

Draft - Road to Adequacy



The Road to Adequacy

Part 1: Adequacy Decisions – Past, Present and Future

1. Introduction

Forty years ago, the Organisation for Economic Cooperation and Development (“OECD”) adopted the ‘Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’¹ to assist in harmonising emergent data protection legislation whilst facilitating the international free flow of data, which it highlighted as necessary for trade and commerce. Although the Guidelines are non-binding, it advised member countries to support each other’s effort. In particular, in ensuring that that personal data are not deprived of protection as a result of their transfer.²

In 1981, the first legally binding international treaty governing the processing of personal data was developed. Of note, the Convention for the Protection of individuals with regard to the automatic processing of personal data (“Convention 108”)³ laid out basic principles for data protection which include the principles of fairness and lawfulness, accuracy, purpose limitation and security. Importantly, Convention 108 introduced provisions which addressed the transborder transfer of personal data to regulate the flow of personal data between States.

Through the 1980s and 90s advances in technology gained pace, facilitating ever increasing transfer of personal data across borders with greater ease. Alongside this was the continued introduction of data protection legislation across the EU and to a lesser extent, internationally.

Against this backdrop, a growing concern arose regarding the ongoing protection of an individual’s personal data once it has been exported from a jurisdiction with data protection legislation and systems, to another jurisdiction without (or with legislation and systems not to an equivalent standard).

In other words, while recognising that cross border data flows are critical for trade (even more so in today’s modern digital economy), the protections afforded to individuals in a jurisdiction and its data protection laws, should not be undermined when personal data leaves that jurisdiction.

In 1995, the European Union (“EU”) sought to address this, among other things, with the adoption of the Data Protection Directive⁴ (the “1995 Directive”), which introduced the adequacy decision principle. In 2018, The EU implemented the General Data Protection Regulation

¹ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, adopted 23 September 1980

² Ibid para 64.

³ Council of Europe Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108

⁴ 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.

("GDPR") as an update and refinement of the principles espoused in the 1995 Directive. This paper explains the key legal frameworks, the adequacy decision in European data protection legislation, specifically focusing on the 1995 Directive and GDPR⁵, including how the principle works, the decisions taken and their current status as well as potential future decisions.

The legal framework of data protection in EU is underpinned by layers of Human Rights, International Treaties as well as EU legal instruments. The Charter for Fundamental Rights and Freedoms ("the Charter")⁶ operates in the EU in a similar way to the US Constitution.

The Charter brings together the fundamental human rights of everyone living in the EU into one legally binding document. The Charter provides two distinct Articles which addresses both right to privacy and data protection. Article 7 of the Charter provides that everyone has the right to respect for his or her private and family life, home, and communications. Article 8 of the Charter specifically references data protection by providing that everyone has the right to the protection of personal data concerning him or her.

In addition, Article 47 of the Charter provides that everyone "...has the right to an effective remedy before a tribunal." Emphasising that everyone "...is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law." The Charter is binding on the European Commission and Member States of the EU following the entry into force of the Treaty of Lisbon in 2009. The Court of Justice of the European Union ("CJEU") is required to interpret all EU legal acts in accordance with the Charter. Consequently, the provisions of the Charter also applies to adequacy decisions.

2. The Adequacy Decision

The adequacy decision is a mechanism that was first introduced by European data protection legislation regarding the equivalence of the protection of personal data afforded by jurisdictions outside of the European Economic Area ("EEA").⁷

Adequacy decisions are determined by the European Commission according to specified criteria and procedure (discussed in the next section), and where made, the concerned jurisdiction is deemed to offer an adequate level of data protection, compared to the EU. An adequacy decision is an implementing act taken by the European Commission (in accordance with 291(2) of the TFEU). The decision can only be repealed by CJEU or the Commission itself.

⁵ 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).

⁶ EU Charter of Fundamental Rights: Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389

⁷ The EEA being all European Union member states, plus Norway, Liechtenstein and Iceland.

The effect of a European Commission adequacy decision is to allow the free flow of personal data from the EEA to the concerned jurisdiction without the need for further safeguards or to obtain any authorisation.

