# Transfers of personal data from the EU to non-EU countries under the EU General Data Protection Regulation after "Schrems II": not a "Mission Impossible"

by

**Douwe Korff**
*Emeritus Professor of International Law, London Metropolitan University*
*Visiting Fellow, Yale University (Information Society Project)*
*Associate, Oxford Martin School, University of Oxford*

April 2021

**Douwe Korff**
*Emeritus Professor of International Law, London Metropolitan University*
*Visiting Fellow, Yale University (Information Society Project)*
*Associate, Oxford Martin School, University of Oxford*

# CONTENTS

**Page:**

1. Introduction 2
2. The European view of data protection as a fundamental, universal human right 4
2.1 The European view 4
2.2 Implications 4
3. The EU General Data Protection Regulation (GDPR) and transfers of personal data from the EU to third countries 8
3.1 The GDPR 8
3.2 The EU GDPR rules on transfers of personal data from the EU to non-EU countries (so-called "third countries") 8
3.2.1 The basic principle: "adequacy" 8
What constitutes a transfer? ..9
3.2.2 The process for the adoption of an adequacy decision 11
3.2.3 Requirements for adequacy 11
3.2.3.1 Adequacy requires "essential equivalence" 11
3.2.3.2 Matters to be taken into account in adequacy assessments 12
Annex: Matters to be taken into account in adequacy assessments 13
3.2.3.3 General rule of law issues 14
3.2.3.4 Core concepts and core "content" principles and requirements 15
- core concepts and the scope of protection 15
- purpose specification and – limitation (and related matters) 17
- grounds for lawful processing ("consent", "legitimate interest" and "law") 18
- special categories of data ("sensitive data") 21
- informing of data subjects 22
- data subject rights 23
- general restrictions 24
- restrictions on onward transfers 25
3.2.3.5 Access to data by third country authorities 25
European case-law including *Schrems II* 26
3.2.3.6 Procedural/enforcement guarantees 29
European case-law including *Schrems II* 29
3.2.4 Transfers on the basis of appropriate safeguards 31
3.2.5 Derogations for occasional, ad hoc transfers 34
4. Conclusions 40

- o – O – o -

**Douwe Korff**
*Emeritus Professor of International Law, London Metropolitan University*
*Visiting Fellow, Yale University (Information Society Project)*
*Associate, Oxford Martin School, University of Oxford*

# Transfers of personal data from the EU to non-EU countries under the EU General Data Protection Regulation after "Schrems II": not a "Mission Impossible"

## 1. Introduction

The EU General Data Protection Regulation (GDPR), which came into application on 25 May 2018,[1] lays down even stricter rules and conditions on the transfer of personal data from the EU[2] to non-EU countries (so-called "third countries") (hereafter: "data transfers") than its predecessor, the 1995 EC Data Protection Directive.[3] The Court of Justice of the European Union (CJEU) has moreover strictly interpreted those rules and conditions, both in relation to transfers based on "adequacy decisions" and in relation to transfers based on standard contract clauses (SCCs). This short paper provides an overview of the resulting data transfer regime.

To that end, it first briefly explains, in section 2, the European view of data protection as a fundamental, universal human right – because that is why the EU legislator and Court feel they have to impose those strict rules and conditions on data transfers. After a brief introduction to the GDPR generally, Section 3 sets out the specific rules and conditions on data transfers. Section 4 provides a summary and conclusions.

The paper is drawn up in the context of a general review of the "adequacy decisions" of third countries issued under the 1995 Data Protection Directive – such a review being required by the GDPR (Article 97) – and of the proposed issuing of an adequacy decision on the United Kingdom, which after "Brexit" is now a third country.

In that latter context (but in fact also earlier, in relation to previous adequacy decisions: see below), it has become clear that there is considerable tension between the legal requirements for adequacy decisions under the GDPR - which are strict – and the desire on the part of the European Commission to issue positive adequacy decisions to major EU trading or security partners. In relation to two draft opinions of the European Data Protection Board (EDPB) on the adequacy of the UK post-Brexit data protection regimes (i.e., the general regime and the law enforcement regime), it was reported that the Commission criticised the draft opinions for being too critical of the UK data protection standards, saying that:[4]

---

[1] 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. 1–88.

[2] The GDPR including the GDPR data transfer regime also applies to the three non-EU Member States of the European Economic Area (EEA), Iceland, Liechtenstein and Norway. However, in this short paper, I will generally just refer to the EU. This should be read as applying to the EU and those three other EEA Member States.

[3] 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. 31–50.

[4] Vincent Manacourt, *EU Privacy Watchdogs approve UK data standards after Commission dressing down*, 14 April 2021, quoting an email from the Commission to the EDPB of 13 April, available at: https://pro.politico.eu/news/eu-privacy-watchdogs-approve-uk-data-standards-after-commission-dressing-down

> If adopted without being significantly rebalanced, these opinions will be welcomed by those who … will use these critical opinions to show that our model is not credible as a global solution and that **adequacy is basically a 'mission impossible'** …

In other words, whatever the law – and the Court – says, the Commission feels the rules should not be too rigidly or too restrictively applied, as that would hamper trade and other cooperation.

This follows on from earlier embarrassments on the part of the Commission, when the Court invalidated first the EU – US 2000 Safe Harbour adequacy decision (in its *Schrems I* judgment)[5] and then its successor, the 2016 Privacy Shield decision (in its *Schrems II* judgment).[6] Both were adopted in spite of major concerns about the adequacy of US privacy law as applied (or not) to EU personal data, and the latter in particular in spite of major concerns about the massive global US surveillance operations exposed by Edward Snowden in 2013, and the manifest lack of safeguards in US law in relation to these.

But also before then, the Commission has had a tendency to adopt positive adequacy decisions on third countries even though it was highly doubtful, even at the time, whether those countries really did provide "adequate" protection, even by the then-applicable standards.[7] What is more, contrary to its official assurances at the time of adopting those decisions that it would closely monitor the laws and practice in the relevant third countries, to see if standards did not drop below the EU ones, and the obligation to review the earlier decisions under the GDPR after that regulation was adopted in 2016, the Commission never actually reconsidered its decisions – even if it was obvious that a third country did not provide adequate protection in terms of relevant Court judgments.[8]

The Commission also does not appear to be in any hurry in carrying out the mandatory reviews required under the GDPR either: the Regulation was adopted on 27 April 2016, came into application on 25 May 2018 and the Commission should have examined the adequacy decisions issued under the 1995 Directive by 25 May 2020 (Article 97 GDR), but no information on any such reviews has to date been made public.

This paper therefore unapologetically takes the legal view. It explores what the GDPR provisions on data transfers, as interpreted by the Court of Justice, require for an adequacy decision. If the Commission were to adopt adequacy decisions in relation to third countries that do not meet those requirements, those decisions may well be invalidated by the Court (irrespective of whether the Commission managed to "persuade" the EDPB and the European Parliament to not be too "demanding" in this respect) – just as the EU – US Safe Harbour- and Privacy Shield decisions were. From a rule of law perspective, such judgments should be welcomed rather than ignored or disparaged.

- o – O – o -

---

5 CJEU, Grand Chamber judgment of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* ("*Schrems I*"), ECLI:EU:C:2015:650.

6 CJEU Grand Chamber judgment of 16 July 2020 in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*"), ECLI:EU:C:2020:559.

7 For a glaring example, see Douwe Korff, Opinion on the future of personal data transfers from the EU/EEA to Israel & the Occupied Territories, January 2021, due for publication shortly.

8 *Idem*.

# 2. The European view of data protection as a fundamental, universal human right[9]

## 2.1 The European view

In Europe, data protection is seen as a fundamental, universal human right. It was first explicitly recognised in a binding international legal instrument, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (better known as the Data Protection Convention, DPC, or "Convention No. 108" after its number in the European Treaties Series), in 1981.[10] As noted in its preamble, this seeks to:

> reconcile the fundamental values of the respect for privacy and the free flow of information between peoples –

both of which are enshrined as fundamental rights in the foundational European human rights instrument, the European Convention of Human Rights (ECHR). Data protection was recognised as a special, *sui generis* right in Article 8 of the EU Charter of Fundamental Rights (CFR), adopted in 2007, which also, separately, reaffirms the rights to privacy (private and family life, home and communications) and freedom of expression and information (Article 7 and 11, respectively). The Charter became legally binding on the EU with the entry into force of the Treaty of Lisbon, in December 2009. The GDPR, if anything, emphases its main human rights aim more strongly than the 1995 Directive",[11] that focussed somewhat more on the aim to enable the smooth operation of the EU Single Market (although the GDPR also retains that latter aim).[12]

## 2.2 Implications

Recognition of data protection as a fundamental human right has important implications in European – including EU – law. In particular, first of all, European human rights law as enshrined in the ECHR and in the EU's treaties and its Charter of Fundamental Rights reflects the post-World War II view that human rights are universal and must be extended to all individuals affected by (private or public sector) entities under the jurisdiction of the relevant state, irrespective of their nationality or status or of where they are.[13]

---

[9] See Douwe Korff and Marie Georges, The Origins and Meaning of Data Protection, January 2020, available at: https://ssrn.com/abstract=3518386

[10] For details, see Douwe Korff and Marie Georges, The DPO handbook, Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, July 2019, Part One, section 1.2.3, *The 1981 Council of Europe Data Protection Convention and its Additional Protocol*. The Convention was recently "modernised"; the "Modernised Convention" is known as "Convention No.108+". *Idem*, section 1.4.7.

[11] For details, see Douwe Korff and Marie Georges, The DPO Handbook (previous footnote), Part One, section 1.3.2, *The main 1995 EC Data Protection Directive*.

[12] Compare Article 1 GDPR with Article 1 of the 1995 Directive, taking into account the relevant recitals.

[13] It was recently argued that surveillance activities undertaken by a state outside the territory of that state are not subject to the European Convention on Human Rights – and it would follow from this that such activities would also not be subject to European data protection instruments. See Theodore Christakis, Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations, Part 2, *On Double Standards and the Way Forward*, 13 April 2021, available at: https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/#comment-35772
(For Part 1, *Countering the US arguments*, see footnote 126, below.) [footnote continues overleaf]

The EU GDPR therefore applies to all processing of personal data by any EU-based entities, irrespective of the nationality or status of the data subjects concerned, or of where they are. When EU companies or public bodies process personal data on individuals who are nationals and residents of a third country, those data therefore benefit from exactly the same protection as is accorded to individuals who are in the EU (legally or otherwise).

Second, in European legal thinking, it follows from the fact that data protection is a fundamental right that the scope of the right should be broad, and broadly interpreted and applied, while any restrictions or limitations on the right must be restrictively interpreted and applied and: (a) be based on clear, precise and in their application foreseeable legal rules (rules that do not give excessive discretion to authorities relying on those rules); (b) serve a "legitimate aim in a democratic society"; (c) be "necessary and proportionate" to that legitimate aim; and (d) be subject to appropriate oversight, with appropriate independent judicial[14] remedies available to anyone whose data protection rights have been affected.

The principle that rights laid down in human rights treaties should be interpreted broadly was expressed by the European Court of Human Rights as early as 1968 in its *Wemhoff* judgment:[15]

> Given that it is a law-making treaty, it is also necessary to seek the interpretation that is most appropriate in order to realise the aim and achieve the object of the treaty, not that which would restrict to the greatest possible degree the obligations undertaken by the Parties.

In the *Golder* case a few years later, the Court applied this approach, by interpreting the "right to a court" (Article 6 ECHR) broadly. In a separate opinion in that case, UK Judge Fitzmaurice forcefully opposed this, arguing, *inter alia*, that the Convention (and other international human rights treaties such as the ICCPR) made "*heavy inroads on some of the most cherished preserves of governments in the sphere of their domestic jurisdiction or* domaine réservé", and that this:[16]

> Not only justif[ies], but positively … demand[s], a cautious and conservative interpretation, particularly as regards any provisions the meaning of which may be uncertain, and where extensive constructions might have the effect of imposing upon the contracting States obligations they had not really meant to assume, or would not have understood themselves to be assuming.

