Council of the
European Union

Brussels, 22 January 2024
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2024) 7 final
Subject:	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC

Delegations will find attached document COM(2024) 7 final.

Encl.: COM(2024) 7 final

EUROPEAN
COMMISSION

Brussels, 15.1.2024
COM(2024) 7 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC

{SWD(2024) 3 final}

1. THE FIRST REVIEW – BACKGROUND AND CONTEXT

The present report contains the findings of the Commission on the first review of the adequacy decisions that were adopted on the basis of Article 25(6) of Directive 95/46/EC[1] (Data Protection Directive).

In these decisions, the Commission determined that eleven countries or territories ensure an adequate level of protection for personal data transferred from the European Union (EU)[2]: Andorra[3], Argentina[4], Canada (for commercial operators)[5], Faroe Islands[6], Guernsey[7], Isle of Man[8], Israel[9], Jersey[10], New Zealand[11], Switzerland[12], and Uruguay[13]. As a result, data transfers from the EU to these countries or territories can take place without additional requirements.

With the entry into application of Regulation (EU) 2016/679[14] (GDPR) on 25 May 2018, the adequacy decisions adopted under the Data Protection Directive remained in force[15]. At the

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

[2] Following its incorporation in the European Economic Area (EEA) Agreement, the GDPR also applies to Norway, Iceland and Liechtenstein. References to the EU in this report should be understood as also covering the EEA States.

[3] Commission Decision 2010/625/EU of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra, OJ L 277, 21.10.2010, p. 27.

[4] Commission Decision 2003/490/EC of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, OJ L 168, 5.7.2003, p. 19.

[5] Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, OJ L 2, 4.1.2002, p. 13.

[6] Commission Decision 2010/146/EU of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data, OJ L 58, 9.3.2010, p. 17.

[7] Commission Decision 2003/821/EC of 21 November 2003 on the adequate protection of personal data in Guernsey, OJ L 308, 25.11.2003, p. 27.

[8] Commission Decision 2004/411/EC of 28 April 2004 on the adequate protection of personal data in the Isle of Man, OJ L 151, 30.4.2004, p. 48.

[9] Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, OJ L 27, 1.2.2011, p. 39.

[10] Commission Decision 2008/393/EC of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey, OJ L 138, 28.5.2008, p. 21.

[11] Commission Implementing Decision 2013/65/EU of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, OJ L 28, 30.1.2013, p. 12.

[12] Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, OJ L 215, 25.08.2000, p. 1.

[13] Commission Implementing Decision 2012/484/EU of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data, OJ L 227, 23.8.2012, p. 11.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

[15] See Article 45(9) GDPR, which provides that decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, repealed or replaced by a Commission decision adopted in accordance with paragraph 3 or 5 of Article 45.

same time, the GDPR has clarified that adequacy findings are 'living instruments', stipulating that the Commission must, on an ongoing basis, monitor developments in third countries that could affect the functioning of existing adequacy decisions[16]. In addition, Article 97 of the GDPR requires the Commission to periodically review these decisions, every four years, in order to determine whether the countries and territories that received an adequacy finding continue to provide an adequate level of protection for personal data.

This first review of the adequacy decisions adopted under the former EU data protection framework was initiated as part of a broader evaluation of the application and functioning of the GDPR on which the Commission presented its findings in its "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"[17]. However, the conclusion of this aspect of the review was postponed in order the take into account the judgment of the Court of Justice in the *Schrems II* case[18], in which the Court provided important clarifications on key elements of the adequacy standard, as well as other related developments. In turn, this led to detailed exchanges with the countries and territories concerned on relevant aspects of their legal framework, oversight mechanisms and enforcement system[19]. The present report takes full account of all these developments, both in the EU and the third countries and territories concerned.

Importantly, this first review takes place against the backdrop of the exponential development of digital technologies. Over the past decades, the importance of adequacy decisions has increased considerably as data flows have become an integral element of the digital transformation of the society and the globalisation of the economy. The transfer of data across borders has become part of the daily operations of European companies of all sizes, across all sectors. More than ever before, respecting privacy is a condition for stable, secure, and competitive commercial flows. In that context, adequacy decisions play an increasingly key role, in many ways. By ensuring that protection travels with the data, they enable safe data flows, respectful of individuals' rights in line with the EU human-centred approach to the digital transformation. By involving a recognition of a third countries' privacy framework as delivering a level of protection that is essentially equivalent to the EU one, they promote convergence between privacy systems based on high standards of protection. Moreover, as explained in this report, rather than being an 'end point', adequacy decisions have laid the foundation for closer cooperation and further regulatory convergence between the EU and like-minded partners. By enabling the free flow of personal data, these decisions have opened up

[16] Article 45(4) GDPR. See also Judgment of the Court of Justice of the EU of 6 October 2015 in Case C-362/14, Maximillian Schrems v Data Protection Commissioner (*Schrems I*), ECLI:EU:C:2015:650, point 76.