2.1 The 1995 Data Protection Directive

The adequacy decision was introduced into pan EU data protection law by the 1995 Directive. Article 25(1) of the 1995 Directive sets out that transfers of personal data to a jurisdiction outside the EEA (i.e. a “third country”) should only take place where the third country in question ensures an adequate level of protection.

It has long been recognised that the cross-border flow of personal data is necessary to support international trade and commerce. In 1995, the extent of data protection laws globally was still somewhat limited and effectiveness varied widely. The adequacy decision was introduced as a measure to ensure that the protections afforded to individuals by the Directive were not undermined when exporting personal data out of the EEA.

To determine whether a third country’s level of protection was adequate, Article 25(2) of the 1995 Directive set out:

“The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.”

The decision on whether a third country’s level of protection was adequate (i.e. the adequacy decision), was the responsibility of the European Commission, as set out in Article 25(6) of the 1995 Directive, as follows:

“The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.”

Article 25 of the 1995 Directive further prohibited personal data transfers to third countries that did not ensure an adequate level of protection (i.e., third countries for which there was no adequacy decision). However, a derogation to the prohibition, allowed for transfers of personal data, subject to the use of other safeguards such as, (i) obtaining the consent of the individual, (ii) the transfer being necessary for the performance of a contract, or (iii) where adequate safeguards were provided by contractual clauses approved by Member States (the so called, Standard Contractual Clauses (“SCCs”).

With the introduction of the adequacy decision in 1995, the EU were the first to create a white list approach to assessing data protection equivalence internationally. The European Commission's first adequacy decisions were the United States (Safe Harbour)⁸ and Switzerland⁹, both made on 26 July 2000, nearly five (5) years after the adoption of the 1995 Directive.

2.2 General Data Protection Regulation

On 14 April 2016, the EU's GDPR was enacted, repealing the 1995 Directive. The GDPR became enforceable on 25 May 2018 and it retained the adequacy decision with a key modification as well as further elaboration on the criteria for making adequacy determinations.

Article 41 of GDPR sets out the criteria, conditions and procedures for the adoption of an adequacy decision by the European Commission (outlined in the next section).

The key modification to the adequacy decision under GDPR is that the European Commission may now expressly assess and make decisions on the adequacy of not only a third country, but also a territory or one or more specified sectors within a third country, or an international organization.¹⁰

The term 'territory' is not defined in GDPR but its use in the text is 'within a third country', which is therefore likely to mean a geographical jurisdiction such as a state or province. Meanwhile, 'international organisation' is defined as meaning,

“...an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries”.¹¹

To date, the European Commission has not made any adequacy decisions regarding a territory or sector within a third country, or regarding an international organisation.

Under GDPR, an adequacy decision is made by means of an implementing act¹² of the European Commission, with decisions subject to a periodic review at least every four years. The periodic review must take into account all relevant developments in the third country or international organisation.

The first adequacy decision made under GDPR concerned Japan. That decision was taken by the European Commission on 23 January 2019 with immediate effect (although discussions between the EU and Japan commenced much earlier). As set out in the particulars of the implementing

⁸ 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce

⁹ 2000/518/EC: Commission Decision 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.

¹⁰ See Article 45(3) of GDPR.

¹¹ See Article 4(26) of GDPR (Definitions).

¹² See Articles 45(3) and 93(2) of the GDPR.

act, the Japan decision is subject to a first review within two years after its entry into force (i.e. by 23 January 2021).¹³

Regarding the status of adequacy decisions made under the 1995 Directive (following the Directive being repealed by GDPR), Article 45(9) of GDPR clarifies that such decisions shall remain in force until ‘amended, replaced or repealed’ by an adequacy decision adopted in accordance with the relevant provisions of GDPR.

To date, the European Commission has not amended, replaced or repealed any adequacy decisions made under the 1995 Directive. However, pursuant to Article 45(4) of GDPR, the European Commission is required, on an ongoing basis, to monitor developments in third countries that could effect the functioning of decisions adopted pursuant to the 1995 Directive.

A list of the adequacy decisions made under both the 1995 Directive and GDPR is provided in Table 1 in section 4 of this paper.