However, in Europe, as the leading experts on the Convention note:[17]

> Such an argument, which emphasizes the character of the Convention as a contract by which sovereign states agree to limitations upon their sovereignty, has now totally given away to an approach that focuses instead upon the Convention's law-making character

---

However, this is not in line with the case-law of the European Court of Human Rights (properly considered), or with the increasingly "functional" (as opposed to territorial) approach to the application of international human rights standards generally, expressly confirmed in the note on Article 1 of the Modernised Council of Europe Data Protection Convention (Convention 108+) in the Explanatory Report on that convention (which cross-refers to a 2014 Council of Europe *Issue Paper* on The Rule of Law on the Internet and in the wider digital environment written by me for the CofE Commissioner for Human Rights). See my comment under Christakis' blog for details.

[14] On the EU legal requirement that Article 47 CFR requires a judicial remedy, see section 3.2.3.6, below.

[15] ECtHR, Case of *Wemhoff v. Germany*, judgment of 27 June 1968, para. 8.

[16] ECtHR, Case of *Golder v. the UK*, judgment of 21 February 1975, separate opinion of Judge Fitzmaurice, paras. 38 – 39.

[17] Harris, O'Boyle and Warbrick, Law of the European Convention on Human Rights, OUP, 2nd edition, p. 6.

> and its role as a European human rights guarantee that must be interpreted so as to permit its development with time.

This also applies to the 1981 Council of Europe Data Protection Convention. Thus, the explanatory memorandum to the first additional protocol to that convention stresses:[18]

> the principle inherent in European law that clauses making exceptions are interpreted restrictively so that the exception does not become the rule.

The same applies *a fortiori* in relation to EU law, where the Charter of Fundamental Rights (that contains the same civil and political rights as the ECHR, plus a series of social-economic rights) is directly applicable as primary Union law. Article 52(1) CFR also reflects the above-mentioned principle as follows:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Both the Article 29 Working Party and the EDPB quoted the principle expressed in the explanatory memorandum to the first additional protocol to the Council of Europe Convention in their guidelines on derogations (discussed in section 3.2.5, below).[19] Moreover, as the EDPB noted, with reference to extensive case-law:[20]

> The European Court of Justice repeatedly underlined that "the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary".

The third implication is that in Europe it is felt that data protection laws should be "omnibus" laws, in that they should lay down principles that apply across the board. While somewhat differing rules could apply to, say, the public sector or the private sector, or to law enforcement and commercial entities, all those rules should still be based on the same fundamentals (in the EU: as set out in Article 8 of the Charter) and reflect the same "core principles" and guarantees (as further discussed in the next section). The EU GDPR is a typical "omnibus" law, applicable to all matters and all activities subject to EU law, except for a number of separated-out areas, for which instruments based on the same principles have been (or are to be) adopted.[21]

---

[18] Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Strasbourg, 8 November 2001, para. 31, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce56

[19] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018, p. 4 (with reference to the Article 29 working document on the same issue, W114, p. 7), available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf

[20] *Idem*, footnote 7. Cf. also the statement in the CJEU *Schrems II* judgment (footnote 6, above, discussed in the next section) that Article 2(2) GDPR, which sets out exceptions to the scope of the GDPR, "must be interpreted strictly" (para. 84, with reference to earlier case-law).

[21] I.e., for law enforcement activities, the so-called Law Enforcement Directive (Directive (EU) 2016/680) and for processing by the EU institutions and bodies, Regulation (EU) 2018/1725. Not all activities in the Common

And a fourth implication, which will also be discussed in section 3, below, with reference to the last sentence in Article 44 GDPR (quoted in sub-section 3.2.1), is that the protection accorded to personal data by the Charter and the GDPR should not be "undermined" if those data are transferred to a third country.

- o – O – o -

Foreign and Security Policy area are yet subject to EU Charter-compliant data protection rules, but this is being corrected, see Douwe Korff and Marie Georges, The DPO Handbook (footnote 10, above), Part One, section 1.4.4 (on the issue of transfers of personal data between different EU data protection regimes, see section 1.4.6). In the economic area, there is also still in place a directive, Directive 2002/58 – the so-called "e-Privacy Directive" – that was adopted as a subsidiary instrument to the 1995 Data Protection Directive. It provides special rules in relation to electronic communications data. But the broader issues, in particular the issue of transfers of personal data to third countries, are still covered by the GDPR, to which the e-Privacy Directive defers. The e-Privacy Directive is in the process of being replaced by an e-Privacy Regulation. For details, see Douwe Korff and Marie Georges, The DPO Handbook, (footnote 10, above), Part One, sections 1.3.3 and 1.4.2.

# 3. The EU General Data Protection Regulation (GDPR) and transfers of personal data from the EU to third countries

## 3.1 The GDPR

The GDPR strengthened the already strong rules in the 1995 Directive on issues such as consent, the processing of sensitive data, data subject rights, profiling, data protection officers, etc. It strongly reaffirmed the principle of accountability and introduced extensive record-keeping requirements through which controllers and processors of personal data must demonstrate their compliance.[22]

It significantly increased the powers of the authorities charged with enforcing the rules, the so-called supervisory authorities (previously more usually referred to as data protection authorities) and the body through which those authorities cooperate and issue EU-wide guidance, the European Data Protection Board (EDPB), the successor to the "Article 29 Working Party" (WP29) that was established under the 1995 Directive. And it introduced new mechanisms for cooperation and consistency in the supervisory authorities' actions.

It also strongly reinforced the rules on transfers of personal data from the EU to third countries, as discussed in the next sub-section.

## 3.2 The EU GDPR rules on transfers of personal data from the EU to non-EU countries (so-called "third countries")

### 3.2.1 The basic principle: "adequacy"

Article 44 GDPR sets out the "general principle for transfers" of personal data to third countries as follows:

*Article 44*

**General principle for transfers**

> Any transfer of personal data which are undergoing processing[23] or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45(1) stipulates that:

> A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

---

22 See Douwe Korff and Marie Georges, The DPO Handbook, (footnote 10, above), Part Two, section 2.3, *The accountability principle*.

23 Note that the concepts of "personal data" and "processing" are defined broadly, leading to a broad scope of EU data protection overall. See below, at 3.2.3.4.

The process for the adoption of an adequacy decision is briefly outlined in sub-section 3.2.2, below, and the elements of the adequacy decision are set out in sub-section 3.2.3.2.

If there is no adequacy decision in place in relation to a specific third country, then, outside of exceptional cases (discussed in sub-section 3.2.5, below), personal data may only be transferred from the EU to the third country if "appropriate safeguards" are adopted to ensure continued protection of the data also after transfer. We discuss this below, at 3.2.4.

First, however, we should note a conceptual issue:

### What constitutes a transfer?

There have been suggestions, including from the UK when its adequacy was being assessed, that when personal data are "merely routed" through a third country, or if EU individuals make use of services in a third country (such as, in particular, software-as-a-service [SaaS] or platform-as-a-service [PaaS] kinds of services, provided from a server in a third country), this may constitute a "transit" but not a "transfers".[24] Not only is there no semantic basis for distinguishing between "transits" and "transfers" in terms of the GDPR (where the term "transit" is not used anywhere),[25] this approach also flies in the face of the views of the European Data Protection Board (EDPB) which has made clear that:[26]

> Remote access by an entity from a third country to data located in the EEA is also considered a transfer.

The use of SaaS or PaaS services offered from third countries (such as the USA) by companies and individuals in the EU necessarily entails the sending of data (including personal data, if only on the end-user of the service, but also often on others, e.g., when a remote HR service is used, on employees) to the server in the third country (and back). In such cases, the data flowing to and from the server in the third country will be exposed to access by the authorities of the third country – and as further discussed in section 3.2.3.5, below, the question of whether such access meets European standards is an important one to assess in the context of taking of adequacy decisions.

Similar considerations arise in relation to personal data stored on a server in the EU, but which is owned by a subsidiary of (say) a US firm that is subject to US surveillance laws (as discussed in section 3.2.4, below, with reference to a recent decision of the French *Conseil d'État*).

Supervisory authorities in several Member States have therefore rightly emphasised the need for full application of the GDPR to such US server-based services – and have expressed serious concerns in this respect.

---

[24] See Douwe Korff, The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, March 2021, section 3.1, *Transfers and transits (what is a transfer?)*, available at: https://www.ianbrown.tech/2021/03/03/the-inadequacy-of-the-eu-commissions-draft-gdpr-adequacy-decision-on-the-uk/

[25] *Idem*.

[26] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020, footnote 22 (reflected in a range of guidance including on direct access by authorities in third countries to data in the EU).

Thus, a data protection impact assessment of the use of Microsoft's Office 365 suite by Dutch ministries, carried out at the request of the Dutch Ministry of Justice in 2018, concluded that the use of the suite created "high risks" to data subject. It said that:[27]

> Government organisations must exert every effort to mitigate the remaining high risks, amongst others by centrally prohibiting the use of the voluntary Connected Services. They must also block the option for users to send personal data to Microsoft to 'improve Office'. **Government organisations should also refrain from using the SharePoint/OneDrive online storage, and delay switching to the web-only version of Office 365 until Microsoft has provided adequate guarantees with regard to the types of personal data and purposes of the processing.**

This led to negotiations between the Dutch government and MS, resulting in "improved audit rights" on the part of the authorities and further DPIAs of MS's Windows 10 Enterprise and other MS offers.[28]

A working group of the German Conference of Data Protection Authorities examined MS Office 365 in 2020 and concluded that:[29]

> The available information shows that **it is not possible to use Microsoft Office 365 in accordance with [EU and German] data protection law**.

The report was approved by a majority vote. Some DPAs felt that this conclusion was "too sweeping", although they accepted that "improvements have to be made".[30] Others drew firmer conclusions. The DPA of the Land Hessen prohibited the use of MS Office 365 by schools in the state, to prevent personal data of school pupils ending up on the (US-based) MS cloud.[31]

These issues are of particular importance in relation to any assessment of the adequacy of the USA in EU GDPR terms – because so many major cloud server providers are based in the USA and offer their services from USA-based cloud servers – but the implications are more general: difficult issues arise under the GDPR whenever an EU entity uses SaaS or PaaS services provided from a third country that has not been held to provide adequate protection to personal data. Moreover, the situation of EU subsidiaries of non-EU-based mother companies must also be considered in this context. I return to this in sub-section 3.2.4.

---

27 DPIA of Diagnostic Data in Microsoft Office ProPlus, commissioned by the Netherlands' Ministry of Justice and Security, 5 November 2018, p. 8, emphasis added, available at: https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/

28 *Idem*.

29 "*[Schlussforderung:] dass auf Basis der genannten Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich ist*"

30 "*Microsoft Office 365: Bewertung Der Datenschutz-Konferenz zu undifferenziert – Nachbesserungen gleichwohl geboten*" – press statement by the DPAs of Stuttgart, Munich, Ansbach, Wiesbaden and Saarbrücken, 2 October 2020, available at: https://www.datenschutz.saarland.de/ueber-uns/oeffentlichkeitsarbeit/detail/pressemitteilung-vom-02102020-stuttgart-muenchen-ansbach-wiesbaden-saarbruecken/

31 *Schulen bewegen sich beim Einsatz von Office 365 auf dünnem Eis* (Schools are on thin ice when they use Office 365), Die Welt, 5 August 2019, available at: https://www.welt.de/wirtschaft/article197952453/DSGVO-Schulen-bei-Office-365-Einsatz-in-Rechtsunsicherheit.html/

### 3.2.2 The process for the adoption of an adequacy decision[32]

The EU body charged with issuing adequacy decisions is the Union's executive body, the European Commission (Art. 45(1)). The decision takes the form of a so-called "implementing act" (Art. 45(3)).