[17] The Communication was published in June 2020 and is available at the following link: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en.

[18] Judgment of the Court of Justice of the EU of 16 July 2020 in Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd. and Maximilian Schrems (*Schrems II*), ECLI:EU:C:2020:559.

[19] The adequacy decision concerning Japan was adopted on the basis of the GDPR and provides for a separate periodic review. The first review was concluded in April 2023 with the Commission's report to the European Parliament and the Council on the first review of the functioning of the adequacy decision for Japan, COM(2023) 275 final, available at the following link https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2023:275:FIN.

commercial channels for EU operators, including by complementing and amplifying the benefits of trade agreements, as well as eased cooperation with foreign partners in a broad range of regulatory fields. By providing a straightforward and comprehensive solution for data transfers without the need for the data exporter to provide further safeguards or obtain any authorisation, they facilitate compliance, in particular by small and medium enterprises, with the international transfer requirements of the GDPR. Finally, thanks to their 'network effect' adequacy decisions adopted by the European Commission are increasingly relevant also beyond theEU, as they do not only allow for the free flow of data with the 30 economies of the EU, but also with many more jurisdictions around the globe[20] that recognise countries for which there is an EU adequacy decision as 'safe destinations' under their own data protection rules.

For all these reasons, as also confirmed by the intense and fruitful dialogue with the third countries/territories concerned underpinning this review, adequacy decisions have become a strategic component of the overall relationship of the EU with these foreign partners and are recognised as a major enabler for deepening cooperation in a broad range of areas. It is therefore particularly important that these decisions can stand the test of time and address new developments and challenges.

2. OBJECT AND METHODOLOGY OF THE REVIEW

The adequacy decisions that are subject to this review have been adopted under the EU data protection framework that preceded the GDPR. While the most recent decisions date back about a decade (e.g., the decisions on New Zealand and Uruguay, both adopted in 2012), others have been in force for more than twenty years (e.g., Canada, adopted in 2001, and Switzerland, adopted in 2000). Since then, the data protection frameworks in all eleven countries and territories have evolved, for instance through legislative or regulatory reforms, developments in the enforcement practice of data protection authorities or case law.

In carrying out its evaluation, the Commission has therefore focussed on developments in the data protection frameworks of the relevant countries and territories that took place since the adoption of the adequacy decision. It has assessed how these developments have further shaped the data protection landscape of the relevant country or territory, and whether, considering these developments, the various regimes continue to ensure an adequate level of protection.

To that end, the evolution of the EU's own data protection regime, in particular with the entry into application of the GDPR, was fully taken into account. In particular, since the adoption of these adequacy decisions, the legal standard applicable to such decisions, as well as the elements relevant for assessing whether a foreign system ensures an adequate level of protection, have been further clarified through the case law of the Court of Justice and the guidance adopted by the Article 29 Working Party and its successor, the European Data Protection Board[21] (EDPB).

[20] Such as e.g., Argentina, Colombia, Israel, Morocco, Switzerland and Uruguay.
[21] The European Data Protection Board gathers the Data Protection Supervisory Authorities in the Member States and the European Data Protection Supervisor.

Notably, the Court of Justice in its ruling of 6 October 2015 in *Schrems I* established that, while a third country cannot be required to ensure a level of protection that is identical to the one guaranteed in the EU, the adequacy test must be understood as requiring an 'essentially equivalent' level of protection[22]. In particular, the Court clarified the means to which the third country in question has recourse for protecting personal data may differ from the ones employed in the Union, as long as they prove, in practice, effective for ensuring an adequate level of protection[23]. The adequacy test therefore requires a comprehensive assessment of the third country's system as a whole, including the substance of privacy protections, their effective implementation and enforcement.