2.3 Adequacy Decisions in Law Enforcement

While the focus of this paper is on adequacy decisions made under the 1995 Directive and GDPR, for completeness, EU data protection legislation also includes the adequacy decision principle in relation to transfers of personal data for law enforcement purposes under the EU Data Protection Law Enforcement Directive.¹⁴ Following the UK’s withdrawal from the EU, it was the first to receive an adequacy decision under the Law Enforcement Directive.

2.4 Adequacy Decisions in Data Protection Law Internationally

Other jurisdictions internationally have also adopted the adequacy decision principle, to recognise equivalence as a means of facilitating free and safe data flows, as a part of their data protection laws.

In the Middle East for example, Israel, the Dubai International Financial Centre (“DIFC”)¹⁵ and the Abu Dhabi Global Market (“ADGM”)¹⁶, include the adequacy decision principle in their respective data protection regimes. The DIFC and ADGM are geographical territories within the United Arab Emirates, established by the Governments of the Emirates of Dubai and Abu Dhabi, respectively, with comprehensive, horizontal data protection regimes.

¹³ See Article 3(4) and Recital 181 of the EU-Japan Adequacy Decision.

¹⁴ 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, OJ L 119, 4.5.2016, p. 89–131.

¹⁵ See Article 26 of the DIFC Data Protection Law 2020.

¹⁶ See Section 4 of the ADGM Data Protection Regulations 2015 (as amended).

More recent examples where the adequacy decision is included are Brazil's General Data Protection Law ("LGPD")¹⁷ and Serbian Law on Personal Data Protection ("LPDP")¹⁸. Interestingly enough, LPDP considers that countries signatories to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data provide an adequate level of protection, unlike GDPR. In addition, countries deemed adequate by the EU are also deemed adequate under the Serbian privacy regime.

3. Adequacy Decision Criteria and Process

The free flow of personal data may occur if a third country (or territory or sector within a third country) or international organisation ensures "an adequate level of protection". This term was introduced in the 1995 Directive¹⁹ and is continued in GDPR.²⁰ In order to determine what constitutes, "an adequate level of protection", the legislation provides the criteria that the European Commission must consider (as well as the procedure).

The criteria has also developed over time with case law. For example, in 2015, the Court of Justice of the European Union ("CJEU") clarified in Case 362/14 ("Schrems") that "an adequate level of protection" requires the third country to ensure a level of protection of fundamental rights and freedoms that are "essentially equivalent" to the guarantees ensured by law in the EU.²¹

The following sets out the criteria and procedure under GDPR, since that is the legislation currently in force, noting that the criteria in GDPR builds on the criteria established in the 1995 Directive, which has been further developed by the CJEU.

3.1 Adequacy Criteria

To assess the adequacy of the level of protection of a third country or international organization, the European Commission must take into account the following elements as set out at Article 45(2) of GDPR:

"(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective

¹⁷ See Article 33 of the Brazilian General Data Protection Law (LGPD).

¹⁸ See Article 64 of the Serbian Law on Personal Data Protection (LPDP).

¹⁹ See Article 25(1) of the 1995 Directive.

²⁰ See Article 45(1) of GDPR.

²¹ CJEU, C-362/14, Maximilian Schrems v. Data Protection Commissioner [GC], 6 October 2015, para. 96.

- administrative and judicial redress for the data subjects whose personal data are being transferred;
- (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
 - (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.”

As can be seen from the text of Article 45(2) above, the criteria consists of assessing three elements broadly being, 1) the content of the data protection rules, 2) the system in place to ensure the effectiveness of the rules and 3) international commitments to the protection of personal data.

In respect of the content of the data protection rules of a third country, the Article 29 Working Party’s Adequacy Referential notes, “the objective is not to mirror, point by point the European legislation but to establish the essential - core elements of that legislation”.²² The Working Party’s Adequacy Referential further elaborates a number of content principles that a third country’s data protection rules and system must contain.