In reaching its decision, the Commission must follow a so-called "comitology" process, set out in the EU Comitology Regulation, Regulation (EU) No 182/2011 (Article 93 GDPR), but with some special features.

Basically, the Commission is charged with drafting the decision, but must, under the GDPR, consult the European Data Protection Board, which must issue an opinion on whether the third country in question provides adequate protection (Article 70(1)(s) GDPR). But the Commission is not bound by the EDPB opinion.

The Commission must also make the draft decision available to the European Parliament – but this too cannot veto it, although the EP can refer a decision once made to the Court of Justice to assess the compatibility of the decision with the EU Treaties and the EU Charter of Fundamental Rights (CFR). The EP did so in relation to the EU Commission Canada PNR Decision. But that can only happen after a decision is taken and in force, and such a challenge takes several years.[33]

Finally, the draft decision must be submitted to the "Article 93 Committee", made up of representatives of the EU Member States, for approval by consensus or by qualified majority. If the Article 93 Committee approves the draft delegated act, the Commission must adopt the act.

### 3.2.3 Requirements for adequacy

#### 3.2.3.1 Adequacy requires "essential equivalence"

The GDPR has introduced more specific and more demanding requirements in relation to transfers of personal data to non-EU countries than were set out in the 1995 Data Protection Directive. Moreover, the Court of Justice of the European Union (CJEU) has applied the relevant requirements strictly, as is reflected in new guidance on the matter from the European data protection authorities, noted in the next sub-section. Crucially, the Court of Justice of the European Union (CJEU) has held that **"adequate protection" must be read as requiring "essentially equivalent" protection to that accorded by EU law**.[34] **This means that in principle all relevant aspects of the GDPR should be addressed in an "essentially equivalent" way in the law in the third country.**

---

[32] For further details, see Douwe Korff & Ian Brown, The inadequacy of UK data protection law, Part One: General inadequacy, submission to the EU institutions, October 2020, section 2.2, *The process for adopting an adequacy decision*, available at: https://www.ianbrown.tech/wp-content/uploads/2020/10/Korff-and-Brown-UK-adequacy.pdf

[33] The EU-Canada PNR Decision was adopted by the Commission om 5 December 2013. The EP adopted a resolution on seeking an opinion from the Court of Justice on 25 November 2014. The Court issued the opinion on 26 July 2017, holding that the decision was in breach of the EU Charter of Fundamental Rights (and spelling out what changes were needed). But in the meantime, and even pending those changes, the PNR decision remained in effect.

[34] CJEU, Grand Chamber judgment of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* ("Schrems I"), ECLI:EU:C:2015:650CJEU, para. 73.

#### 3.2.3.2 Matters to be taken into account in adequacy assessments

Article 45(2) sets out the main matters that the Commission must take into account in its assessment of the adequacy of the law in a third country as follows:

> When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
>
> (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 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.

Following the *Schrems I* "essential equivalence" test, the WP29 expanded on the requirements for an adequacy decision in its "**Adequacy Referential**", the final version of which was adopted in November 2017 and endorsed by the European Data Protection Board at its first meeting on 25 May 2018.[35] The full list of issues to be assessed, as set out in this Adequacy Referential (with three issues reflecting the discussion in section 2, above) are set out in an annex to the present sub-section. Here, it will suffice to note that the Adequacy Referential focusses on two main elements:

- whether the law relating to privacy/the processing of personal data in the third country provides "essentially equivalent" protection to such data as is provided in the EU, in that they reflect **the substantive "core content" principles and requirements** of EU data protection law as elaborated in the GDPR (whereby the Adequacy Referential

[35] Article 29 Working Party, Adequacy Referential, adopted on 28 November 2017, as last revised and adopted on 6 February 2018 (WP254rev01), available at:
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
EDPB endorsement:
https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf
The 2017/2018 referential replaced very old previous guidance in the WP29 Working Document – Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive (WP12), adopted on 24 July 1998, available at:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf

distinguishes between the main content principles and "examples of additional principles"); and

- whether the law in the third country provides for **"procedural/enforcement" guarantees** that are "essentially equivalent" to those provided for in the GDPR;

Except in one respect, the Adequacy Referential does not elaborate on the requirement in Article 45(2) GDPR that an adequacy assessment should include **a general assessment of whether the rule of law and respect for human rights and fundamental freedoms is ensured in the third country concerned** – but given that this is explicitly mentioned in Article 45(2), this paper will give attention this. The one rule of law aspect that the Adequacy Referential does address is the question of "*essential guarantees for law enforcement and national security access to limit the interferences to fundamental rights*."

The Adequacy Referential also says that that document "*should be updated at a later stage*" as concerns the questions of "*applying the approach to countries that have ratified Convention 108*" and of "*applying the approach to industry self-regulation*" which were addressed in the predecessor to the Adequacy Referential, WP12 (which is now seriously outdated).

In the coming sections (3.2.3.3 – 3.2.3.6) I briefly note in turn:

- general rule of law issues relevant to adequacy;
- the main content principles and requirements relevant to adequacy;
- the question of access to data by authorities of the third country; and
- the main procedural/enforcement guarantees relevant to adequacy.

In the last two of these sections (on the question of access to data by third country authorities and on procedural/enforcement guarantees), we add detailed references to the *Schrems I* and *Schrems II* judgments, in which those issues were addressed with specific reference to the USA. (The Court did not, in either of the *Schrems* judgments, or in any other judgment, address the broader rule of law issues in relation to the USA or whether US privacy laws provide "essentially equivalent" substantive protection to personal data outside of the issue of law enforcement and intelligence agencies' access.)

---

### Annex to section 3.2.3.2, *Matters to be taken into account in adequacy assessments*

The matters listed at B. – E., below, are specifically listed in the WP29 Adequacy Referential. The matters listed at A. reflect the discussion in section 2, above.

**A. Rule of law and respect for human rights requirements:**

1) Human rights as universal or national rights

2) Interpretation of human rights-related law

3) Omnibus laws v. sectoral regulation

**B. Content Principles:**

1) Concepts

2) Grounds for lawful and fair processing for legitimate purposes

3) The purpose limitation principle

4) The data quality and proportionality principle

5) Data retention principle

6) The security and confidentiality principle

7) The transparency principle

8) The right of access, rectification, erasure and objection

9) Restrictions on onward transfers

10) Restrictions generally

**C. Examples of additional content principles:**

1) Special categories of data

2) Direct marketing

3) Automated decision making and profiling

**D. Procedural and Enforcement Mechanisms:**

1) Competent Independent Supervisory Authority

2) The data protection system must ensure a good level of compliance

3) Accountability

4) The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms

**E. Essential guarantees in third countries for law enforcement and national security access to limit interferences to fundamental rights:**

1) Processing should be based on clear, precise and accessible rules (legal basis)

2) Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated

3) The processing has to be subject to independent oversight

4) Effective remedies need to be available to the individuals

---

### 3.2.3.3 General rule of law issues

In section 2, sub-section 2.1, it was noted that in Europe, data protection is seen as a fundamental, universal human right; and in sub-section 2.2 the implications were discussed. These are notably:

- that the privacy- or data protection laws of any state should apply to all processing of all the personal data of all individuals affected by (private or public sector) entities under the jurisdiction of the relevant state, irrespective of their nationality or status or of where they are (*principle of universality*);[36]

[36] See footnote 13, above.

- that the concepts and rights enshrined in such laws should be broadly applied and interpreted, and any limitations on those rights narrowly applied and interpreted (*principles of legality, legitimate purpose, necessity and proportionality*);
- that there should be appropriate independent judicial avenues of redress for anyone whose data protection rights have been breached (*principle of effective remedies*); and
- that the above should preferably be reflected in "omnibus" laws.

The first and second points relate to the **scope** of the laws that are to be assessed. If they do not apply universally (in particular, if they do not apply to non-nationals or non-residents), or if within their area of application, they only apply to limited categories of data or to limited kinds of activities (or if relevant concepts are, by EU standards, excessively narrowly interpreted: see below, at 3.2.3.4, first indent), they cannot be said to provide "essentially equivalent" protection to the GDPR.

The second point also means that in any adequacy assessment close attention should be given to **exceptions to or exemptions from** the laws that are to be assessed. If they provide "essentially equivalent" rights but then add exceptions to those rights that are not "necessary" or "proportionate" by European standards (as set out in Article 23 GDPR, which expressly uses those terms), there is no overall "essential equivalence"; and the same applies if there are excessive exemptions from the in-principle equivalent rules and standards. See below, at 3.2.3.4, penultimate indent.

This has specific implications in relation to access to personal data by state authorities, as discussed at 3.2.3.5, below.

The third point (redress) is a general rule of law/human rights requirement, set out in Article 47 of the EU Charter of Fundamental Rights. We will discuss this issue in section 3.2.3.6, below, with reference also to the more specific GDPR requirements in this respect, and relevant CJEU case-law (in particular *Schrems II*).

The fourth point is not absolute, as is clear from the fact that adequacy decisions can be issued for distinct sectors of third countries. But the point is that if there are a range of laws that address data protection-related issues (either in general or in a specific sector), they should all be based on the same fundamental principles.

#### 3.2.3.4 Core concepts and core "content" principles and requirements

This brief paper cannot discuss in any detail all the 13 principles listed in the Adequacy Referential (see the annex to section 3.2.3.2, at B. and C.). It focuses on the issues and principles set out below with very brief comments and clarifications.

- **core concepts and the scope of protection**

The GDPR rests on a number of core concepts, the two most important of which are "personal data" and "processing". Both are deliberately defined very broadly, in order to ensure that (in line with the general EU human rights approach discussed at 2.1 and 2.2, above) the right to data protection – that applies to all processing of any personal data – is broadly applied. Specifically, these terms are defined as follows:

> '**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

> identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
>
> '**processing**' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
>
> (Article 4(1) and (2) GDPR)

Recital 26 further clarifies that:

> The principles of data protection should apply to any information concerning an identified or identifiable natural person. **Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.** To determine whether a natural person is identifiable, account should be taken of **all the means reasonably likely to be used, such as singling out, *either by the controller or by another person* to identify the natural person *directly or indirectly***.

The CJEU has interpreted the terms "personal data" and "processing" in numerous cases. Without going into detail here, it should be noted that the Court rightly holds that the EU legislator wants data protection to apply broadly, in line with the Charter, and follows that same approach. For instance, regarding the element "any information" in the definition of "personal data", the Court held in *Nowak*:[37]

> As the Court has held previously, the scope of Directive 95/46 [now the GDPR] is very wide and the personal data covered by that directive is varied.
>
> The use of the expression 'any information' in the definition of the concept of 'personal data', within Article 2(a) of Directive 95/46 [Article 4(1) GDPR], reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject.

As Kuner *et al*. observe:[38]

> In essence, it is difficult to conceive any operation performed on personal data which would fall outside the definition of 'processing'.

The Article 29 Working Party adopted the same approach in its 2007 opinion on the concept of personal data:[39]

> It needs to be noted that [the definition of personal data in the 1995 Data Protection Directive, which is essentially retained in the GDPR (which if anything further stresses its broad scope)] reflects the intention of the European lawmaker for a wide notion of

---

[37] CJEU judgment of 20 December 2017 in Case C-434/16, *Peter Nowak v Data Protection Commissioner*, ECLI:EU:C:2017:994, paras. 33 – 34, case reference omitted. For a detailed discussion of the extensive case-law, see Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds) and Laura Drechsler (Asst Ed.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020, commentary on Article 4(1).

[38] Kuner *et al*. (previous footnote), commentary on Article 4(2).

[39] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007 (WP136), p. 4, footnote references omitted.