Moreover, the Court clarified that the Commission's assessment should not be limited to the general data protection framework of the third country but should also include the rules governing access to personal data by public authorities, in particular for law enforcement and national security purposes[24]. Using the Charter of Fundamental Rights as a benchmark, the Court identified several requirements these rules should comply with to meet the 'essential equivalence' standard. For example, legislation in this area should lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data[25]. It should also provide individuals with the possibility to pursue legal remedies in order to have access to personal data relating to them, or to obtain the rectification or erasure of such data[26].

The GDPR has built upon the clarifications provided by the Court of Justice by setting out a detailed catalogue of elements that the Commission must take into account in an adequacy assessment[27]. Moreover, in its *Schrems II* ruling of 16 July 2020, the Court of Justice has further elaborated on the standard of 'essential equivalence', in particular with respect to the rules on access to personal data by public authorities for law enforcement and national security purposes. In particular, it has clarified that the 'essential equivalence' standard requires that relevant legal frameworks binding public authorities in the third countries and territories concerned include minimum safeguards ensuring that such authorities cannot access data beyond what is necessary and proportionate to pursue legitimate objectives, and data subjects enjoy effective and enforceable rights against such authorities[28].

The evolution of the adequacy standard is also reflected in the guidance that was originally adopted by the Article 29 Working Party and then endorsed by the EDPB[29]. This guidance, and in particular the so-called "adequacy referential", further clarifies the elements the Commission

[22] *Schrems I*, points 73, 74 and 96. See also Recital 104 of Regulation (EU) 2016/679, which refers to the standard of essential equivalence.
[23] *Schrems I*, point 74.
[24] *Schrems I*, point 90.
[25] *Schrems I*, point 91.
[26] *Schrems I*, point 95.
[27] Article 45(2) GDPR.
[28] *Schrems II*, points 180-182.
[29] Adequacy Referential, WP 254 rev. 01, 6 February 2018 (available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

must take into account when carrying out an adequacy assessment, including by providing an overview of 'essential guarantees' for access to personal data by public authorities. The latter builds in particular on the case law of the European Court of Human Rights and was updated by the EDPB to take into account the clarifications provided by the Court of Justice in the *Schrems II* judgment[30]. Importantly, the adequacy referential also acknowledges that the standard of 'essential equivalence' does not involve a point-to-point replication ('photocopy') of EU rules, given that the means of ensuring a comparable level of protection may vary between different privacy systems, often reflecting different legal traditions.

Therefore, to determine whether the eleven adequacy decisions adopted under the former rules continue to meet the standard set by the GDPR, the Commission has not only taken into account the evolution of the data protection frameworks in the countries and territories concerned, but also the evolution in the interpretation under EU law of the adequacy standard itself. This also includes an assessment of the legal framework governing the access to and use of personal data transferred from the EU by public authorities of the countries or territories that were found to provide an adequate level of protection on the basis of Article 25(6) of the Data Protection Directive.

3. REVIEW PROCESS

As described above, for each of the countries or territories concerned, the evaluation of the existing adequacy decisions covers the data protection framework and any developments with respect to that legal framework since the adequacy finding was adopted, as well as the rules governing government access to data – in particular, for law enforcement and national security purposes. In the past years, the Commission services have taken several steps to conduct this assessment, in close cooperation with each of the relevant countries or territories.

To assist the Commission with its monitoring obligations, each of the eleven countries or territories provided the Commission with comprehensive information on developments in its data protection regime since the adoption of the adequacy decision. In addition, from each of the eleven countries or territories the Commission sought detailed information concerning the rules on government access to personal data, in particular for law enforcement and national security purposes that apply in the relevant country or territory. The Commission also sought information from public sources, oversight and enforcement authorities as well from local experts on the functioning of the decisions and on relevant developments in the law and practice of each of the countries and territories concerned, both as regards the data protection rules applicable to private operators and with respect to government access. Finally, where relevant, due account has been taken of the international commitments subscribed by these countries/territories under regional or universal instruments.