Data protection laws only provide protection to individuals if they are followed in practice.²³ Regarding a system to ensure effectiveness, the European Commission must consider and evaluate the existence and effective functioning of a supervisory body for data protection. The effectiveness of supervisory authorities is assessed by factors including resourcing, range of powers, and enforcement actions taken for non-compliance with data protection requirements. Additionally, individuals must have access to judicial redress, rather than relying solely on data protection supervisors.

Finally, the European Commission must assess a third country’s commitment to the individuals’ privacy and data protection by way of conventions entered into and participation in multilateral systems. For example, whether or not a country has ratified Convention 108+.²⁴ The reason lies in the fact that Convention 108+ principles, provisions relating to data protection authorities, individual’s rights, list of exceptions and restrictions are closely aligned with GDPR. Also, the Convention Committee is entrusted with a task of assessing compliance of candidates with the Convention 108+ provisions and preparing a report for the Council of Europe’s Committee of

²² Article 29 Working Party, Adequacy Referential, WP254, adopted 28 November 2017.

²³ Article 29 Working Party, Working Document – Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, WP12, adopted 24 July 1998.

²⁴ Council of Europe, Amending Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 223).

Ministers on the level of data protection in those countries. Therefore, countries that have ratified Convention 108+ are strong candidates to receive an adequacy status under GDPR.

3.2 Adequacy Process

The adequacy process involves a multistep formal comitology procedure pursuant to Article 45(3) and Article 93(2) of GDPR.²⁵

The process commences with exploratory discussions between representatives of the European Commission and the government of a third country. These discussions may be initiated by either the European Commission or the government of the third country.

The European Commission's decision making process for either initiating or agreeing to a request to enter into such discussions may be based on various factors. A 2017 communication from the Commission to the European Parliament and the Council highlights that the Commission's approach to date can be classified into three categories:

- 1) *Countries that are closely integrated with the EU* (i.e. Switzerland, Andorra, Faeroe Islands, Guernsey, Jersey, Isle of Man),
- 2) *Important trading partners* (i.e. Argentina, Canada, Israel, United States [and Japan]), and
- 3) *Countries playing a pioneering role in data protection in their region* (i.e. New Zealand and Uruguay).²⁶

Should the exploratory discussions move forward, the European Commission conducts an assessment of the third country in accordance with the adequacy criteria and prepares a draft Commission decision (i.e. the Implementing Act). The drafting process may involve consultation with relevant experts.

As part of the adequacy assessment process, the EDPB in its opinion will recommend the Commission investigate or obtain clarity on certain specific points or call out areas of concern for the Commission. For example, in their opinion on the Japanese decision the EDPB stated:

*"The use of consent as a basis for data transfers from Japan to a third country in the Japanese legal system raises concerns as the EDPB considers that the information given to the EU data subject prior to consenting seems not to be comprehensive."*²⁷

²⁵ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 sets out the rules concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.

²⁶ European Commission, Communication from the Commission to the European Parliament and the Council, "Exchanging and Protecting Personal Data in a Globalised World", January 10, 2017.

²⁷ Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan

The draft decision is then sent to the European Data Protection Board (“EDPB”) to provide an opinion on the draft. The EDBP represents the data protection authorities of EU member states. As a part of the comitology procedure, after addressing any feedback or concerns raised by the EDBP, the draft decision is then provided to a committee of representatives from EU member states for approval (requiring a qualified majority). Subject to that approval, the European Commission may then adopt the decision.

4. Adequacy Decisions Made

Since the introduction of the adequacy decision in the 1995 Directive, the European Commission has made fourteen (14) adequacy decisions. Thirteen (13) out of fourteen (14) decisions being made under the 1995 Directive with three (3) of those being partial decisions (i.e. Canada, EU-US Safe Harbour and EU-US Privacy Shield). Two (2) decisions have been invalidated by the CJEU, and the one decision under GDPR to date, concerns Japan (which is also a partial decision).

Table 1, below sets out all of the European Commission’s adequacy decisions under both the 1995 Directive and GDPR (listed in alphabetical order).