> "personal data", maintained throughout the legislative process. The Commission's original proposal explained that "*as in Convention 108, a broad definition is adopted in order to cover all information which may be linked to an individual*". The Commission's modified proposal noted that "*the amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual*", a wish that also the Council took into account in the common position.

This is precisely because:

> The objective of the rules contained in the Directive is to protect individuals.

In various other sections, we shall note that this same approach also informs the interpretation of other concepts and rules in the GDPR: the aim is always to ensure broad protection and to limit any restrictions and limitations on protections or rights.

This is stressed here because, as noted earlier, any third country privacy or data protection law that applies to less broadly-defined categories of personal information, or to less broadly-defined kinds of actions carried out with or on personal information, cannot be said to provide "essentially equivalent" protection to the GDPR.

- **purpose specification and -limitation (and related matters):**

Under the GDPR, personal data must be "collected for *specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*" (Article 5(1)(b), which cross-refers to Article 89 in relation to further processing for research purposes; that article sets out more specific conditions in that regard).

The WP29 has stressed that:[40]

> Data are collected for certain aims; these aims are the 'raison d'être' of the processing operations. As a prerequisite for other data quality requirements, purpose specification will determine the relevant data to be collected, retention periods, and all other key aspects of how personal data will be processed for the chosen purpose/s.
>
> First, any purpose must be **specified**, that is, sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation. …
>
> Second, to be **explicit**, the purpose must be sufficiently unambiguous and clearly expressed. Comparing the notion of 'explicit purpose' with the notion of 'hidden purpose' may help to understand the scope of this requirement …
>
> Third, purposes must also be **legitimate**. This notion goes beyond the requirement to have a legal ground for the processing … and … extends to other areas of law. Purpose specification … and the requirement to have a legal ground [for processing] … are thus two separate and cumulative requirements.
>
> The use of the term 'legitimate' … provides a link … also to broader legal principles of applicable law, such as non-discrimination. The notion of legitimacy must also be

[40] Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP203), adopted on 2 April 2013, pp. 11 – 12, emphases added, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

> interpreted within the context of the processing, which determines the 'reasonable expectations' of the data subject. …

It is important to stress the difference between "legality" and "legitimacy" in the law of European states, especially in continental European ones. Cf. the German distinct concepts of "*gesetzwidrig*" and "*unrechtmässig*" and the French concepts of "*illégale*" and "*illicite*" or "*déloyale*". The latter terms come close to "improper" or "unfair" in English. As it is put in Dutch law: an act is "*onrechtmatig*" (not "legitimate") if "*it violates someone else's legal rights, or is in breach of a statutory duty, or is contrary to what is appropriate in social interactions under unwritten law.*" This gives relevant regulatory authorities and courts wide discretion in their determination of whether certain acts – *in casu*, certain processing activities – are in accordance with the principle of "legitimacy".

Any law in a third country that allows for processing or further processing of personal data for insufficiently clearly spelled out purposes (e.g., any "business purpose"), or for "unfair" purposes (purposes that are societally unacceptable even if perhaps not directly contrary to any particular law), cannot be said to provide "essentially equivalent" protection to the GDPR.

Under European data protection law and principles, the (specific and specified) purpose also determines major other matters. Thus, personal data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*" (Article 5(1)c)), as well as "*accurate and, where necessary, kept up to date*" (Article 5(1)(d)). Data that are "adequate" and "relevant" (sufficient) and (sufficiently) "accurate" and "up to date" for one purpose may not be adequate, relevant or sufficiently accurate or up to date for another purpose. Subject to limited exceptions (e.g., for research) personal data should also not be retained (in identifiable form) for longer than is "necessary for the purposes for which the personal data are processed" (Article 5(1)(e)).

Any law in a third country that does not lay down rules on the quality of personal data, or that does not clearly limit retention of personal data with reference to the purpose(s) of the processing, cannot be said to provide "essentially equivalent" protection to the GDPR.

- **grounds for lawful processing ("consent", "legitimate interest" and "law"):**[41]

  **Consent:**[42]

The GDPR requires that there is a lawful ground for all processing of personal data, and one important such ground is that the individual concerned (in EU terminology, the data subject)

---

[41] The Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (the equivalent to Article 6(1)(f) GDPR), adopted on 9 April 2014 (WP217), in fact discusses each of the legal grounds in that directive – which broadly are repeated (with additional specifications) in the GDPR. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[42] For extensive further details and guidance (with many specific examples), see the Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259rev.01), adopted on 16 April 2018, which were endorsed by the European Data Protection Board at its first plenary meeting on 25 May 2018, and the EDPB Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020, which updated the WP29 guidelines, in particular in respect of "cookie walls" and "scrolling". These are available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (WP259rev.01) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (EDPB 05/2020)

gave their consent (Article 6(1)(a)). However, under the GDPR, consent is only valid if it is "*freely given* [see below], *specific* [i.e., for a clearly-defined specific purpose: see the previous indent] and *informed*" [i.e., given after the individual has been provided with relevant information: see below, fifth indent]; it must take the form of an "*unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*" (Article 4(11) GDPR). Consent may not be implied from failure to "opt out" of proposed processing: "*Silence, pre-ticked boxes or inactivity [do not] constitute consent*" (Recital 32).

The controller must keep proof of such consent having been obtained; consent for processing of personal data may not be "wrapped up" with wider matters, as in a company's general terms and conditions, but must be sought separately, "*in an intelligible and easily accessible form, using clear and plain language*"; consent may be withdrawn at any time and "*it shall be as easy to withdraw as to give consent*"; and in assessing whether consent was freely given, "*utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*" (Article 7). If there is a *difference in power* between the party seeking consent and the data subject (e.g., an employer seeking consent from its employees, or a prospective employer seeking consent from a job applicant, or a bank dealing with a consumer applying for a loan), this also raises doubts about the validity of such consent. There are special, even stricter rules in relation to any child's consent in relation to information society services (see Article 8).

If a law in a third country allows processing of personal data on the basis of "consent" that would not be regarded as valid under the GDPR (such as "consent" that is implied from non-action or not "unticking" a pre-ticked consent box, or "consent" that is wrapped up with wider issues, or obtained in a situation in which the data subject may have felt she had no choice), that law does not provide "essentially equivalent" protection compared to the GDPR in this regard. This would apply *a fortiori* if such a law were to allow public authorities to process personal data, or anyone sensitive data, on the basis of implied "consent" or "consent" obtained in an unequal context.

**Legitimate interest:**

Another important legal basis for processing of personal data is that:

> [the] processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (Article 6(1)(f) GDPR)

This legal basis cannot be invoked or relied upon by public authorities in the performance of their public tasks (Article 6(1), last sentence). Rather, such processing must be based on law: see under the next heading. Nor can it be relied upon to process sensitive data (see the fourth indent, below). Moreover, as the Article 29 Working Party already stressed in relation to the 1995 Data Protection Directive in 2014: [43]

[43] Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (footnote 41, above), section III.3, on p. 23.

> [This ground for lawful processing] calls for a balancing test: the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject. The outcome of the balancing test largely determines whether Article 7(f) [Article 6(1)(f) GDPR] may be relied upon as a legal ground for processing.
>
> [T]his is not a straightforward balancing test which would simply consist of weighing two easily quantifiable and easily comparable 'weights' against each other. Rather, … carrying out the balancing test may require a complex assessment taking into account a number of factors.

On the side of the controller, there must be:[44]

> a real and present interest, something that corresponds with current activities or benefits that are expected in the very near future. In other words, interests that are too vague or speculative will not be sufficient.

By contrast, "*the 'interests' and 'rights' [of the individual]*", against which the interests of the controller must be weighed, "*should be given a broad interpretation*".[45]

Both entities' interests are "*on a spectrum*":[46]

> Legitimate interests [of controllers] can range from insignificant through somewhat important to compelling. Similarly, the impact on the interests and rights of the data subjects may be more or may be less significant and may range from trivial to very serious.
>
> Legitimate interests of the controller, when minor and not very compelling may, in general, only override the interests and rights of data subjects in cases where the impact on these rights and interests are even more trivial. On the other hand, important and compelling legitimate interests may in some cases and subject to safeguards and measures justify even significant intrusion into privacy or other significant impact on the interests or rights of the data subjects.

We refer to the Article 29 Working Party opinion for further details, considerations and examples.[47]

Suffice it to note here that a test in a third country's law that allows processing of personal data without the consent of the individuals concerned because it is "useful" or even "necessary" for the interests of the entity collecting and further processing the data (the controller), without seeking to counter-balance this against the interests of the individuals in some meaningful way, cannot be said to provide "essentially equivalent" protection to the GDPR. This applies *a fortiori* if the processing entity is a public body (see under the next heading).

---

44 *Idem*, p. 24.

45 *Idem*, p. 29.

46 *Idem*, p. 30.

47 Note in particular the following example on p. 26:
"In its opinion on SWIFT [WP128 of 20 November2006] although the Working Party acknowledged the legitimate interest of the company in complying with the subpoenas under US law, to avoid the risk of being sanctioned by US authorities, it concluded that Article 7(f) [Article 6(1)(f) GDPR] could not be relied on. The Working Party considered in particular that because of the far-reaching effects on individuals of the processing of data in a 'hidden, systematic, massive and long term manner', 'the interests (f)or fundamental rights and freedoms of the numerous data subjects override SWIFT's interest not to be sanctioned by the US for eventual non-compliance with the subpoenas'."

**Law:**

I noted under the previous heading that the "legitimate interest" legal basis for processing cannot be invoked or relied upon by public authorities in the performance of their public tasks (Article 6(1), last sentence). Rather, under the GDPR, processing that is undertaken "*for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*" – i.e., mainly processing by public authorities (or by private companies to which public sector activities have been outsourced) – is subject to a range of important conditions that again reflect the European fundamental rights approach to data protection. Thus, first of all, the processing – and the data – must be "**necessary**" for the relevant specific public sector task (Article 6(1)(e)). But the GDPR in fact requires much more than that. Thus:

- the **basis** for the processing must be "*laid down by Union **law** or Member State **law***";
- the **purpose** of the processing must be "***necessary** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*";
- that law must "*meet **an objective of public interest** and be **proportionate** to the legitimate aim pursued*"; and
- in the relevant law, the details "may" – but the text suggests, generally ought to – **clarify how the principles in the Regulation should be "adapted" to the specific context**, by specifying more precisely:
  - the **general conditions** governing the lawfulness of processing by the controller;
  - the **types of data** which are subject to the processing;
  - the **data subjects** concerned;
  - the entities to, and the purposes for which, the personal data may be **disclosed**;
  - the **purpose limitation**;
  - **storage periods**; and
  - the **specific processing operations and processing procedures** involved, including measures to ensure lawful and fair processing (including, but not only, in relation to the special processing situations addressed in Chapter IX of the Regulation, i.e., processing that relates to the exercise of freedom of expression and information, processing of and access to official documents, processing of a national identification number, processing in the context of employment, processing for research purposes, processing relating to obligations of professional secrecy, and processing by religious associations).

(Article 6(3))

While these requirements need perhaps not be as fully applied to third countries as they must be to EU Member States, the above does mean that processing by third country public authorities that is not at least to some significant extent and in some significant detail regulated in the law of the third country, cannot be said to provide "essentially equivalent" protection compared to the GDPR.

- **special categories of data ("sensitive data"):**

The GDPR lays down especially strict rules on the processing of "*personal data revealing **racial or ethnic origin**, **political opinions**, **religious or philosophical beliefs**, or **trade union membership***" and on "*the processing of **genetic data**, **biometric data** for the purpose of uniquely identifying a natural person, data concerning **health** or data concerning a natural person's **sex life or sexual orientation***" (Article 9(1), emphases added). The processing of these "*special categories of personal data*" (often referred to as "*sensitive data*") is in principle prohibited, subject to a number of exceptions (that must be narrowly interpreted), including that "*the data subject has given explicit consent to the processing of those personal data for one or more specified purposes*"; that the personal data were "*manifestly made public by the data subject*"; or that the processing is "*necessary for the establishment, exercise or defence of legal claims*" (Article 9(2)(a), (e) and (f), respectively).

