskemu parlamentu in Svetu o prvem pregledu izvajanja sklepa o ustreznosti za Japonsko, COM(2023) 275 final, ki je na voljo na naslednji povezavi: <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=COM:2023:275:FIN>.

Evropska komisija, so zaradi „mrežnega učinka“ vse pomembnejši tudi zunaj EU, saj omogočajo prosti pretok podatkov ne le s 30 gospodarstvi EU, temveč tudi s številnimi drugimi jurisdikcijami po vsem svetu²⁰, ki države, za katere je izdan sklep EU o ustreznosti, priznavajo kot „varne destinacije“ v skladu s svojimi pravili o varstvu podatkov.

Iz vseh teh razlogov, kot potrjuje tudi poglobljen in ploden dialog z zadevnimi tretjimi državami/ozemlji, na katerem temelji ta pregled, so sklepi o ustreznosti postali strateški element splošnih odnosov EU s temi tujimi partnericami in so priznani kot pomemben dejavnik, ki omogoča poglobitev sodelovanja na najrazličnejših področjih. Zato je zlasti pomembno, da lahko ti sklepi prestanejo preskus časa ter da se z njimi obravnavajo nov razvoj dogodkov in novi izzivi.

2. PREDMET IN METODOLOGIJA PREGLEDA

Sklepi o ustreznosti, na katere se nanaša ta pregled, so bili sprejeti na podlagi okvira EU za varstvo podatkov, ki je veljal pred sprejetjem splošne uredbe o varstvu podatkov. Medtem ko so bili najnovejši sklepi sprejeti pred približno desetimi leti (npr. sklepa v zvezi z Novo Zelandijo in Urugvajem, ki sta bila sprejeta leta 2012), drugi veljajo že več kot 20 let (npr. sklep v zvezi s Kanado, ki je bil sprejet leta 2001, in sklep v zvezi s Švico, ki je bil sprejet leta 2000). Od takrat so se okviri za varstvo podatkov v vseh 11 državah in ozemljih spremenili, na primer z zakonodajnimi ali regulativnimi reformami, razvojem prakse izvrševanja organov za varstvo podatkov ali sodno prakso.

Komisija se je zato pri izvedbi ocene osredotočila na razvoj okvirov za varstvo podatkov zadevnih držav in ozemelj od sprejetja sklepa o ustreznosti. Ocenila je, kako je ta razvoj nadalje vplival na področje varstva podatkov v zadevni državi oziroma ozemlju in ali različne ureditve ob upoštevanju tega razvoja še naprej zagotavljajo ustrezno raven varstva.

V ta namen so se v celoti upoštevale spremembe ureditve EU na področju varstva podatkov, zlasti zaradi začetka uporabe splošne uredbe o varstvu podatkov. Natančneje, pravni standard, ki se uporablja za take sklepe, in elementi, pomembni za oceno, ali tuj sistem zagotavlja ustrezno raven varstva, so bili od sprejetja teh sklepov o ustreznosti dodatno pojasnjeni s sodno prakso Sodišča in smernicami, ki sta jih sprejela Delovna skupina iz člena 29 in njen naslednik, Evropski odbor za varstvo podatkov²¹ (EOVP).

Sodišče je v sodbi z dne 6. oktobra 2015 v zadevi Schrems I namreč odločilo, da čeprav ni mogoče zahtevati, da tretja država zagotavlja povsem enako raven varstva, kot je raven, zagotovljena v pravnem redu Unije, je treba preskus ustreznosti razumeti tako, da se z njim zahteva „v bistvenem enaka“ raven varstva²². Natančneje, pojasnilo je, da so lahko sredstva, ki jih zadevna tretja država uporabi za varstvo osebnih podatkov, drugačna od sredstev, uporabljenih v Uniji, če se v praksi izkažejo za učinkovita pri zagotavljanju ustrezne ravni

²⁰ Na primer Argentina, Kolumbija, Izrael, Maroko, Švica in Urugvaj.

²¹ Evropski odbor za varstvo podatkov združuje nadzorne organe za varstvo podatkov v državah članicah in Evropskega nadzornika za varstvo podatkov.

²² Sodba Schrems I, točke 73, 74 in 96. Glej tudi uvodno izjavo 104 Uredbe (EU) 2016/679, ki se sklicuje na standard osnovne enakovrednosti.

varstva²³. Za preskus ustreznosti je zato potrebna celovita ocena sistema tretje države kot celote, vključno z vsebino varstva zasebnosti ter njegovim učinkovitim izvajanjem in izvrševanjem.