On that basis, the Commission has engaged in an intense dialogue with each of the countries and territories concerned. In the context of this dialogue, many of said countries and territories

[30] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en).

have modernised and strengthened their privacy legislation through comprehensive or partial reforms (e.g., Andorra, Canada, Faroe Island, Switzerland, New Zealand), prompted amongst other by the need to ensure the continuity of the adequacy decisions. Some of these countries have adopted regulations and/or guidance by their data protection authority to introduce new data protection requirements (e.g., Israel, Uruguay) or clarifying certain privacy rules (e.g., Argentina, Canada, Guernsey, Jersey, Isle of Man, Israel, New Zealand), building on enforcement practice or case law. Moreover, in order to address relevant differences in the level of protection, additional safeguards for personal data transferred from Europe have been – when needed to ensure the continuity of the adequacy decision– negotiated and agreed with some of the countries and territories concerned. For example, the Canadian government extended the rights of access and correction with respect to personal data processed by the public sector to all individuals, regardless of their nationality or place of residence (whereas these rights were in the past only available to Canadian citizens, permanent residents or individuals present in Canada)[31]. As another example, the Israeli government introduced specific safeguards to reinforce the protection of personal data transferred from the European Economic Area which notably create new obligations in the area of data accuracy and data retention, strengthen the rights to information and deletion and introduce additional categories of sensitive data[32].

In parallel, the Commission services gathered the views of and regularly informed the European Parliament (committee on Civil Liberties, Justice and Home Affairs)[33] the Council (through the Data Protection Working Party)[34], the EDPB[35], and the GDPR Multi-Stakeholder Expert Group[36] (which includes representatives of civil society, industry, academia and legal practitioners) on the progress of the evaluation.

This report and the accompanying Staff Working Document (SWD) are therefore the result of close cooperation with each of the countries and territories concerned, as well as consultation with and feedback from relevant EU institutions and bodies. They rely on a variety of sources, including legislation, regulatory acts, case law, decisions and guidance from data protection authorities, reports from (independent) oversight bodies and input from stakeholders. Prior to the adoption of this report, all of the afforementioned countries and territories have been given the opportunity to verify the factual accuracy of the information provided on their system in the SWD.

---

[31] Section 12 of the Privacy Act, Privacy Act Extension Order, No. 1 and Privacy Act Extension Order, No. 2.
[32] Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023, published in the Israeli Official Gazette (*Reshumut*) on 7 May 2023.
[33] See, e.g., European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP), available at the following link: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EN.html.
[34] See, e.g., Council position and findings on the application of the General Data Protection Regulation (GDPR), adopted on 19 December 2019, available at the following link: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf.
[35] See e.g. contribution of the EDPB to the evaluation of the GDPR under Article 97, adopted on 18 February 2020, available at the following link: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.
[36] See, e.g., the report from the Multistakeholder Expert Group on the GDPR evaluation, available at the following link: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&do=groupDetail.groupMeeting&meetingId=21356.

4. MAIN FINDINGS AND CONCLUSIONS

The first review has demonstrated that since the adoption of the adequacy decisions, the data protection frameworks in place in each of the eleven countries or territories have further converged with the framework of the EU. Moreover, in the area of government access to personal data, the first review has shown that the law of these countries or territories imposes appropriate safeguards and limitations and provides oversight and redress mechanisms in this area.

The detailed findings concerning each of the eleven countries or territories are presented in the Commission SWD which accompanies the present report. Based on these findings, the Commission concludes that each of the eleven countries and territories continues to ensure an adequate level of protection for personal data transferred from the European Union within the meaning of the GDPR, as interpreted by the Court of Justice. The findings for each of the adequate countries and territories are summarised below.

4.1. Andorra

The Commission welcomes the developments in the Andorran legal framework since the adoption of the adequacy decision, including legislative amendments and activities of supervisory bodies. In particular, the adoption of Qualified Law 29/2021 on the protection of personal data that entered into force in May 2022 has contributed to an increased level of data protection, as the Law is closely aligned with the GDPR in its structure and main components.

In the area of government access to personal data, public authorities in Andorra are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching legal framework and international commitments, notably the Andorran Constitution, the European Convention on Human Rights (ECHR) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108 and the amending Protocol, creating the modernised Convention 108+), as well as from specific data protection rules applying to the processing of personal data in the law enforcement context that essentially replicate the core elements of the Directive (EU) 2016/680[37]. In addition, Andorran law imposes a number of specific conditions and limitations on the access to and use of personal data by public authorities, and it provides oversight and redress mechanisms in this area.

Based on the overall findings set out in the SWD, the Commission concludes that Andorra continues to provide an adequate level of protection for personal data transferred from the EU.

[37] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

With respect to the specific data protection rules that currently apply to data processing by law enforcement authorities, the Commission welcomes the Andorran legislator's intention to replace these rules with a more comprehensive regime that will be even further aligned with the rules that apply in the EU. The Commission will closely monitor future developments in this area.