As concerns "explicit consent", the requirement of "explicitness" is of course in addition to the demanding general GDPR requirements for consent noted earlier.

In some other areas or for some purposes, such as employment, social security and social protection, for reasons of substantial public interest, for the purposes of preventive or occupational medicine or public health, or for research, sensitive data may be processed on the basis of EU or EU Member State law – but only provided the relevant law is "*necessary*" and "*proportionate*" to the relevant matter or interest, and contains "*suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*" (cf. Article 9(2)(b), (g), (h), (i) and (j), respectively).

More specifically, as already noted above, *sensitive data cannot lawfully be processed on the basis of the "legitimate interest" ground for lawful processing*: there is no "legitimate interest" exception in the second paragraph of Article 9 GDPR (the one containing the exceptions to the in-principle prohibition on the processing of sensitive data).

Laws of third countries that do not impose similarly tough restrictions and conditions on the processing of sensitive personal data – or that apply such restrictions to less broad kinds of data, e.g., by not treating trade union membership as sensitive – do not provide "essentially equivalent" protection compared to the GDPR. The same applies if they allow the (further) processing of sensitive data on the basis that the data subject provided the data to the controller (cf. the "third party doctrine" in US law):[48] under the GDPR providing of personal information to a third party does not constitute "manifestly making the data public by the data subject", and neither does release of one's data on a social media platform to a limited (even if fairly wide) group.

[48] The third-party doctrine is a United States legal doctrine that holds that people who voluntarily give information to third parties—such as banks, phone companies, internet service providers (ISPs) and e-mail service providers—have "no reasonable expectation of privacy." Although recently heavily criticised by Members of Congress and individual judges on the Supreme Court (most notably Justice Sotomayor), it has not (yet?) been overturned or significantly changed. See the US Congressional Research Service report by Richard M. Thompson II, The Fourth Amendment Third Party Doctrine, 2014, available at: https://fas.org/sgp/crs/misc/R43586.pdf

- **informing of data subjects:**

The GDPR contains two provisions on the information that must always be provided to data subjects, either when data are obtained directly from them (Article 13) or when data on them are obtained from others (Article 14), and another provision, Article 12, spells out the modalities and conditions for this informing. The Article 19 Working Party and the EDPB both stress that the provision of the following information is particularly important when the consent of an individual is concerned:[49]

i. the controller's identity;
ii. the purpose of each of the processing operations for which consent is sought;
iii. what (type of) data will be collected and used;
iv. the existence of the right to withdraw consent;
v. information about the use of the data for automated decision-making (with cross-reference to Article 22(2)(c) and the WP29 2018 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679);[50] and
vi. on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards (with reference to Article 46).

Laws in third countries that do not require controllers to provide at least this information to data subjects can again not be regarded as providing "essentially equivalent" protection compared to the GDPR.

- **data subject rights:**

The GDPR grants data subjects the following important rights:

- the right to **information** about the processing of their data (cf. also the information duties noted in the third indent, above);
- the right of **access** to the data subject's data, free of charge;
- the right of **rectification** of inaccurate data and to have incomplete data supplemented;
- the right to **erasure** of data if they are no longer needed (and in some other cases, such as when the data subject withdraws consent or submits a justified objection to the processing) ("the right to be forgotten");
- the right to **restriction** of processing (i.e., the blocking of data pending a dispute);
- the right to have **third parties** to whom the data were disclosed **informed** of any rectifications, erasures or restrictions (unless this is impossible or involves disproportionate effort);

[49] Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259.01) (footnote 31, above), p. 13, and EDPB Guidelines 05/2020 on consent under Regulation 2016/679, (*idem*), para. 64 on p. 14 , footnote references omitted.

[50] Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), adopted on 6 February 2018 and endorsed by the EDPB on 25 May 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

- the right to **data portability** (i.e., to have their data sent to them, or transferred to another controller, in a "structured, commonly used and machine-readable format") in certain cases, such as changing one's information society service provider;[51]
- the right to **object** to processing carried out in relation to a public interest task or that is based on the controller's "legitimate interest" (on the latter, see the first indent, above), including profiling for those purposes (see the next indent); if there is such an objection, the controller may not continue with the processing unless "the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims"; and
- the right **not to be subject to automated individual decision-making, including profiling**.[52]

(Articles 12 – 22 GDPR)

- **General restrictions:**

**All the above rights and obligations may be limited (restricted).** However, as Article 23 makes clear, any such restrictions must be set out in law (a "legislative measure") – which must be clear and precise and foreseeable in its application,[53] respect the "*essence*" of the rights, and must be "*necessary*" and "*proportionate*" to one of a series of important (legitimate) aims in a democratic society including (in paraphrase):

- national security;
- defence;
- public security;
- criminal legal investigations and prosecutions;
- important public tasks and interests; or
- the protection of the data subject or the rights and freedoms of others.

The above rights and the restrictions cannot be discussed here in any detail. Suffice it to note that the absence of any of these rights from any third-country laws being assessed will raise serious doubts as to whether those laws provide for "essentially equivalent" protection to the GDPR. The laws should at the very least include the rights of information, access and rectification: without those, no third country law can be said to provide adequate data protection. There must also be clear limitations on profiling and automated individual decision-making. Moreover, even if the main rights are recognised, they should not be subject to what would be seen in the EU as excessive carve-outs or exceptions: exceptions and derogations from data subject rights in third-party laws that are not limited to serving a major societal interest, or that are too sweeping compared to the strict conditions of Article 23, noted above, cannot be said to provide "equivalent protection" to the GDPR.

---

[51] See the Article 29 Working Party Guidelines on the right to data portability (WP242rev.01), adopted on 27 October 2017 and endorsed by the EDPB on 25 May 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

[52] See the Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (footnote 50, above).

[53] See section 2.2, above.

- **Restrictions on onward transfers:**

Article 44 GDPR makes clear that the conditions imposed on transfers of personal data from the EU to a third country also apply to "onward transfers" from the relevant third country to another third country. And if an adequacy decision applies only to certain entities or sectors in a third country, the same applies as concerns onward transfers of personal data from covered entities or sectors to entities or sectors that are not covered by the adequacy decision. As it is put in recital 101:

> when personal data are transferred from the [European] Union to controllers, processors or other recipients in third countries …, the level of protection of natural persons ensured in the [European] Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country … to controllers, processors in the same or another third country …

#### 3.2.3.5 Access to data by third country authorities

In its 2016 *Schrems I* judgment,[54] the Court noted that the decision in which the EU Commission held that the Safe harbour Agreement provided adequate protection (Decision 2000/50) wrongly did:

> not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.
>
> [And neither] does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind.
>
> (paras. 88 – 89)

Those were the main reasons for invalidating the Safe harbour Agreement (which was then replaced by the Privacy Shield Agreement until that too was invalidated by the Court).

The first point made by the Court is reflected in Article 45(2)(a) GDPR, according to which one of the issues to be assessed as part of the "rule of law" element of an adequacy assessment must be the legal regime for "*access of public authorities [of the third country in question] to personal data*". The Court elaborated on this in its *Schrems II* judgment,[55] as noted below. (The second point, about access to remedies, is addressed in the next sub-section, 3.2.3.6.)

**NB:** I already noted at 3.2.1, above, that remote access by an entity from a third country to data located in the EU is also considered a transfer. Moreover, in a recent decision of the French *Conseil d'État*, it was held that the use by an EU company of a server in the EU that was managed by an EU-based subsidiary company of a US parent company (*in casu*, AWS Luxembourg SARL, a daughter of AWS Inc. in the USA) also exposed the data on the server to access by the authorities in the USA, because the mother company was subject to US surveillance laws and could be ordered to order its daughter company to allow access.[56] We will discuss this case further at 3.2.4, below.

---

54 See footnote 5, above.

55 See footnote 6, above.

56 *Conseil d'État* order of 12 March 2021 in urgency proceedings (acting as *juge des référés*) N° 450163, *Association Interhop et autres*, available at: https://www.dalloz.fr/documentation/Document?id=CE_LIEUVIDE_2021-03-12_450163#texte-integral

### European case-law including *Schrems II*:

There is extensive case-law of both the European Court of Human Rights and the Court of Justice of the European Union relating to state surveillance.[57] Here, the following more specific references to the CJEU's *Schrems II* judgment must suffice.

In *Schrems II*, the Court reiterated, first of all, that:

> the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter [right to private and family life, home and communications, and right to protection of personal data], whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference.
>
> (para. 171, case references omitted)

Access by authorities of a third country to personal data of EU persons that are transferred to the third country (or that are accessed directly by such authorities while in the EU)[58] therefore *ipso facto* also constitutes an interference with – and a limitation on – the rights of the EU persons concerned. This means that the principles discussed in section 2.2, above, as also reflected in the EDPB "core content" requirements discussed in the previous sub-section (in particular under the heading "Law"), must be applied to such access. In the words of the Court:

> in accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be **provided for by law** and **respect the essence of those rights and freedoms**. Under the second sentence of Article 52(1) of the Charter, subject to the principle of **proportionality**, limitations may be made to those rights and freedoms only if they are **necessary** and **genuinely meet objectives of general interest recognised by the Union** or the need to protect **the rights and freedoms of others**.
>
> Following from the previous point, it should be added that **the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned** ( … ).
>
> Lastly, in order to satisfy the requirement of proportionality according to which **derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary**, the legislation in question which entails the interference must lay down **clear and precise rules** governing the scope and application of the measure in question and imposing **minimum safeguards**, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. **[The legislation] must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of**

---

[57] For an overview of the standards set by the case-law, see Douwe Korff & Ian Brown, The inadequacy of UK data protection law, Part Two, UK Surveillance, submission to EU bodies, November 2020, section 3.1, *Issues and applicable standards*, available at: https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-Part-Two-DK-IB201130.pdf

[58] See again sub-section 3.2.1, above, under the heading "*What constitutes a transfer?*".

> **such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.** The need for such safeguards is all the greater where personal data is subject to automated processing ( … ).
>
> (*Schrems II*, paras. 174 – 176, emphases added, references to CJEU Opinion 1/15, in which these points were first made, omitted)

The Court then applied these principles to the legal regimes under which US law enforcement and intelligence authorities could demand or gain access to data including personal data on individuals in the EU. The Court examined in detail in particular the US President-issued Executive Order 12333 (EO 12333) and Presidential Policy Directive 28 (PPD-28), as well as Section 702 of the Foreign Intelligence Surveillance Act (FISA) and the United States Foreign Intelligence Surveillance Court (FISC), established under it. The Court assessed these regimes and in particular the limitations and guarantees inherent in them by reference to their descriptions in the Privacy Shield adequacy decision (quoted in the section in the judgment headed "*The Privacy Shield Decision*", at paras. 42 – 49 of the judgment). Without going into details here,[59] the Court held as follows:

> It is thus apparent that **Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances … that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter**, as interpreted by the case-law set out in paragraphs 175 and 176 [of the judgment, quoted above], according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.
>
> …
>
> It should be added that PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply, allows for '"bulk" collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection', as stated in a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision. That possibility, which allows, in the context of the surveillance programmes based on **EO 12333**, access to data in transit to the United States without that access being subject to any judicial review, **does not**, in any event, **delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data**.

**It follows therefore that neither Section 702 of the FISA, nor EO 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.**

[59] For those details, see the Commission Privacy Shield decision and the parts of it quoted in these paragraphs in the *Schrems II* judgment.

> In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter.