Poleg tega je Sodišče pojasnilo, da se Komisija pri oceni ne bi smela omejiti na splošni okvir za varstvo podatkov tretje države, temveč bi morala vključiti tudi pravila, ki urejajo dostop javnih organov do osebnih podatkov, zlasti za namene kazenskega pregona in nacionalne varnosti²⁴. Sodišče je na podlagi Listine o temeljnih pravicah kot referenčnega merila opredelilo več zahtev, ki bi jih morala ta pravila izpolnjevati, da bi dosegla standard „osnovne enakovrednosti“. Zakonodaja na tem področju bi morala na primer določati jasna in natančna pravila, ki urejajo obseg in uporabo ukrepa ter določajo minimalne zahteve, tako da imajo osebe, za katerih osebne podatke gre, zadostna jamstva, ki omogočajo učinkovito varovanje njihovih podatkov pred zlorabo, nezakonitim dostopom do teh podatkov in njihovo uporabo²⁵. Posameznikom bi morala tudi omogočati, da uporabijo pravna sredstva za pridobitev dostopa do osebnih podatkov, ki se nanje nanašajo, ali dosežejo popravo ali izbris takih podatkov²⁶.

Splošna uredba o varstvu podatkov temelji na pojasnilih Sodišča, saj določa podroben seznam elementov, ki jih mora Komisija upoštevati pri ocenjevanju ustreznosti²⁷. Poleg tega je Sodišče v sodbi Schrems II z dne 16. julija 2020 podrobneje predstavilo standard „osnovne enakovrednosti“, zlasti v zvezi s pravili o dostopu javnih organov do osebnih podatkov za namene kazenskega pregona in nacionalne varnosti. Zlasti je pojasnilo, da morajo v skladu s standardom „osnovne enakovrednosti“ ustrezni pravni okviri, ki so za javne organe v zadevnih tretjih državah in ozemljih zavezujoči, vključevati minimalne zaščitne ukrepe, ki zagotavljajo, da dostop teh organov do podatkov ne presega tistega, kar je potrebno in sorazmerno za doseganje legitimnih ciljev, ter da imajo posamezniki, na katere se nanašajo osebni podatki, dejanske in izvršljive pravice, ki jih lahko uveljavljajo proti takim organom²⁸.

Razvoj standarda ustreznosti je upoštevan tudi v smernicah, ki jih je prvotno sprejela Delovna skupina iz člena 29, nato pa jih je potrdil EOVP²⁹. V teh smernicah, zlasti v t. i. referenčnem dokumentu o ustreznosti, so dodatno pojasnjeni elementi, ki jih mora Komisija upoštevati pri ocenjevanju ustreznosti, med drugim z zagotovitvijo pregleda „temeljnih jamstev“ za dostop javnih organov do osebnih podatkov. Ta referenčni dokument temelji zlasti na sodni praksi Evropskega sodišča za človekove pravice, EOVP pa ga je posodobil, da bi se upoštevala pojasnila Sodišča v sodbi Schrems II³⁰. Pomembno je, da se v referenčnem dokumentu o ustreznosti priznava tudi, da standard „osnovne enakovrednosti“ ne vključuje neposrednega posnemanja („kopiranja“) pravil EU, saj se lahko načini zagotavljanja primerljive ravni varstva

²³ Sodba Schrems I, točka 74.

²⁴ Sodba Schrems I, točka 90.

²⁵ Sodba Schrems I, točka 91.

²⁶ Sodba Schrems I, točka 95.

²⁷ Člen 45(2) splošne uredbe o varstvu podatkov.

²⁸ Sodba Schrems II, točke 180–182.

²⁹ Referenčni dokument o ustreznosti, WP 254 rev. 01, z dne 6. februarja 2018 (na voljo na: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

³⁰ Priporočila 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe (na voljo na: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_sl).

med različnimi sistemi varstva zasebnosti razlikujejo, pri čemer pogosto odražajo različne pravne tradicije.

Zato je Komisija pri ugotavljanju, ali 11 sklepov o ustreznosti, sprejetih na podlagi prejšnjih pravil, še naprej izpolnjuje standard iz splošne uredbe o varstvu podatkov, upoštevala ne le razvoj okvirov za varstvo podatkov v zadevnih državah in ozemljih, temveč tudi razvoj razlage samega standarda ustreznosti na podlagi prava EU. To vključuje tudi oceno pravnega okvira, ki ureja dostop do osebnih podatkov, prenesenih iz EU, in uporabo teh podatkov s strani javnih organov držav oziroma ozemelj, za katere je bilo na podlagi člena 25(6) Direktive o varstvu podatkov ugotovljeno, da zagotavljajo ustrezno raven varstva.

3. POSTOPEK PREGLEDA

Kot je opisano zgoraj, ocena obstoječih sklepov o ustreznosti za posamezno zadevno državo oziroma ozemlje zajema okvir za varstvo podatkov in ves razvoj dogodkov v zvezi s tem pravnim okvirom od sprejetja ugotovitve o ustreznosti, pa tudi pravila, ki urejajo vladni dostop do podatkov, zlasti za namene kazenskega pregona in nacionalne varnosti. Službe Komisije so v zadnjih letih v tesnem sodelovanju z vsemi zadevnimi državami oziroma ozemlji sprejele več ukrepov za izvedbo te ocene.