Table 1 – EU Adequacy Decisions

No.	Jurisdiction	Decision Date	End Date	Legislation
1	Andorra	19 October 2010	N/A	1995 Directive
2	Argentina	30 June 2003	N/A	1995 Directive
3	Canada*	20 December 2001	N/A	1995 Directive
4	Faroe Islands	5 March 2010	N/A	1995 Directive
5	Guernsey	21 November 2003	N/A	1995 Directive
6	Israel	31 January 2011	N/A	1995 Directive
7	Isle of Man	28 April 2004	N/A	1995 Directive
8	Japan**	23 January 2019	N/A	GDPR
9	Jersey	8 May 2008	N/A	1995 Directive
10	New Zealand	19 December 2012	N/A	1995 Directive
11	Switzerland	26 July 2000	N/A	1995 Directive
12	Uruguay	21 August 2012	N/A	1995 Directive
13	United States (Safe Harbour)*	26 July 2000	6 October 2015	1995 Directive
14	United States (Privacy Shield)*	12 July 2016	16 July 2020	1995 Directive

*Partial adequacy decisions.

**First adequacy decision pursuant to GDPR.

The European Commission is required under GDPR to publish the list of third countries, territories or sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is not ensured. The list is made available in the Official Journal of the European Union and at the European Commission's website as follows:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#relatedlinks

4.2 Partial Adequacy Decisions

The 1995 Directive did not expressly provide for a 'partial' adequacy decision. However, the decisions concerning Canada and the United States are considered 'partial' as they are limited in scope.

In respect of Canada, the decision applies only in relation to private entities subject to the Canadian Personal Information Protection and Electronic Documents Act (so called "PIPEDA"). Meanwhile, the United States Safe Harbour and Privacy Shield decisions only applied to U.S. companies that agreed to abide by the Safe Harbour, or subsequently, the Privacy Shield Principles.

The first adequacy decision made under GDPR, concerning Japan, is also a partial decision, as it does not cover all personal data transfers from the EU to Japan. The decision provides that Japan ensures an 'adequate level of protection' for personal data transferred from the EU to businesses in Japan that are subject to the Act on the Protection of Personal Information (so called "APPI"). APPI is not applicable to government entities in Japan.²⁸

4.3 Annulment of the Decisions Concerning the United States

Whilst no adequacy decisions have to date been repealed, two decisions have been ruled invalid by the CJEU, both concerning the United States. The first decision concerning the United States (Safe Harbour) was, as noted above, a partial decision, issued on 26 July 2000. Safe Harbour was ruled invalid by the CJEU on 6 October 2015 in the Schrems case.²⁹

That case was triggered by a complaint from Maximillian Schrems to the Irish Data Protection Commissioner, raising concerns over Facebook Ireland's reliance on the Safe Harbour decision to transfer personal data from the EU to the U.S. The concern was based on the scope of access that U.S. intelligence agencies have to personal data in the U.S., which was revealed by Edward Snowden in 2013.

Prior to the CJEU decision, the European Commission had already been in dialogue with the U.S. Department of Commerce to enhance Safe Harbour. As a result of the CJEU decision, and given

²⁸ See Article 1(1) of the EU-Japan Adequacy Decision.

²⁹ See Case C-362/14, Maximillian Schrems v Data Protection Commissioner.

the importance of transatlantic data flows, discussions continued and on 12 July 2016 the Commission issued a new decision concerning the U.S. named, Privacy Shield. Privacy Shield was a more detailed framework than Safe Harbour and also sought to address the issue of U.S. government surveillance.

However, concerns remained regarding U.S. government access to data and following a new complaint raised by Mr Schrems concerning the Privacy Shield, on 16 July 2020, the CJEU subsequently ruled the Privacy Shield to be invalid (so called “Schrems II”).³⁰

On 10 August 2020, the European Commissioner for Justice, Mr Didier Reynders and the U.S. Secretary of Commerce, Mr Wilber Ross, issued a joint press statement confirming that the U.S. Department of Commerce and the European Commission have initiated discussions to,

“evaluate the potential for an enhanced EU-US Privacy Shield framework to comply with the Court of Justice of the European Union in the Schrems II case.”³¹

At the time of writing, it remains to be seen what the outcome of those discussions will be.