(paras. 180 and 183 – 185, emphases and box added)

This passage is quoted at length because, while of course specific to the situation and rules in the USA, the approach taken by the Court is clearly universally applicable to the laws and practices of any third country.

The EDPB has since clarified the kinds of limitations and guarantees that should be in place in order to ensure that access to personal data by intelligence agencies meets the European – and in particular the EU Treaties and Charter – requirements, in its recommendations 02/2020 on the European Essential Guarantees for surveillance measures (EEGs).[60] Here, it must suffice to note that, in line with my discussion of data protection as a fundamental right in sections 2.1 and 2.2, above, the EEGs note the following:[61]

> Following the analysis of the jurisprudence, the EDPB considers that the applicable legal requirements to make the limitations to the data protection and privacy rights recognised by the Charter [for the purposes of national security] justifiable can be summarised in four European Essential Guarantees:
>
> A. Processing should be based on clear, precise and accessible rules [that are foreseeable in their application];
>
> B. [Strict] necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated [which must relate to a serious threat to national security that is shown to be genuine and present or foreseeable];
>
> C. An independent oversight mechanism should exist; and
>
> D. Effective remedies need to be available to the individual.
>
> The Guarantees are based on the fundamental rights to privacy and data protection that apply to everyone, irrespective of their nationality.
>
> (Words in square brackets that reflect the elaborations on each of the "essential guarantees" provided for in the EEGs added. We refer to the full document for important further detail.)

Laws in third countries that do not meet the above-mentioned European Essential Guarantees for surveillance measures (EEGs) tests cannot be said to provide "essentially equivalent" protection to the GDPR.

---

60 EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

61 *Idem*, para. 24.

#### 3.2.3.6 Procedural/enforcement guarantees

As the Article 29 Working Party puts it, with reference to *Schrems I*:[62]

> [a]lthough the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those employed within the European Union, a system consistent with the European one must be [in place].

Such a system is "characterized by the existence of the following elements":[63]

- there must be one or more "completely independent" and impartial supervisory authorities with effective supervisory and enforcement powers;
- the system should ensure "a good level of compliance" in practice, which can be ensured through sanctions, verifications and audits;
- the system should ensure accountability, by "*oblig[ing] data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority*", e.g., through data protection impact assessments, the keeping of records or log files of data processing activities, the designation of data protection officers, or data protection by design and by default; and
- the system must provide "*support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms*".

**European case-law including *Schrems II*:**

The existence and quality of procedural guarantees in the USA against undue surveillance, and their availability to EU persons, was one of the two main issues in *Schrems II* (the other was the question of access to transferred data by US authorities itself, discussed in the previous section). Here, the following brief points must suffice.[64]

The CJEU assessed the issue in the light of Article 47 of the EU Charter of Fundamental Rights that reads as follows:

> *Article 47*
>
> **Right to an effective remedy and to a fair trial**
>
> Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.
>
> Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.
>
> Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

The first paragraph is based on Article 13 of the ECHR that reads:

---

62 WP29 Adequacy Referential (footnote 35, above), section C.

63 *Idem* (paraphrased).

64 For details, see Douwe Korff & Ian Brown, The inadequacy of UK data protection law, Part Two, UK Surveillance (footnote 57, above), section 3.1.2, points 6 and 7.

> Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

However, as the EU Fundamental Rights Agency (FRA) notes:[65]

> in [European] Union law the protection is more extensive since it guarantees the right to **an effective [judicial] remedy** before a **court**.
>
> (emphasis added)

Specifically, the Court has held that:[66]

> it is apparent from the Court's case-law that [Article 47 of the Charter] constitutes a reaffirmation of **the principle of effective judicial protection**, a general principle of European Union law stemming from the constitutional traditions common to the Member States, which has been enshrined in Articles 6 and 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950.
>
> (emphases added)

Or as the Court put it, even more forcefully, in *Schrems II*, with reference to both "settled case-law" and specifically *Schrems I*, para. 95:

> According to settled case-law, **the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law.** Thus, **legislation not providing for any possibility for an individual to pursue legal remedies** in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, **does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter**.
>
> (para. 187, emphases added)

In *Schrems II*, the Court went on to discuss both the absence of proper judicial redress for EU individuals under the relevant US laws in relation to the collecting of personal data on them by the US intelligence authorities, and the question of whether this was compensated for by the introduction of an Ombudsman Mechanism in 2016. [67] In the first respect, the Court ruled in relation to the main applicable legal US instruments, Presidential Policy Directive (PPD) 28 and Executive Order (EO) 12333, that:

> **[T]he US Government has accepted, in reply to a question put by the Court, that PPD-28 does not grant data subjects actionable rights before the courts against the US authorities. Therefore, the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter**, contrary to the requirement in Article 45(2)(a) of the GDPR that a finding of equivalence depends, inter alia, on whether

---

65 EU Fundamental Rights Agency, EU Charter of Fundamental Rights, Article 47 commentary, at: https://fra.europa.eu/en/eu-charter/article/47-right-effective-remedy-and-fair-trial

66 CJEU, Third Chamber Judgment of 27 June 2013 in Case C-93/12, *ET Agrokonsulting-04-Velko Stoyanov v. Izpalnitelen direktor na Darzhaven fond 'Zemedelie' – Razplashtatelna agentsia*, para. 59, with references to, *inter alia*, Case 222/84 *Johnston* [1986] ECR 1651, paragraph 18; Case C-432/05 *Unibet* [2007] ECR I-2271, paragraph 37; and Case C-334/12 *RX-II Arango Jaramillo and Others v EIB* [2013] ECR, paragraph 40. Emphasis added.

67 The Ombudsperson Mechanism is described in a letter from the US Secretary of State to the European Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, set out in Annex III to the Privacy Shield decision.

> data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights.
>
> **As regards the monitoring programmes based on EO 12333, it is clear from the file before the Court that that order does not confer rights which are enforceable against the US authorities in the courts either.**
>
> (paras. 181 – 182, emphases added)

And as concerns the Ombudsman Mechanism, the Court held that this:

> **does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.**
>
> Therefore, in finding, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in that third country under the EU-US Privacy Shield, the Commission disregarded the requirements of Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter.
>
> (paras. 197 – 198, emphases added, cross-references to earlier case-law and the Advocate General's opinion omitted)

These parts of the judgment are again quoted here because, although they of course relate specifically only to the USA, they clearly indicate the general approach the Court takes to the issue of procedural guarantees.

Third countries that do not provide effective judicial remedies to EU persons in relation to the processing of those persons' personal data in those countries, including in respect of access to those data by the third country's intelligence agencies, cannot be held to provide "essentially equivalent" protection to the GDPR.

### 3.2.4 Transfers on the basis of appropriate safeguards

In this paper, I focus on the question of what requirements under EU law and case-law and the EDPB Adequacy Referential should be met for any third country to provide for an adequate level of data protection. However, I will still briefly note the other possibilities for transfers from the EU to third countries under the GDPR.

Outside of exceptional cases (which we will very briefly discuss in the next section), transfers of personal data from the EU to any third country that has not been held to provide adequate protection by the European Commission may only take place provided that "appropriate safeguards" are adopted to ensure the continued protection of the data in the third country, also after transfer. Article 46 lists a number of specific instruments that can be used to provide such safeguards, of which the most important for the purpose of this paper are "standard data protection clauses adopted by the Commission" (Art. 46(2)(c)). Multinational corporations can also use so-called "Binding Corporate Rules" (BCRs) that have been approved by the relevant (competent) supervisory authority or authorities (involving the Article 63 "consistency mechanism" between different authorities where necessary) (Article 47 – see there for details).

The Commission has recently issued a series of draft new standard contract clauses (SCCs), in a modular format, for consultation.[68] This is not the place to discuss them in detail. Rather, it should be noted that in relation to the issue of access to transferred data by the authorities of a third country they suffer from the same inherent limitation as the previous SCCs, as discussed by the CJEU in *Schrems II*:

> it must be borne in mind that, according to Article 46(1) of the GDPR, in the absence of a Commission adequacy decision, it is for the controller or processor established in the European Union to provide, inter alia, appropriate safeguards. Recitals 108 and 114 of the GDPR confirm that, where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor '*should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject*' and that '*those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies … in the Union or in a third country*'.
>
> **Since by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries**, … , but that Article 44, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, require that the level of protection of natural persons guaranteed by that regulation is not undermined, **it may prove necessary to supplement the guarantees contained in those standard data protection clauses.** In that regard, recital 109 of the regulation states that '*the possibility for the controller … to use standard data-protection clauses adopted by the Commission … should [not] prevent [it] … from adding other clauses or additional safeguards'* and states, in particular, that the controller *'should be encouraged to provide additional safeguards … that supplement standard [data] protection clauses*'.
>
> It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. **In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection**.
>
> (paras. 131 – 133, italics and emphases added)

The EDPB has issued a set of draft recommendations on how to comply with the above requirements, i.e., on how to decide (after determining the measures already taken, such as any in-use SCCs) whether supplementary measures are needed (which requires an assessment, by the data exporter, of the laws and practices of the relevant third country) and if so, what they might be.[69] They can be legal, by adding further stipulations to the SCCs (e.g.,

---

[68] European Commission, Data protection - standard contractual clauses for transferring personal data to non-EU countries (draft implementing act), 12 November 2020, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

[69] EDPB, (draft) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020, available at:

that the data importer provides information of these laws or practices; or certifying that there are no back doors into its systems), or technical, such as using (strong) encryption, or pseudonymising the data, with the key retained by the EU data exporter, or separating out different parts of the data.

However, **such measures will often not be effective if a data importer who is subject to laws allowing for undue access to data by the importing country's authorities needs access to the data in the clear**, as the EDPB explains with the following examples:[70]

> **Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear**
>
> A data exporter uses a cloud service provider or other processor to have personal data processed according to its instructions in a third country.
>
> If
>
> 1. a controller transfers data to a cloud service provider or other processor,
> 2. the cloud service provider or other processor needs access to the data in the clear in order to execute the task assigned, and
> 3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,71
>
> then the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear.
>
> …
>
> **Use Case 7: Remote access to data for business purposes**
>
> A data exporter makes personal data available to entities in a third country to be used for shared business purposes. A typical constellation may consist of a controller or processor established on the territory of a Member State transferring personal data to a controller or processor in a third country belonging to the same group of undertakings, or group of enterprises engaged in a joint economic activity. The data importer may, for example, use the data it receives to provide personnel services for the data exporter for which it needs human resources data, or to communicate with customers of the data exporter who live in the European Union by phone or email.
>
> If
>
> 1. a data exporter transfers personal data to a data importer in a third country by making it available in a commonly used information system in a way that allows the importer direct access of data of its own choice, or by transferring it directly, individually or in bulk, through use of a communication service,
> 2. the importer uses the data in the clear for its own purposes,
> 3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,

https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

[70] EDPB, (draft) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (previous footnote), paras. 88 – 91, pp, 26 – 27, emphases added.

then the EDPB is incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights.

**In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.**

There have already been real cases in which such issues have arisen. Thus, on 12 March 2021, in France, the *Conseil d'État* held that the use by a French agency processing information on COVID vaccination appointments on behalf of the French Ministry of Health, of a server managed by AWS Luxembourg raised issues under the GDPR because the Luxembourg entity was subject to directions from its US mother company, AWS Inc., which could be subject to US surveillance laws. But in that case, the court held the use of the server was permissible because sufficient measures had been taken (including encryption) and the data were not health data as such.[71]

A few days later, on 15 March 2021, the Bavarian data protection authority held that the use of the newsletter tool Mailchimp by a Germany company was unlawful as Mailchimp might qualify as "electronic communication service provider" under US surveillance law and the EU controller did not assess the risk that the US authorities might therefore gain access to the data, and therefore also did not consider what supplementary measures might be needed.[72]

We mention the above here because it shows that if, in a third country, the authorities of that third country can demand or gain access to personal data under laws or rules that do not meet the *Schrems II*/EDPB EEGs standards, then not only can the country not be held to provide "adequate"/"essentially equivalent" protection to the GDPR (see above, at 3.2.3.5), but in addition personal data may only be transferred to that country under SCCs if appropriate, effective "supplementary measures" are adopted in addition to the SCCs – but this can only provide continued protection to the data if the data transferred under the relevant SCCs are not transferred in the clear.