Da bi Komisiji pomagali pri njenih obveznostih spremljanja, ji je vseh 11 držav oziroma ozemelj predložilo izčrpne informacije o razvoju ureditve varstva podatkov od sprejetja sklepa o ustreznosti. Poleg tega je Komisija od vseh 11 držav oziroma ozemelj zahtevala podrobne informacije o pravilih, ki se v zadevni državi ali na zadevnem ozemlju uporabljajo za vladni dostop do osebnih podatkov, zlasti za namene kazenskega pregona in nacionalne varnosti. Komisija je iz javnih virov ter od nadzornih in izvršilnih organov, pa tudi od lokalnih strokovnjakov zahtevala tudi informacije o izvajanju sklepov ter o ustreznem razvoju zakonodaje in prakse posamezne zadevne države in ozemlja, tako v zvezi s pravili o varstvu podatkov, ki se uporabljajo za zasebne subjekte, kot tudi v zvezi z vladnim dostopom. Nazadnje, po potrebi so bile ustrezno upoštewane mednarodne obveznosti, ki so jih te države/ozemlja prevzeli v okviru regionalnih ali univerzalnih instrumentov.

Komisija je na tej podlagi začela poglobljen dialog s posamezno zadevno državo oziroma ozemljem. V okviru tega dialoga so številni od njih posodobili in okrepili svojo zakonodajo o varstvu zasebnosti s celovitimi ali delnimi reformami (npr. Andora, Kanada, Ferski otoki, Švica, Nova Zelandija), med drugim zaradi potrebe po zagotovitvi kontinuitete izvajanja sklepov o ustreznosti. Nekatere od teh držav so sprejele predpise in/ali smernice svojega organa za varstvo podatkov, da bi uvedle nove zahteve glede varstva podatkov (npr. Izrael, Urugvaj) ali pojasnile nekatera pravila o zasebnosti (npr. Argentina, Kanada, Guernsey, Jersey, Otok Man, Izrael, Nova Zelandija), ki temeljijo na praksi izvrševanja ali sodni praksi. Da bi se odpravile pomembne razlike v ravni varstva, so bili poleg tega, kadar je bilo to potrebno za zagotovitev kontinuitete izvajanja sklepa o ustreznosti, z nekaterimi zadevnimi državami in ozemlji dogovorjeni in sklenjeni dodatni zaščitni ukrepi za osebne podatke, prenesene iz Evrope. Kanadska vlada je na primer pravice do dostopa in popravka v zvezi z osebnimi podatki, ki jih obdeluje javni sektor, razširila na vse posameznike, ne glede na njihovo državljanstvo ali prebivališče (medtem ko so te pravice v preteklosti imeli le kanadski

državljeni, osebe s stalnim prebivališčem v Kanadi ali posamezniki, prisotni na njenem ozemlju)³¹. Še en primer so posebni zaščitni ukrepi, ki jih je izraelska vlada uvedla za okrepitev varstva osebnih podatkov, prenesenih iz Evropskega gospodarskega prostora, ter ki zlasti prinašajo nove obveznosti na področju točnosti in hrambe podatkov, krepijo pravice do informacij in izbrisa ter uvajajo dodatne kategorije občutljivih podatkov³².

Hkrati so službe Komisije zbrale mnenja Evropskega parlamenta (Odbor za državljanske svoboščine, pravosodje in notranje zadeve)³³, Sveta (prek Delovne skupine za varstvo podatkov)³⁴, EOVP³⁵ in večdeležniške strokovne skupine iz splošne uredbe o varstvu podatkov³⁶ (ki vključuje predstavnike civilne družbe, industrije, akademikov in delavcev v pravni stroki) ter jih redno obveščale o napredku pri ocenjevanju.

To poročilo in priloženi delovni dokument služb Komisije sta torej rezultat tesnega sodelovanja z vsemi zadevnimi državami in ozemlji, pa tudi posvetovanj z ustreznimi institucijami in organi EU ter njihovih povratnih informacij. Temeljita na različnih virih, med drugim na zakonodaji, regulativnih aktih, sodni praksi, sklepih in smernicah organov za varstvo podatkov, poročilih (neodvisnih) nadzornih organov ter prispevkih deležnikov. Pred sprejetjem tega poročila so imele vse navedene države in ozemlja možnost preveriti vsebinsko točnost informacij o njihovem sistemu, navedenih v delovnem dokumentu služb Komisije.

4. GLAVNE UGOTOVITVE IN SKLEPI

Prvi pregled je pokazal, da so se od sprejetja sklepov o ustreznosti okviri za varstvo podatkov, vzpostavljeni v vsaki od 11 držav oziroma ozemelj, še bolj zblížali z okvirom EU. Poleg tega je na področju vladnega dostopa do osebnih podatkov prvi pregled pokazal, da so s pravom teh držav oziroma ozemelj uvedeni ustrezni zaščitni ukrepi in omejitve ter zagotovljeni mehanizmi nadzora in pravnega varstva na tem področju.

Podrobne ugotovitve v zvezi z vsako od 11 držav oziroma ozemelj so predstavljene v delovnem dokumentu služb Komisije, ki je priložen temu poročilu. Komisija na podlagi teh ugotovitev ugotavlja, da vseh 11 držav in ozemelj še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz Evropske unije, v smislu splošne uredbe o varstvu podatkov, kot jo

³¹ Člen 12 zakona o varstvu zasebnosti, odlok št. 1 o dopolnitvi zakona o varstvu zasebnosti in odlok št. 2 o dopolnitvi zakona o varstvu zasebnosti.