4.2. Argentina

The Commission welcomes the developments in the Argentinian legal framework since the adoption of the adequacy decision, including legislative amendments, case law and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, the independence of the Argentinian data protection supervisory authority, was significantly strengthened through Decree No. 746/17, which entrusted the *Agencia de Acceso a la Información Pública* (AAIP) with the responsibility for overseeing compliance with the data protection law. In addition, the AAIP issued a number of binding regulations and opinions which clarify how the data protection framework is to be interpreted and applied in practice, thus helping to keep the data protection law up to date. Argentina also strengthened its international commitments in the field of data protection by joining the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data and its additional Protocol in 2019, and by ratifying the amending Protocol creating the modernised Convention 108+ in 2023.

In the area of government access to personal data, public authorities in Argentina are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching legal framework and international commitments, notably the Argentinian Constitution, the American Convention on Human Rights, Convention 108 and Convention 108+, as well as from the Argentinian data protection rules (Law 25.326 on Personal Data Protection of 4 October 2000) that are also applicable to the processing of personal data by Argentinian public authorities, including for law enforcement and national security purposes. In addition, Argentinian law imposes a number of specific conditions and limitations on the access to and use of personal data for criminal law enforcement and national security purposes, and it provides oversight and redress mechanisms in this area.

Based on the overall findings set out in the SWD, the Commission concludes that Argentina continues to provide an adequate level of protection for personal data transferred from the EU.

At the same time, the Commission recommends enshrining the protections that have been developed at sub-legislative level in legislation to enhance legal certainty and consolidate these requirements. The draft Data Protection Bill that was recently introduced in the Argentinian Congress could offer an opportunity to codify such developments, and thereby further strengthen the Argentinian privacy framework. The Commission will closely monitor future developments in this area.

4.3. Canada

The Commission welcomes the developments in the Canadian legal framework since the adoption of the adequacy decision, including several legislative amendments, case law and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, the Personal Information Protection and Electronic Documents Act (PIPEDA) has been further strengthened through different amendments (e.g., on the conditions for valid consent and data breach notifications), while key data protection requirements (e.g., on the processing of sensitive data) have been further clarified through case law as well as guidance issued by the Canadian federal data protection authority, the Office of the Privacy Commissioner. At the same time, the Commission recommends enshrining some of the protections that have been developed at sub-legislative level in legislation to enhance legal certainty and consolidate these requirements. The ongoing legislative reform of PIPEDA could notably offer an opportunity to codify such developments, and thereby further strengthen the Canadian privacy framework. The Commission will closely monitor future developments in this area.

In the area of government access to personal data, public authorities in Canada are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching constitutional framework (the Canadian Charter of Rights and Freedoms), case law, specific legislation regulating access to data, as well as data protection rules (i.e., the Privacy Act and similar laws at provincial level) that also apply to the processing of personal data by Canadian public authorities, including for law enforcement and national security purposes. In addition, the Canadian legal system provides effective oversight and redress mechanisms in this area, including through a recent extension of data subject rights and redress possibilities for non-Canadian nationals or residents.

Based on the overall findings set out in the SWD, the Commission concludes that Canada continues to provide an adequate level of protection for personal data transferred from the EU to recipients subject to PIPEDA. As noted above, PIPEDA is currently subject to a legislative reform which could further strengthen privacy protections, including in areas that are relevant for the adequacy finding.

4.4. Faroe Islands

The Commission welcomes the developments in the legal framework of the Faroe Islands since the adoption of the adequacy decision, including legislative amendments, case law and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, the Faroe Islands have significantly modernised their data protection framework by adopting the Data Protection Act, which entered into force in 2021 and closely aligned the Faroese regime with the GDPR.

In the area of government access to personal data, public authorities in the Faroe Islands are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards

follow from the overarching legal framework and international commitments, notably the constitutional framework and the ECHR , as well as from specific laws regulating government access to data and data protection rules that apply to the processing of personal data for criminal law enforcement (the Act on the Processing of Personal Data by Law Enforcement Authorities that was set into force in the Faroe Islands in 2022 and transposes the legislation that was adopted by Denmark to implement Directive (EU) 2016/680 in the Faroe Islands) and national security purposes (contained in the Act on the Security and Intelligence Service). In addition, effective oversight and redress mechanisms are available in this area.

Based on the overall findings set out in the SWD, the Commission concludes that the Faroe Islands continue to provide an adequate level of protection for personal data transferred from the EU.