5. Benefits of Adequacy

Adequacy decisions provide multiple benefits to various parties, as outlined in the following.

5.1 Protection of Individuals’ Personal Data

Modern technology is driving an enormous and ever increasing flow of personal data across borders in today’s digital age. The adequacy decision ensures that the privacy protections provided to individuals under European data protection legislation are maintained when their personal data is exported to third countries. Given the ease with which personal data can be transferred across borders, and without uniform data protection laws internationally, the absence of either an adequacy decision or appropriate safeguards would undermine the integrity of Europe’s data protection legislation and fail to provide the protection to individuals that was intended.

Regarding the requirement for an adequacy decision or other safeguards available for data transfers outside of the EEA, the European Commission’s 2017 paper on exchanging and protecting personal data globally states:

“The primary purpose of these rules is to ensure that when the personal data of Europeans are transferred abroad, the protection travels with the data.”³²

³⁰ See Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems.

³¹ Joint press statement from European Commissioner for Justice, Mr Didier Reynders and the U.S. Secretary of Commerce, Mr Wilber Ross, 10 August 2020, Brussels.

³² Ibid footnote 22.

However, given that there are currently only twelve (12) adequacy decisions in force, two (2) of which being partial adequacy decisions (Canada and Japan), arguably the application of the adequacy decision alone as a means for ensuring the protected free flow of personal data, has had limited application to date. This is not surprising given that EU data protection law is widely considered to be the 'gold standard' internationally.

Since personal data is exported from the EU to third countries that do not have an adequacy decision, clearly there is widespread use of other safeguards to ensure that data flows continue, safely.

5.2 Ease of data flows

The Commission's adequacy decisions currently in force provide for the free and safe flow of personal data from the EEA to the concerned third countries without the need for other safeguards or authorisations.

As noted in the introduction, the importance of the free flow of personal data for trade and commerce was recognised over forty years ago by the OECD in its Privacy Guidelines, which were first adopted in 1980, and stated:

"Restrictions on these [data] flows could cause serious disruption in important sectors of the economy, such as banking and insurance."³³

The free (and safe) flow of personal data is a greatly beneficial objective. It provides economic benefits to society by supporting commerce and trade, as well as fostering technology and innovation. The free flow of personal data also reduces regulatory burden and the cost to businesses associated with employing other safeguards to ensure that the data is protected (absent an adequacy decision).

5.3 Proliferation and Convergence of Data Protection Legislation

The EU's adequacy decision has also had the effect of exporting and promoting European privacy principles and standards internationally. Following the introduction of the 1995 Directive a number of countries either introduced or enhanced their privacy legislation and this trend has continued in the years since.

GDPR in particular, since its adoption, has become a key reference for data protection law internationally and a catalyst for the continued introduction or modernisation of data protection laws around the world.³⁴

³³ *Ibid* footnote 1.

³⁴ European Commission, Communication from the Commission to the European Parliament and the Council, "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", June 24, 2020.

More new countries (62) have enacted data protection laws in the decade between 2010 – 2019 than in any previous decade, with the total number of data protection laws globally now in excess of 140.³⁵ The countries enacting new data protection laws cover all corners of the globe from the Middle East and Africa, to Central and South Asia as well as the Caribbean and South America, with varying levels of influence from GDPR.

Convergence of data protection laws serves a number of useful purposes from providing uniform privacy protection to individuals around the world, whilst enabling personal data flows. Convergence is also extremely beneficial for business by reducing the legal complexity, conflicts of laws and compliance costs associated with dealing with multiple disparate privacy laws wherever those businesses operate.

6. Future Adequacy Decisions

On 24 June 2020, the European Commission published its first report on an evaluation and review of the GDPR following two years of application (the “Report”).³⁶ The Report provides a number of useful insights in respect of possible new adequacy decisions, as well as the status of existing decisions (i.e. decisions under the 1995 Directive).

With regard to possible new adequacy decisions, the Report notes that the adequacy process with the Republic of Korea is at an advanced stage, while exploratory talks are ongoing with “important partners” in Asia and Latin America. The Report further confirms that an adequacy assessment of the United Kingdom is in process.