### 3.2.5 Derogations for occasional, ad hoc transfers

Finally, mention should be made of the derogations from the normal transfer rules for "specific situations", provided for in Article 49 GDPR. This article allows for transfers of personal data from the EU to a third country that has not been held to provide "adequate"/"essentially equivalent" protection, without the adoption of any of the kinds of "appropriate safeguards" referred to in Article 46 (such as standard contract clauses: see the previous sub-section) when:

- "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards" (Article 49(1)(a));

---

[71] Éric Landot, *Vaccinations et gestion des données personnelles : innocuité du dispositif selon le Conseil d'Etat*, 15 March 2021, available at: https://blog.landot-avocats.net/2021/03/15/vaccinations-et-gestion-des-donnees-personnelles-innocuite-du-dispositif-selon-le-conseil-detat/

[72] https://gdprhub.eu/index.php?title=BayLDA_-_LDA-1085.1-12159/20-IDV
For the full text of the decision (Aktenzeichen: LDA-1085.1-12159/20-IDV), scroll down.

- the transfer is necessary in a contractual context (Article 49(1)(b) and (c));

  (But note that the above bases for transfers may not be relied upon in relation to "activities carried out by public authorities in the exercise of their public powers": Article 49(3));

- the transfer is necessary for "important reasons of [a] public interest" that is "recognised in [European] Union law or in the law of the Member State to which the controller [data exporter?] is subject" (Article 49(1)(d) read together with Article 49(4));

- the transfer is necessary in relation to legal claims (Article 49(1)(e));

- the transfer is necessary to protect the "vital interests" of the data subject or some other person (Article4(1)(f));

- the transfer is made from a public register – but only provided the rules on consultation of the register are adhered to and the transfer does not include "the entirety of the personal data or entire categories of the personal data contained in the register" (Article 49(1)(g) read together with Article 49(2)); or

- the transfer "is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject" (but this derogation is heavily circumscribed, as noted below) (Article 49(1), second sub-clause).

In 2018, the EDPB adopted guidelines on these derogations.[73] In these, it first of all reiterated, in line with what was discussed in sections 2.1 and 2.2, that:[74]

> [I]n accordance with the principles inherent in European law, the derogations [in Article 49] must be interpreted restrictively so that the exception does not become the rule.

It consequently strongly emphasised the exceptional nature of the derogations and their very limited scope:[75]

> **Occasional and not repetitive transfers**
>
> The EDPB notes that the term "occasional" is used in recital 111 and the term "not repetitive" is used in the "compelling legitimate interests" derogation under Article 49 par. 1 §2. These terms indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions, for example, under random, unknown circumstances and within arbitrary time intervals. For example, a data transfer that occurs regularly within a stable relationship between the data exporter and a certain data importer can basically be deemed as systematic and repeated and can therefore not be considered occasional or not-repetitive. Besides, a transfer will for example generally be considered to be non-occasional or repetitive when the data importer is granted direct access to a database (e.g. via an interface to an IT-application) on a general basis.

---

73 EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (footnote 19, above). These built on the earlier Article 29 Working Party Guidelines on Article 49 of Regulation 2016/679 (Updated), adopted on 6 February 2018 (WP261), which was not included among the WP29 documents endorsed by the EDPB (see footnote 35, above), precisely because the EDPB wanted to revisit the issue – but the EDPB nevertheless still largely follows the WP29 guidelines.

74 *Idem*, p. 4.

75 *Idem*, pp. 4 – 5.

In other words, none of the derogations in Article 49 can be invoked to justify regular, repeated transfers of personal data from the EU to a non-adequate third country: only occasional, ad hoc, non-repetitive transfers can ever be allowed under them.

Secondly, the EDPB stresses that Article 49 does not override the special provision in Article 48 GDPR, according to which controllers or processors in the EU may not comply with any judgment of a court or tribunal, or any decision of an administrative authority, of a third country requiring a controller or processor to transfer or disclose personal data, outside of the usual mutual international legal assistance arrangements:[76]

> In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement.

Third, the EDPB applies the conditions for each of the derogations very strictly, as the following quotes on the main derogations may illustrate:[77]

> [T]he GDPR sets a high threshold for the use **the derogation of consent**. This high threshold, combined with the fact that the consent provided by a data subject can be withdrawn at any time, means that consent might prove not to be a feasible long term solution for transfers to third countries. …
>
> In view of recital 111, data transfers on the grounds of [**the derogations relating to contracts**][78] may take place "*where the transfer is occasional and necessary in relation to a contract (…)*"
>
> In general, although the derogations relating to the performance of a contract may appear to be potentially rather broad, they are being limited by the criterions of "*necessity*" and of "*occasional transfers*". …
>
> The "*necessity test*" limits the number of cases in which recourse can be made to [**the derogations relating to contracts**]. It requires a close and substantial connection between the data transfer and the purposes of the contract.
>
> This derogation cannot be used for example when a corporate group has, for business purposes, centralized its payment and human resources management functions for all its staff in a third country[79] as there is no direct and objective link between the performance of the employment contract and such transfer [which in addition will also not be seen as occasional].[80] Other grounds for transfer as provided for in Chapter V such as standard

---

76 *Idem*, p. 5.

77 *Idem*, p. 8. In this short paper, I am not discussing the special derogations for situations in which a transfer is "***necessary in order to protect the vital interests of the data subject or of other persons**, where the data subject is physically or legally incapable of giving consent*" (Article 49(1)(f)), or relating to **transfers made from a public register** (Article 49(1)(g) and (2)). In regards to the latter, it will suffice to recall that such transfers may only take place if the conditions for consultation of the register have been met, and may not include the entirety of the personal data or entire categories of the personal data contained in the register (Article 49 (2)).

78 There is one derogation relation to transfers that are "*necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request*" (Article 49(1)(b)) and a separate one for transfers "*necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person*" (Article 49(1)(c)).

79 The WP29 in this regard referred to situations "*[w]here an organization has, for business purposes, outsourced activities such as payroll management to service providers outside the EU*".

80 The words in square brackets are taken from footnote 22 in the EDPB Guidelines.

> contractual clauses or binding corporate rules may, however, be suitable for the particular transfer. …

It will often not be easy to draw the line between "occasional" and "non-occasional" transfers, as these examples show:[81]

> It [will] have to be established on a case by case basis whether data transfers or a data transfer would be determined as "*occasional*" or "*non-occasional*".
>
> A transfer here may be deemed occasional for example if personal data of a sales manager, who in the context of his/her employment contract travels to different clients in third countries, are to be sent to those clients in order to arrange the meetings. A transfer could also be considered as occasional if a bank in the EU transfers personal data to a bank in a third country in order to execute a client's request for making a payment, as long as this transfer does not occur in the framework of a stable cooperation relationship between the two banks.[82]
>
> On the contrary, transfers would not qualify as "occasional" in a case where a multi-national company organises trainings in a training centre in a third country and systematically transfers the personal data of those employees that attend a training course (e.g. data such as name and job title, but potentially also dietary requirements or mobility restrictions). Data transfers regularly occurring within a stable relationship would be deemed as systematic and repeated, hence exceeding an "occasional" character. Consequently, in this case many data transfers within a business relationship may not be based on Article 49 (1) (b).
>
> According to Article 49(1) (3), [the derogations relating to contracts] cannot apply to activities carried out by public authorities in the exercise of their public powers.[83]

While the **derogation relating to transfers that are "*necessary for important reasons of public interest*"** (Article 49(1)(d), "usually referred to as the '**important public interest derogation**'") can be relied upon, not only by public authorities but also by private entities,[84] it must also be very restrictively applied:[85]

> According to Article 49 (4), only public interests recognized in Union law or in the law of the Member State to which the controller is subject can lead to the application of this derogation.
>
> However, for the application of this derogation, **it is not sufficient that the data transfer is requested (for example by a third country authority) for an investigation which serves a public interest of a third country which, in an abstract sense, also exists in EU or Member State law. Where for example a third country authority requires a data transfer for an investigation aimed at combatting terrorism, the mere existence of EU or member state legislation also aimed at combatting terrorism is not as such a sufficient trigger to apply Article 49 (1) (d) to such transfer.** Rather, as emphasized by

---

81 *Idem*, p. 9.

82 Arguably, all banks using the IBAN, BIC or SWIFT codes can be said to be in a "stable cooperation relationship" with each other, especially if they carry out many transactions using these numbers – as pretty much all commercial banks will. This means that the derogations relating to contracts (see footnote 78, above) will have very limited use in relation to bank transfers.

83 The Guidelines use the same sentence in relation to the two contract derogations, on pp. 9 and 10.

84 *Idem*, p. 10, with reference to the examples in recital 112.

85 *Idem*, emphasis added.

> the WP29, predecessor of the EDPB, in previous statements,[86] the derogation only applies when it can also be deduced from EU law or the law of the member state to which the controller is subject that such data transfers are allowed for important public interest purposes including in the spirit of reciprocity for international cooperation. The existence of an international agreement or convention which recognises a certain objective and provides for international cooperation to foster that objective can be an indicator when assessing the existence of a public interest pursuant to Article 49 (1) (d), as long as the EU or the Member States are a party to that agreement or convention.

Clearly, in the absence of a relevant international cooperation agreement such as an MLAT, public and private entities who are asked for personal data on the "important public interest" basis by a non-EU entity should exercise great caution in this regard (and if there is an MLAT in place between the country from which the request is made and the EU country of establishment of the requested entity, that requested entity should ask the requesting entity to use the process under the MLAT, rather than providing the requested data outside of the formal framework: see the second point, above). If compliance with a request were to be subsequently held to be not warranted under this derogation – and possibly also held to be in breach of Article 48 – the entity that wrongly disclosed the data would be liable to significant administrative sanctions and demands for compensation for any damage from the individuals concerned. Moreover, such disclosures should never become routine:[87]

> Where transfers are made in the usual course of business or practice, the EDPB strongly encourages all data exporters (in particular public bodies [such as, for example, financial supervisory authorities exchanging data in the context of international transfers of personal data for administrative cooperation purposes])[88] to frame these by putting in place appropriate safeguards in accordance with Article 46 rather than relying on the derogation as per Article 49(1)(d). …

As to the **derogation relating to legal claims**:[89]

> [t]he combination of the terms "legal claim" and "procedure" implies that the relevant procedure must have a basis in law, including a formal, legally defined process, but is not necessarily limited to judicial or administrative procedures ("or any out of court procedure"). As a transfer needs to be made in a procedure, a close link is necessary between a data transfer and a specific procedure regarding the situation in question. The abstract applicability of a certain type of procedure would not be sufficient. …
>
> Whilst there may be a temptation for a data exporter to transfer all possibly relevant personal data in response to a request or for instituting legal procedures, this would not be in line with this derogation or with the GDPR more generally as this (in the principle of data minimization) emphasizes the need for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. …
>
> [O]nly a set of personal data that is actually necessary [should be] transferred and disclosed. … [And] [s]uch transfers should only be made if they are occasional.

Moreover:[90]

---

86 Article 29 Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128), p. 25. [original footnote]

87 *Idem*, p. 11.

88 Words in square brackets taken from footnote 33.

89 *Idem*, p. 12.

90 *Idem*, p. 13.

> Data controllers and data processors need to be aware that national law may also contain so-called "blocking statutes", prohibiting them from or restricting them in transferring personal data to foreign courts or possibly other foreign official bodies.