4.5. Guernsey

The Commission welcomes the developments in the Guernsey legal framework since the adoption of the adequacy decision, including legislative amendments and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, Guernsey has significantly modernised its data protection framework by adopting the Data Protection (Bailiwick of Guernsey) Law 2017 which applies since 2019 and aligns the Guernsey regime closely with the GDPR.

In the area of government access to personal data, public authorities in Guernsey are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching legal framework and international commitments, notably the ECHR and Convention 108, as well as from Guernsey data protection rules, including the specific provisions for the processing of personal data in the law enforcement context set out in the Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018. In addition, Guernsey law imposes a number of specific conditions and limitations on the access to and use of personal data for criminal law enforcement and national security purposes, and it provides oversight and redress mechanisms in this area.

Based on the overall findings set out in the SWD, the Commission concludes that Guernsey continues to provide an adequate level of protection for personal data transferred from the EU.

4.6. Isle of Man

The Commission welcomes the developments in the Manx legal framework since the adoption of the adequacy decision, including legislative amendments and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, the Isle of Man adopted new legislation in 2018 (the Data Protection Act 2018, complemented by the Data Protection (Application of GDPR) Order 2018) that incorporates most of the provisions of the EU's data protection framework into the Manx legal order while making only minor adjustments on specific aspects, in particular to adapt the framework to the local context.

In the area of government access to personal data, public authorities in the Isle of Man are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching legal framework and international commitments, notably the ECHR and Convention 108, as well as from Manx data protection rules, including the specific provisions for the processing of personal data in the law enforcement context set out in the Data Protection (Application of LED) Order 2018 and the LED Implementing Regulations 2018. In addition, Manx law imposes a number of specific limitations on the access to and use of personal data for criminal law enforcement and national security purposes, and it provides oversight and redress mechanisms in this area.

Based on the overall findings set out in the SWD, the Commission concludes that the Isle of Man continues to provide an adequate level of protection for personal data transferred from the EU.

4.7. Israel

The Commission welcomes the developments in the Israeli legal framework since the adoption of the adequacy decision, including legislative amendments, case law and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, Israel introduced specific safeguards to reinforce the protection of personal data transferred from the European Economic Area by adopting Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023. Israel also strengthened the requirements for data security by adopting Privacy Protection (Data Security) Regulations, 5777-2017 and consolidated the independence of its data protection supervisory authority in a binding government resolution.

In the area of government access to personal data, public authorities in Israel are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching legal framework, notably the Israeli Basic Law, as well as from the Protection of Privacy Law, 5741-1981 and the Regulations adopted thereunder, which apply to the processing of personal data by Israeli public authorities, including for law enforcement and national security purposes. In addition, Israeli law imposes a number of specific limitations on the access to and use of personal data for criminal law enforcement and national security purposes, and it provides oversight and redress mechanisms in this area.

Based on the overall findings set out in the SWD, the Commission concludes that Israel continues to provide an adequate level of protection for personal data transferred from the EU.

At the same time, the Commission recommends enshrining in legislation the protections that have been developed at sub-legislative level and by case law, in order to enhance legal certainty and solidify these requirements. The Privacy Protection Bill (Amendment No. 14), 5722-2022 that has recently been introduced into the Israeli Parliament offers an important opportunity to

consolidate and codify such developments, and thereby further strengthen the Israeli privacy framework. The Commission will closely monitor future developments in this area.

4.8. Jersey

The Commission welcomes the developments in the Jersey legal framework since the adoption of the adequacy decision, including legislative amendments, case law and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, Jersey has significantly modernised its data protection framework by adopting the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018 which entered into force in 2018 and align the Jersey regime closely with the GDPR.

In the area of government access to personal data, public authorities in Jersey are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching legal framework and international commitments, notably the ECHR and Convention 108, as well as from Jersey data protection rules, including the specific provisions for the processing of personal data in the law enforcement context set out in the Data Protection (Jersey) Law 2018, as modified by Schedule 1 to that Law. In addition, Jersey law imposes a number of specific limitations on the access to and use of personal data for criminal law enforcement and national security purposes, and it provides oversight and redress mechanisms in this area.

Based on the overall findings set out in the SWD, the Commission concludes that Jersey continues to provide an adequate level of protection for personal data transferred from the EU.