³² Predpisi o varstvu zasebnosti (navodila za podatke, ki so bili v Izrael preneseni iz Evropskega gospodarskega prostora), 5783–2023, objavljeni v Uradnem listu Izraela (*Reshumut*) 7. maja 2023.

³³ Glej na primer Resolucijo Evropskega parlamenta z dne 25. marca 2021 o poročilu Komisije o oceni izvajanja Splošne uredbe o varstvu podatkov dve leti po začetku uporabe (2020/2717(RSP), ki je na voljo na naslednji povezavi: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_SL.html.

³⁴ Glej na primer stališče in ugotovitve Sveta o uporabi splošne uredbe o varstvu podatkov, ki so bili sprejeti 19. decembra 2019 in so na voljo na naslednji povezavi: <https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/sl/pdf>.

³⁵ Glej na primer Prispevek EOVP k oceni splošne uredbe o varstvu podatkov na podlagi člena 97, ki je bil sprejet 18. februarja 2020 in je na voljo na naslednji povezavi: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

³⁶ Glej na primer poročilo večdeležniške strokovne skupine za oceno splošne uredbe o varstvu podatkov, ki je na voljo na naslednji povezavi: <https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=sl&do=groupDetail.groupMeeting&meetingId=21356>.

razlaga Sodišče. Ugotovitve za posamezno ustrezno državo in ozemlje so povzete v nadaljevanju.

4.1. Andora

Komisija pozdravlja razvoj andorskega pravnega okvira od sprejetja sklepa o ustreznosti, vključno z zakonodajnimi spremembami in dejavnostmi nadzornih organov. Sprejetje organskega zakona 29/2021 o varstvu osebnih podatkov, ki je začel veljati maja 2022, je prispevalo k višji ravni varstva podatkov, saj je zakon po svoji strukturi in glavnih elementih tesno usklajen s splošno uredbo o varstvu podatkov.

Na področju vladnega dostopa do osebnih podatkov za javne organe v Andori veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko ti organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega pravnega okvira in mednarodnih zavez, zlasti iz andorske ustave, Evropske konvencije o človekovih pravicah (EKČP) in Konvencije Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108 in Protokol o spremembi, iz katerih izhaja posodobljena Konvencija št. 108+), pa tudi iz posebnih pravil o varstvu podatkov, ki se uporabljajo za obdelavo osebnih podatkov v okviru kazenskega pregona in so v bistvu enaki temeljnemu elementu Direktive (EU) 2016/680³⁷. Poleg tega po andorskem pravu velja več posebnih pogojev in omejitev glede dostopa javnih organov do osebnih podatkov in njihove uporabe teh podatkov, prav tako so zagotovljeni mehanizmi nadzora in pravnega varstva na tem področju.

Komisija na podlagi splošnih ugotovitev, predstavljenih v delovnem dokumentu služb Komisije, ugotavlja, da Andora še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz EU.

Komisija v zvezi s posebnimi pravili o varstvu podatkov, ki se trenutno uporabljajo za obdelavo podatkov s strani organov kazenskega pregona, pozdravlja namero andorskega zakonodajalca, da ta pravila nadomesti s celovitejšo ureditvijo, ki bo še skladnejša s pravili, ki se uporabljajo v EU. Komisija bo budno spremljala prihodnji razvoj dogodkov na tem področju.

4.2. Argentina

Komisija pozdravlja razvoj argentinskega pravnega okvira od sprejetja sklepa o ustreznosti, vključno z zakonodajnimi spremembami, sodno prakso in dejavnostmi nadzornih organov, ki je prispeval k višji ravni varstva podatkov. Natančneje, neodvisnost argentinskega nadzornega organa za varstvo podatkov je bila znatno okrepljena z odlokom št. 746/17, s katerim je *Agencia de Acceso a la Información Pública* (AAIP) pooblaščen za nadzor nad skladnostjo s pravom o varstvu podatkov. Poleg tega je agencija AAIP izdala več zavezujočih uredb in mnenj, s

³⁷ Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ.

katerimi je pojasnjeno, kako je treba okvir za varstvo podatkov razlagati in uporabljati v praksi, s čimer je prispevala k posodobitvi prava o varstvu podatkov. Argentina je okrepila tudi svoje mednarodne zaveze na področju varstva podatkov, saj se je leta 2019 pridružila Konvenciji Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov in njenemu dodatnemu protokolu ter leta 2023 ratificirala Protokol o spremembi, iz katerega izhaja posodobljena Konvencija št. 108+.

Na področju vladnega dostopa do osebnih podatkov za javne organe v Argentini veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko ti organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega pravnega okvira in mednarodnih zavez, zlasti argentinske ustave, Ameriške konvencije o človekovih pravicah, Konvencije št. 108 in Konvencije št. 108+, pa tudi iz argentinskih pravil o varstvu podatkov (zakon št. 25.326 o varstvu osebnih podatkov z dne 4. oktobra 2000), ki se prav tako uporabljajo za obdelavo osebnih podatkov s strani argentinskih javnih organov, med drugim za namene kazenskega pregona in nacionalne varnosti. Poleg tega po argentinskem pravu velja več posebnih pogojev in omejitev glede dostopa do osebnih podatkov in njihove uporabe za namene kazenskega pregona in nacionalne varnosti, zagotovljeni pa so tudi mehanizmi nadzora in pravnega varstva na tem področju.