As noted at section 2.2 of this paper, Article 45(4) of GDPR requires the European Commission to monitor developments in third countries that could effect the functioning of decisions adopted pursuant to the 1995 Directive, on an ongoing basis.

In this regard, the Report notes that the Commission has engaged in “an intense dialogue” with all of the eleven³⁷ concerned third countries to assess whether they meet the standard set by GDPR. The Report observes that in some cases, the concerned third countries have modernised their privacy laws (e.g. New Zealand), whilst additional safeguards are being discussed with some countries “to address relevant differences in protection.”

With regard to timing, the Commission is due to issue a report on its evaluations of the existing adequacy decisions following Schrems II.³⁸ As noted above, that judgement was issued on 16 July 2020. The reason for awaiting that judgement before releasing its evaluation, according to the

³⁵ see Greenleaf, Graham and Cottier, Bertil, “2020 Ends a Decade of 62 New Data Privacy Laws”, (2020) 163 Privacy Laws & Business International Report, pp. 24-26.

³⁶ *Ibid* footnote 29.

³⁷ See Table 1 of this paper for the list of the 11 in force decisions under the 1995 Directive.

³⁸ See Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems.

Commission, was in case it provided clarifications, which may be relevant to the adequacy standard.

When the Commission's evaluation report is issued, the potential outcomes of those evaluations may involve several scenarios. Article 45(9) of GDPR clarifies that decisions shall remain in force until 'amended, replaced or repealed' by an adequacy decision adopted in accordance with the relevant provisions of GDPR.

Out of the 11 decisions under review, only Canada is a partial decision. Depending on its evaluation of the current state of the adequacy of those third countries, the Commission may conceivably propose to amend or replace the existing decisions with either a decision allowing 'full' data transfers to continue (i.e. no change), or a partial decision (reducing the scope of a previous decision).

Whilst repealing an existing decision is also a possibility, it is likely to be a last resort. The Commission must first consult with the concerned third country to seek to remediate the situation.³⁹ Given the importance and benefits of adequacy decisions as tool for trade and international cooperation⁴⁰, there is also likely to be a strong will by both the Commission and any concerned third country to ensure the continuity of decisions.

However, should the Commission repeal an existing decision, then it should provide a transition period in order to enable EU data controllers to put other safeguards in place to enable the continued flow of personal data to the concerned third country.

In relation to the U.S., as noted in section 4.3, discussions are ongoing between the European Commission and U.S. Department of Commerce to enhance or replace the Privacy Shield as a result of Schrems II.

Meanwhile, the European Commission must complete its review of the Japan decision by 23 January 2021.

7. Conclusion

The adequacy decision was introduced in EU data protection law with the 1995 Directive as a means to facilitate the free flow of personal data internationally, whilst ensuring that the protections afforded to individual's personal data (and EU data protection legislation) were not undermined.

It is continued and modified under GDPR to allow for not only a decision regarding a third country, but also a territory or sector within a third country or an international organisation.

³⁹ See Article 45(6).

⁴⁰ *Ibid* footnote 29.

Despite the benefits provided by adequacy decisions, both for the protection of individuals as well as ease of doing business and facilitating trade and innovation, the number of decisions adopted to date has been few. Currently there are only 12 decisions in force, two of which are partial decisions. However, this is not surprising when the test for adequacy is essential equivalence, and EU data protection law is considered to be the gold standard internationally.

Notwithstanding this point, more countries globally have introduced data protection laws in the last 10 years than ever before, several being heavily influenced by GDPR, which may in time, lead to further Commission decisions being adopted. Perhaps, the European Commission could assess on a priority basis whether countries that have ratified Convention 108+ provide an adequate level of protection, as their data protection legislation should be closely aligned with GDPR. This would increase the number of adequate countries and ease transfers of personal data.

In the interim, there are many key decisions looming for the European Commission regarding adequacy, including or involving (in no particular order), the United Kingdom, the United States, and reviews regarding the Japan decision and all 11 decisions issued under the 1995 Directive. The outcome of these decisions and reviews will be instructive for future decisions and the future of the adequacy decision principle overall.