4.9. New Zealand

The Commission welcomes the developments in the New Zealand legal framework since the adoption of the adequacy decision, including legislative amendments, case law and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, the data protection regime underwent a comprehensive reform with the adoption of the Privacy Act 2020 that further increased the convergence with the EU's data protection framework, notably as regards the rules for international transfers of personal data and the powers of the data protection authority (the Office of the Privacy Commissioner).

In the area of government access to personal data, public authorities in New Zealand are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching constitutional framework (e.g., the Bill of Rights Act) and case law, as well as specific laws regulating government access to data and provisions of the Privacy Act that also apply to the processing of personal data by criminal law enforcement and national security authorities. In addition, the New Zealand legal system provides for different oversight and redress mechanisms in this area.

Based on the overall findings set out in the SWD, the Commission concludes that New Zealand continues to provide an adequate level of protection for personal data transferred from the EU. The Commission also welcomes the recent introduction of a bill before the Parliament by the New Zealand government to amend the Privacy Act 2020 to further strengthen the existing transparency requirements. The Commission will closely monitor future developments in this area.

4.10. Switzerland

The Commission welcomes the developments in the Swiss legal framework since the adoption of the adequacy decision, including legislative amendments, case law and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, the modernised Federal Act on Data Protection that has further increased the convergence with the EU's data protection framework, notably with respect to the protections for sensitive data and the rules on international data transfers. Switzerland also strengthened its international commitments in the field of data protection by ratifying Convention 108+ in September 2023.

In the area of government access to personal data, public authorities in Switzerland are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching legal framework and international commitments, notably the Swiss Federal Constitution, the ECHR and Convention 108+, as well as from Swiss data protection rules, including the Federal Act on Data Protection and specific data protection rules that apply to criminal law enforcement (e.g., the Criminal Procedure Code) and national security authorities (e.g., the Intelligence Service Act). In addition, Swiss law imposes a number of specific limitations on the access to and use of personal data for criminal law enforcement and national security purposes, and it provides oversight and redress mechanisms in this area.

Based on the overall findings set out in the SWD, the Commission concludes that Switzerland continues to provide an adequate level of protection for personal data transferred from the EU.

4.11. Uruguay

The Commission welcomes the developments in Uruguay's legal framework since the adoption of the adequacy decision, including several legislative amendments, case law and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, Uruguay modernised and strengthened its Law 18.331 on the Protection of Personal Data and the Habeas Data Action of 2008 through legislative amendments in 2018 and 2020 which broadened the territorial scope of the data protection legislation, created new accountability requirements (such as impact assessments, data protection by design and by default, data breach notification and the appointment of data protection officers) and introduced additional protections for biometric data. Uruguay also strengthened its international commitments in the field of data protection by joining the Convention 108 in 2019, and by ratifying Convention 108+ in 2021.

In the area of government access to personal data, public authorities in Uruguay are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching legal framework and international commitments, notably the Uruguayan Constitution, the American Convention on Human Rights, Convention 108 and Convention 108+, as well as from the data protection rules in Law 18.331 on the Protection of Personal Data and the Habeas Data Action that apply to the processing of personal data by public authorities in Uruguay, notably for law enforcement and national security purposes. In addition, Uruguayan law imposes a number of specific conditions and limitations on the access to and use of personal data by public authorities, and it provides oversight and redress mechanisms in this area.

Based on the overall findings made as part of this first review, the Commission concludes that Uruguay continues to provide an adequate level of protection for personal data transferred from the EU.

5. FUTURE MONITORING AND COOPERATION

The Commission recognises and very much values the excellent cooperation with the relevant authorities in the each of the countries and territories concerned in the conduct of this review. The Commission will continue to closely monitor developments in the protection frameworks and actual practice of the countries and territories concerned. In case of developments in an adequate country or territory that would negatively affect the level of data protection found adequate, the Commission will, where necessary, make use of its powers under Article 45(5) GDPR to suspend, amend or withdraw an adequacy decision.

This review confirms that the adoption of an adequacy decision is not an ‘end point’ but provides an opportunity to further intensify the dialogue and cooperation with like-minded international partners on data flows and digital matters more generally. In this regard, the Commission looks forward to future exchanges with the relevant authorities to further strengthen cooperation at international level on promoting safe and free data flows, including through strengthened enforcement cooperation. To step up this dialogue and promote the exchange of information, and experience, the Commission intends to organise a high-level meeting in 2024, bringing together representatives from the EU and all countries that benefit from an adequacy decision.