Komisija na podlagi splošnih ugotovitev, predstavljenih v delovnem dokumentu služb Komisije, ugotavlja, da Argentina še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz EU.

Hkrati Komisija priporoča, da se v zakonodajo vključi varstvo, ki je bilo oblikovano na podzakonodajni ravni, da se poveča pravna varnost in uveljavijo te zahteve. Priložnost za kodifikacijo takega razvoja in s tem dodatno okrepitev argentinskega okvira za varstvo zasebnosti bi lahko predstavljal osnutek zakona o varstvu podatkov, ki je bil nedavno predložen v argentinskem kongresu. Komisija bo budno spremljala prihodnji razvoj dogodkov na tem področju.

4.3. Kanada

Komisija pozdravlja razvoj kanadskega pravnega okvira od sprejetja sklepa o ustreznosti, vključno z več zakonodajnimi spremembami, sodno prakso in dejavnostmi nadzornih organov, ki je prispeval k višji ravni varstva podatkov. Zakon o varstvu osebnih podatkov in elektronskih dokumentih (PIPEDA) je bil dodatno okrepljen z različnimi spremembami (npr. o pogojih za veljavno privolitev in obveščanju o kršitvah varstva podatkov), ključne zahteve glede varstva podatkov (npr. o obdelavi občutljivih podatkov) pa so bile dodatno pojasnjene s sodno prakso in smernicami, ki jih je izdal kanadski zvezni organ za varstvo podatkov, tj. urad pooblaščenca za zasebnost. Hkrati Komisija priporoča, da se v zakonodajo vključijo nekateri elementi varstva, ki so bili oblikovani na podzakonodajni ravni, da se poveča pravna varnost in uveljavijo te zahteve. Priložnost za kodifikacijo tega razvoja in s tem za dodatno okrepitev kanadskega okvira za varstvo zasebnosti bi lahko predstavljala zlasti tekoča zakonodajna reforma zakona PIPEDA. Komisija bo budno spremljala prihodnji razvoj dogodkov na tem področju.

Na področju vladnega dostopa do osebnih podatkov za javne organe v Kanadi veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko ti organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega ustavnega okvira (kanadska listina o pravicah in svoboščinah), sodne prakse, posebne zakonodaje, ki ureja dostop do podatkov, ter pravil o varstvu podatkov (tj. zakon o zasebnosti in podobni zakoni na ravni provinc), ki se prav tako uporabljajo za obdelavo osebnih podatkov s strani kanadskih javnih organov, med drugim za namene kazenskega pregona in nacionalne varnosti. Poleg tega kanadski pravni sistem na tem področju zagotavlja učinkovite mehanizme nadzora in pravnega varstva, med drugim z nedavno razširitvijo pravic posameznikov, na katere se nanašajo osebni podatki, in možnostmi pravnega varstva za nekanadske državljane ali rezidente.

Komisija na podlagi splošnih ugotovitev, predstavljenih v delovnem dokumentu služb Komisije, ugotavlja, da Kanada še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz EU prejemnikom, za katere velja zakon PIPEDA. Kot je navedeno zgoraj, je zakon PIPEDA trenutno predmet zakonodajne reforme, ki bi lahko dodatno okrepila varstvo zasebnosti, tudi na področjih, ki so pomembna za ugotovitev ustreznosti.

4.4. *Ferski otoki*

Komisija pozdravlja razvoj pravnega okvira Ferskih otokov od sprejetja sklepa o ustreznosti, vključno z zakonodajnimi spremembami, sodno prakso in dejavnostmi nadzornih organov, ki je prispeval k višji ravni varstva podatkov. Natančneje, Ferski otoki so svoj okvir za varstvo podatkov znatno posodobili s sprejetjem zakona o varstvu podatkov, ki je začel veljati leta 2021 in s katerim je bila ferska ureditev tesno usklajena s splošno uredbo o varstvu podatkov.

Na področju vladnega dostopa do osebnih podatkov za javne organe na Ferskih otokih veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko ti organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega pravnega okvira in mednarodnih zavez, zlasti ustavnega okvira in EKČP, pa tudi iz posebnih zakonov, ki urejajo vladni dostop do podatkov, in pravil o varstvu podatkov, ki se uporabljajo za obdelavo osebnih podatkov za namene kazenskega pregona (zakon o obdelavi osebnih podatkov s strani organov kazenskega pregona, ki je na Ferskih otokih začel veljati leta 2022, z njim pa je bila prenesena zakonodaja, ki jo je Danska sprejela za izvajanje Direktive (EU) 2016/680 na Ferskih otokih) in nacionalne varnosti (iz zakona o varnostni in obveščevalni službi). Poleg tega so na tem področju na voljo učinkoviti mehanizmi nadzora in pravnega varstva.

Komisija na podlagi splošnih ugotovitev, predstavljenih v delovnem dokumentu služb Komisije, ugotavlja, da Ferski otoki še naprej zagotavljajo ustrezno raven varstva osebnih podatkov, prenesenih iz EU.

4.5. *Guernsey*

Komisija pozdravlja razvoj pravnega okvira Guernseyja od sprejetja sklepa o ustreznosti, vključno z zakonodajnimi spremembami in dejavnostmi nadzornih organov, ki je prispeval k

višji ravni varstva podatkov. Natančneje, Guernsey je svoj okvir za varstvo podatkov znatno posodobil s sprejetjem zakona (Bailiffovega okrožja Guernsey) o varstvu podatkov iz leta 2017, ki se uporablja od leta 2019 in s katerim je ureditev Guernseyja tesno usklajena s splošno uredbo o varstvu podatkov.

Na področju vladnega dostopa do osebnih podatkov za javne organe na Guernseyju veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko taki organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega pravnega okvira in mednarodnih zavez, zlasti EKČP in Konvencije št. 108, pa tudi iz pravil Guernseyja o varstvu podatkov, vključno s posebnimi določbami za obdelavo osebnih podatkov v okviru kazenskega pregona, ki jih vsebuje odlok (Bailiffovega okrožja Guernsey) o varstvu podatkov (kazenski pregon in s tem povezane zadeve) iz leta 2018. Poleg tega po pravu Guernseyja velja več posebnih pogojev in omejitev glede dostopa do osebnih podatkov in njihove uporabe za namene kazenskega pregona in nacionalne varnosti, prav tako so zagotovljeni mehanizmi nadzora in pravnega varstva na tem področju.

Komisija na podlagi splošnih ugotovitev, predstavljenih v delovnem dokumentu služb Komisije, ugotavlja, da Guernsey še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz EU.

4.6. Otok Man

Komisija pozdravlja razvoj pravnega okvira Otoka Man od sprejetja sklepa o ustreznosti, vključno z zakonodajnimi spremembami in dejavnostmi nadzornih organov, ki je prispeval k višji ravni varstva podatkov. Natančneje, Otok Man je leta 2018 sprejel novo zakonodajo (zakon o varstvu osebnih podatkov iz leta 2018, ki je bil dopolnjen z odlokom o varstvu podatkov (uporaba splošne uredbe o varstvu podatkov) iz leta 2018), s katero je v pravni red Otoka Man vključena večina določb okvira EU za varstvo podatkov, hkrati pa so uvedene le manjše prilagoditve v zvezi s posebnimi vidiki, zlasti za prilagoditev okvira lokalnim razmeram.

Na področju vladnega dostopa do osebnih podatkov za javne organe na Otoku Man veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko ti organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega pravnega okvira in mednarodnih zavez, zlasti EKČP in Konvencije št. 108, pa tudi iz pravil Otoka Man o varstvu podatkov, vključno s posebnimi določbami za obdelavo osebnih podatkov v okviru kazenskega pregona, ki jih vsebujejo odlok o varstvu podatkov (uporaba direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj) iz leta 2018 ter izvedbene uredbe o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj iz leta 2018. Poleg tega po pravu Otoka Man velja več posebnih omejitev glede dostopa do osebnih podatkov in njihove uporabe za namene kazenskega pregona in nacionalne varnosti, prav tako so zagotovljeni mehanizmi nadzora in pravnega varstva na tem področju.

Komisija na podlagi splošnih ugotovitev, predstavljenih v delovnem dokumentu služb Komisije, ugotavlja, da Otok Man še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz EU.

4.7. *Izrael*

Komisija pozdravlja razvoj izraelskega pravnega okvira od sprejetja sklepa o ustreznosti, vključno z zakonodajnimi spremembami, sodno prakso in dejavnostmi nadzornih organov, ki je prispeval k višji ravni varstva podatkov. Natančneje, Izrael je uvedel posebne zaščitne ukrepe za okrepitev varstva osebnih podatkov, prenesenih iz Evropskega gospodarskega prostora, s sprejetjem predpisov o varstvu zasebnosti (navodila za podatke, ki so bili v Izrael preneseni iz Evropskega gospodarskega prostora), 5783–2023. Prav tako je okreplil zahteve glede varstva podatkov, in sicer s sprejetjem predpisov o varstvu zasebnosti (varnost podatkov), 5777–2017, neodvisnost svojega nadzornega organa za varstvo podatkov pa je utrdil z zavezujočo vladno resolucijo.

Na področju vladnega dostopa do osebnih podatkov za javne organe v Izraelu veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko ti organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega pravnega okvira, zlasti iz izraelske ustave, pa tudi iz zakona o varstvu zasebnosti, 5741–1981, in uredb, ki so bile sprejete na njegovi podlagi in se uporabljajo za obdelavo osebnih podatkov s strani izraelskih javnih organov, med drugim za namene kazenskega pregona in nacionalne varnosti. Poleg tega po izraelskem pravu velja več posebnih omejitev glede dostopa do osebnih podatkov in njihove uporabe za namene kazenskega pregona in nacionalne varnosti, prav tako so zagotovljeni mehanizmi nadzora in pravnega varstva na tem področju.

Komisija na podlagi splošnih ugotovitev, predstavljenih v delovnem dokumentu služb Komisije, ugotavlja, da Izrael še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz EU.

Hkrati Komisija priporoča, da se v zakonodajo vključi varstvo, ki je bilo oblikovano na podzakonodajni ravni in s sodno prakso, da se poveča pravna varnost in uveljavijo te zahteve. Pomembno priložnost za uveljavitev in kodifikacijo tega razvoja ter s tem nadaljnjo okrepitev izraelskega okvira za zasebnost predstavlja osnutek zakona o varstvu zasebnosti (sprememba št. 14), 5722–2022, ki je bil nedavno predložen v izraelskem parlamentu. Komisija bo budno spremljala prihodnji razvoj dogodkov na tem področju.

4.8. *Jersey*

Komisija pozdravlja razvoj pravnega okvira Jerseyja od sprejetja sklepa o ustreznosti, vključno z zakonodajnimi spremembami, sodno prakso in dejavnostmi nadzornih organov, ki je prispeval k višji ravni varstva podatkov. Natančneje, Jersey je svoj okvir za varstvo podatkov znatno posodobil s sprejetjem zakona (Jerseyja) o varstvu podatkov iz leta 2018 in zakona (Jerseyja) o organu za varstvo podatkov iz leta 2018, ki sta začela veljati leta 2018 in s katerima je ureditev Jerseyja tesno usklajena s splošno uredbo o varstvu podatkov.

Na področju vladnega dostopa do osebnih podatkov za javne organe v Jerseyju veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko ti organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega pravnega okvira in mednarodnih zavez, zlasti EKČP in Konvencije št. 108, pa tudi iz pravil Jerseyja o varstvu podatkov, vključno s posebnimi določbami za obdelavo osebnih podatkov v okviru kazenskega pregona, ki jih vsebuje zakon (Jerseyja) o varstvu podatkov iz leta 2018, kakor je bil spremenjen s Prilogo 1 k navedenemu zakonu. Poleg tega po pravu Jerseyja velja več posebnih omejitev glede dostopa do osebnih podatkov ter njihove uporabe za namene kazenskega pregona in nacionalne varnosti, prav tako so zagotovljeni mehanizmi nadzora in pravnega varstva na tem področju.

Komisija na podlagi splošnih ugotovitev, predstavljenih v delovnem dokumentu služb Komisije, ugotavlja, da Jersey še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz EU.

4.9. Nova Zelandija

Komisija pozdravlja razvoj pravnega okvira Nove Zelandije od sprejetja sklepa o ustreznosti, vključno z zakonodajnimi spremembami, sodno prakso in dejavnostmi nadzornih organov, ki je prispeval k višji ravni varstva podatkov. Natančneje, izvedena je bila celovita reforma ureditve varstva podatkov, in sicer s sprejetjem zakona o zasebnosti iz leta 2020, ki je še povečal zbliževanje z okvirom EU za varstvo podatkov, zlasti kar zadeva pravila za mednarodne prenose osebnih podatkov in pooblastila organa za varstvo podatkov (urad pooblaščenca za varstvo zasebnosti).

Na področju vladnega dostopa do osebnih podatkov za javne organe na Novi Zelandiji veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko ti organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega ustavnega okvira (npr. zakona o listini o pravicah) in sodne prakse, pa tudi iz posebnih zakonov, ki urejajo vladni dostop do podatkov, in določb zakona o zasebnosti, ki se prav tako uporabljajo za obdelavo osebnih podatkov s strani organov kazenskega pregona in nacionalnih varnostnih organov. Poleg tega so v pravnem sistemu Nove Zelandije zagotovljeni različni mehanizmi nadzora in pravnega varstva na tem področju.

Komisija na podlagi splošnih ugotovitev, predstavljenih v delovnem dokumentu služb Komisije, ugotavlja, da Nova Zelandija še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz EU. Pozdravlja tudi dejstvo, da je vlada Nove Zelandije nedavno v parlamentu predložila osnutek zakona za spremembo zakona o zasebnosti iz leta 2020, da bi se dodatno okrepile obstoječe zahteve glede preglednosti. Komisija bo budno spremljala prihodnji razvoj dogodkov na tem področju.

4.10. Švica

Komisija pozdravlja razvoj švicarskega pravnega okvira od sprejetja sklepa o ustreznosti, vključno z zakonodajnimi spremembami, sodno prakso in dejavnostmi nadzornih organov, ki je prispeval k višji ravni varstva podatkov. Natančneje, posodobljen je bil zvezni zakon o varstvu podatkov, s čimer se je še povečalo zbliževanje z okvirom EU za varstvo podatkov, zlasti v zvezi z varstvom občutljivih podatkov in pravili o mednarodnih prenosih podatkov. Švica je okrepila tudi svoje mednarodne zaveze na področju varstva podatkov, in sicer z ratifikacijo Konvencije št. 108+ septembra 2023.

Na področju vladnega dostopa do osebnih podatkov za javne organe v Švici veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko ti organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega pravnega okvira in mednarodnih zavez, zlasti iz švicarske zvezne ustave, EKČP in Konvencije št. 108+, pa tudi iz švicarskih pravil o varstvu podatkov, vključno z zveznim zakonom o varstvu podatkov in posebnimi pravili o varstvu podatkov, ki se uporabljajo za kazenski pregon (npr. zakonik o kazenskem postopku) in nacionalne varnostne organe (npr. zakon o obveščevalnih službah). Poleg tega po švicarskem pravu velja več posebnih omejitev glede dostopa do osebnih podatkov in njihove uporabe za namene kazenskega pregona in nacionalne varnosti, prav tako so zagotovljeni mehanizmi nadzora in pravnega varstva na tem področju.

Komisija na podlagi splošnih ugotovitev, predstavljenih v delovnem dokumentu služb Komisije, ugotavlja, da Švica še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz EU.

4.11. Urugvaj

Komisija pozdravlja razvoj urugvajskega pravnega okvira od sprejetja sklepa o ustreznosti, vključno z več zakonodajnimi spremembami, sodno prakso in dejavnostmi nadzornih organov, ki je prispeval k višji ravni varstva podatkov. Natančneje, Urugvaj je posodobil in okrepil zakon št. 18.331 o varstvu osebnih podatkov in pravnem sredstvu *Habeas Data* iz leta 2008, in sicer z zakonodajnimi spremembami v letih 2018 in 2020, s katerimi je bilo razširjeno ozemeljsko področje uporabe zakonodaje o varstvu podatkov, ustvarjene so bile nove zahteve glede odgovornosti (kot so ocene učinka, vgrajeno in privzeto varstvo podatkov, obveščanje o kršitvah varstva podatkov in imenovanje pooblaščenecov za varstvo podatkov) in uvedeno je bilo dodatno varstvo biometričnih podatkov. Urugvaj je okrepil tudi svoje mednarodne zaveze na področju varstva podatkov, in sicer s pristopom h Konvenciji št. 108 leta 2019 in ratifikacijo Konvencije št. 108+ leta 2021.

Na področju vladnega dostopa do osebnih podatkov za javne organe v Urugvaju veljajo jasna, natančna in dostopna pravila, v skladu s katerimi lahko ti organi dostopajo do podatkov, prenesenih iz EU, in jih nato uporabijo za cilje javnega interesa, zlasti za namene kazenskega pregona in nacionalne varnosti. Te omejitve in zaščitni ukrepi izhajajo iz splošnega pravnega okvira in mednarodnih zavez, zlasti iz urugvajske ustave, Ameriške konvencije o človekovih pravicah, Konvencije št. 108 in Konvencije št. 108+, pa tudi iz pravil o varstvu podatkov, vsebovanih v zakonu št. 18.331 o varstvu osebnih podatkov in pravnem sredstvu *Habeas Data*, ki se uporabljajo za obdelavo osebnih podatkov s strani javnih organov v Urugvaju, zlasti za

namene kazenskega pregona in nacionalne varnosti. Poleg tega po urugvajskem pravu velja več posebnih pogojev in omejitev glede dostopa javnih organov do osebnih podatkov in njihove uporabe teh podatkov, prav tako so zagotovljeni mehanizmi nadzora in pravnega varstva na tem področju.

Komisija na podlagi splošnih ugotovitev v okviru tega prvega pregleda ugotavlja, da Urugvaj še naprej zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz EU.

5. PRIHODNJE SPREMLJANJE IN SODELOVANJE

Komisija potrjuje in zelo ceni odlično sodelovanje z ustreznimi organi v vseh zadevnih državah in ozemljih pri izvedbi tega pregleda. Še naprej bo pozorno spremljala razvoj na področju okvirov za varstvo ter dejansko prakso zadevnih držav in ozemelj. V primeru razvoja dogodkov v ustrezni državi oziroma ozemlju, ki bi negativno vplival na raven varstva podatkov, ki se šteje za ustrezno, bo po potrebi uporabila svoja pooblastila na podlagi člena 45(5) splošne uredbe o varstvu podatkov in začasno odložila, spremenila ali razveljavila sklep o ustreznosti.

Ta pregled potrjuje, da sprejetje sklepa o ustreznosti ni „končni cilj“, temveč priložnost za nadaljnjo krepitev dialoga in sodelovanja s podobno mislečimi mednarodnimi partnericami na področju pretoka podatkov in digitalnih zadev na splošno. V zvezi s tem Komisija z zanimanjem pričakuje prihodnje izmenjave z ustreznimi organi za nadaljnjo krepitev sodelovanja na mednarodni ravni pri spodbujanju varnega in prostega pretoka podatkov, med drugim z okrepljenim sodelovanjem pri izvrševanju. Da bi pospešila ta dialog ter spodbudila izmenjavo informacij in izkušenj, namerava leta 2024 organizirati srečanje na visoki ravni, na katerem bodo sodelovali predstavniki EU in vseh držav, za katere je bil sprejet sklep o ustreznosti.