The "legal claim" derogation should also (again) not normally be relied upon if there is a formal mutual assistance arrangement available: see above, *re* Article 48.

Both the GDPR itself and the guidance from the EDPB stress the particular exceptionality of **the "compelling legitimate interest" derogation** (which was not in the 1995 Data Protection Directive) (Article 49(1), second sub-clause). The word "compelling" of course in itself already indicates that there is a particularly high threshold to overcome. The EDPB stresses that:[91]

> **This derogation is envisaged by the law as a last resort**, as it will only apply where "a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation is applicable"

Article 49(1), second sub-clause, also stipulates that this derogation may only be relied on in relation to transfers that are "*not repetitive*" and that "*concern[ ] only a limited number of data subjects*". The article adds that a transfer on this basis may only take place if:

> the controller has **assessed** all the circumstances surrounding the data transfer and has on the basis of that assessment provided **suitable safeguards** with regard to the protection of personal data. (emphasis added)

**The controller must, moreover:**

> **inform the supervisory authority of the transfer [i.e., of each specific transfer on this basis].** (emphasis added)

Both in order to comply with the general "accountability" principle underpinning the whole of the GDPR,[92] and in order to be able to "demonstrate" to the supervisory authority that the controller has indeed assessed all the circumstances and has adopted all "suitable safeguards", the EDPB "recommends":[93]

> that the data exporter records all relevant aspects of the data transfer e.g. the compelling legitimate interest pursued, the "competing" interests of the individual, the nature of the data transferred and the purpose of the transfer.

The controller must also:

> **inform the data subject of the transfer and of**[94] **the compelling legitimate interests pursued.** (Article 49(1), second sub-clause, last sentence.)

Here, it will suffice to note that transfers on the basis of the derogations in Article 49 GDPR can really only be relied on in relation to special, incidental cases – and even then, they are heavily circumscribed. For organisations that need or want to transfer personal data from the EU to any non-adequate third country on a regular basis, in some kind of structured context (e.g., a commercial relationship, or inside a group of companies, or between public bodies), they are of very limited use.

- o – O – o -

91 *Idem*, p. 14, emphasis added.

92 See footnote 22, above.

93 *Idem*, p. 17.

94 The official English version of the GDPR here has "on", but this is clearly a typo, as is also clear from the other language versions including the French and German ones.

## 4. Conclusions

I noted in the Introduction that the European Commission apparently feels that strict application of the GDPR rules on third country "adequacy" "*is basically a* ***'mission impossible'***". On the other hand, the Court of Justice takes the view that those rules should be strictly applied – and that latter view is underpinned by the fact that data protection is firmly embedded in the EU constitutional order as a *sui generis* fundamental right (see section 2 of the present paper). The European Data Protection Board appears to lean towards the Court's view (as behoves a body of supposedly independent regulators) – but also appears to be wavering under pressure from the Commission (as the UK adequacy process appears to show).

This is not the only context in which the Commission appears to be reluctant to follow the Court's judgments on fundamental data protection rights: a similar tendency is also clear in relation to compulsory bulk retention of e-communications data. Not only are some EU Member States (notably France) expressly trying to evade the Charter in this respect,[95] but the Commission is unwilling to take action against Member States that have failed to comply with the Court's data retention judgments, and is even actively preparing new European legislation that would appear to be incompatible with the CJEU case-law.[96]

The anti-Court stand of the Commission and "some" Member States is a direct challenge to the principle of respect for the rule of law within the EU legal order. At a time when there is already a crisis, with significant deviation from the rule of law in several Member States, this is the worst example the Commission can set.

***And is it really "impossible" to live by the Treaty, Charter and GDPR rules as interpreted by the Court? Of course not.***

Yes, the GDPR and the Court are demanding in relation to the issue of adequacy: only third countries that really and truly provide "essentially equivalent" protection to that ensured in the EU,[97] in all relevant respects (substance, access by authorities, procedural safeguards), should be allowed to benefit from free (unimpeded) data transfers. If it were different, the high standards set by the Treaties, the Charter and the GDPR would be undermined – and the

---

95 *Paris pousse le Conseil d'Etat à défier la justice européenne sur les données de connexion* (Paris urges the Council of State to defy European law in relation to communication data), Le Monde, 8 April 2021, available at:
https://www.lemonde.fr/societe/article/2021/04/08/paris-pousse-le-conseil-d-etat-a-defier-la-justice-europeenne-sur-les-donnees-de-connexion_6075938_3224.html
See my comments on this case in the section on "*Implications for the EU Member States*" at the end of this paper.

96 For a recent animated "exchange of views" between the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and the European Commission on the issue of data retention and the CJEU judgments, on 13 April 2021, see:
https://multimedia.europarl.europa.eu/en/committee-on-civil-liberties-justice-and-home-affairs_20210413-1345-COMMITTEE-LIBE_vd
For a discussion of the issues, see EDRi, Data Retention Revisited, September 2020, available at:
https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf

97 At least to the extent that EU law applies: see again the comments on "*Implications for the EU Member States*" at the end of this paper.

European legislator has made very clear that that must be avoided at all costs, especially in the context of data transfers (see Article 44 GDPR, last sentence, and recital 101).

As the Court of Justice put it in its *Schrems I* judgment:

> the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 [now the GDPR] read in the light of the Charter. **If there were no such requirement [of "essential equivalence"], the objective [of compliance with the express obligation laid down in Article 8(1) of the Charter to protect personal data] would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 [now the GDPR] read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.** (para. 73, emphasis added)

Consequently:

> **the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46 [now Chapter V GDPR], read in the light of the Charter, should be strict.**
>
> (para. 78, with reference, by analogy, to the Court's judgment in *Digital Rights Ireland and Others*, C 293/12 and C 594/12, EU:C:2014:238, paragraphs 47 and 48, emphasis added).

The Commission should not try to go against the Charter, the Court and the express will of the European legislator as neatly summarised above.

It is true that at present few countries outside the EU and the EEA can be honestly said to really provide "essentially equivalent" protection to the EU GDPR. So only a few, if any, positive adequacy decisions ought to be issued (or retained) at present.[98] But that does not render the principle useless. Rather, **the GDPR is seen globally as the gold standard, with many countries or jurisdictions at least trying to emulate its strict regime**. For instance:

> "While the GDPR was created to protect citizens of the EU, its impact spans much farther. The [**California** Consumer Privacy Act, CCPA] is an outcome of the GDPR's reaching influence, shifting government priorities and making them more willing to protect individual privacy."[99]
>
> "[In order to obtain a positive EU adequacy decision], **Japan** agreed to implement additional safeguards to align with the EU's [GDPR] standards."[100]

---

98 Several adequacy decisions issued under the 1995 Data Protection Directive that are currently still in force clearly do not meet the CJEU and EDPB adequacy standards (see, e.g., on Israel, footnote 7, above), and as Ian Brown and I have argued, the UK should not be accorded one and the ones on the other "British Islands" (Guernsey, Jersey and the Isle of Man) should be repealed: see Douwe Korff & Ian Brown, The inadequacy of UK data protection law in general and in view of UK surveillance laws - *Executive Summary* with a discussion of the implications for other countries and territories including Australia, Canada, New Zealand, Gibraltar and the EU Member States, submission to EU bodies, November 2020 (cf. footnotes 32 and 57, above), available at: https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-ExecSumm-DK-IB201130.pdf

99 Varonis, *California Consumer Privacy Act (CCPA) vs. GDPR*, 17 June 2020, available at: https://www.varonis.com/blog/ccpa-vs-gdpr/

100 *Data protection in Japan to Align With GDPR*, Skadden Insights, 24 September 2018, available at:

> "**Uruguay** has a data protection system that follows EU data protection rules."[101]
>
> "The **Brazilian** General Data Protection Law (LGPD) … is Brazil's first comprehensive data protection regulation and it is largely aligned to the EU General Data Protection Act (GDPR)."[102]
>
> "The **South African** Protection of Personal Information Act 2013 … was principally based on the EU Data Protection Directive 95/46/EC … [but] certain stricter provisions were included in the initial text, based on earlier versions of the GDPR."[103]
>
> Etcetera.

The laws in the above countries and states may not yet really be completely "equivalent" (or even "essentially equivalent") to the EU GDPR – but that is no reason to abandon the high European standards, or weaken them in practice. On the contrary, it should be a reason to continue to urge these countries, and any others that seek to protect personal data and privacy, to continue to bring their laws fully in line with the EU GDPR – and thus with international human rights standards. After all, European companies and public authorities are able to operate within the framework of the GDPR (although enforcement could be greatly improved). So why not others in other countries that respect fundamental rights and the rule of law?

In any case, the absence of an adequacy decision on a third country does not mean that transfers of personal data from the EU to that country are rendered impossible. Rather, as the Court stressed in *Schrems I*:

> Recitals 108 and 114 of the GDPR confirm that, where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor '*should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject*' and that '*those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies … in the Union or in a third country*'.

As noted in sub-section 3.2.4, above, there are various types of "appropriate safeguards" including standard contract clauses (SCCs) and, for multinational corporations, Binding Corporate Rules (BCRs).

Commission- or supervisory authority-approved SCCs and BCRs can to a very large extent ensure continued protection of personal data at the EU level, also after transfer, and thereby largely enable most data transfers to "non-adequate" third countries – except in one respect: if the authorities of the relevant third country have excessive powers of access to the transferred data, i.e., powers of access that do not meet the standards set by the CJEU in *Schrems II* with reference to the Charter, as reflected in the EDPB's European Essential Guarantees (EEGs) for surveillance. In such cases, either "supplementary measures" must be

---

https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr

101 OneTrust Data Guidance, *Uruguay - Data Protection Overview*, available at: https://www.dataguidance.com/notes/uruguay-data-protection-overview (€)

102 DLA Piper, *Data Protection Laws of the World*, 28 January 2021,available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=BR

103 IAPP, *After 7-year wait, South Africa's Data Protection Act enters into force*, 1 July 2020, available at: https://iapp.org/news/a/after-a-7-year-wait-south-africas-data-protection-act-enters-into-force/

adopted by the data exporter – or, if these too cannot prevent undue access, the transfer must not take place. The Court has made very clear that that is the consequence of the high level of protection accorded to personal data by the Treaties and the Charter – and the GDPR:

> **Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned.** That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.
>
> (CJEU, *Schrems II* judgment, para. 135, emphases added.)

The problem with this is not the strictness of the rule or the lack of "balance" or "flexibility" in the application of the rule, but the existence in too many countries of excessive surveillance powers on the part of the authorities. The remedy should therefore not be to water down the principle, but rather, to counter such rules of law-incompatible powers. **In simple terms: the Commission is barking up the wrong tree.**

## Implications

### i. Implications for third countries and the international community:

As Ian Brown and I have pointed out in our submissions to the EU on the inadequacy of the UK's data protection regime,[104] the UK (and other third countries) will have to choose: they must either bring their surveillance laws and practices in line with the European minimum standards as set out in the EDPB's European Essential Guarantees, and can then enjoy free data exchanges with the EU (or at least transfers on the basis of SCCs or BCRs); or they will have to face and accept the negative consequences of not providing "essentially equivalent" protection to personal data as are guaranteed in the EU.[105] And the same applies to the other "British Isles" and territories associated with the UK and its surveillance laws and practices: Guernsey, Jersey and the Isle of Man, and Gibraltar[106] (to which one could add the UK "sovereign" military base in Cyprus), and to the other "5EYES" countries that the UK closely cooperates with in the global surveillance arrangements exposed by Edward Snowden: the USA, Australia, Canada and New Zealand (and other third countries that indulge in mass surveillance).[107]

This may be unpalatable for the European Commission and for those EU Member States that are not really opposed to mass surveillance (and indeed carry it out themselves) and are therefore unhappy with the Court of Justice's strong stand (see point ii, below). But that is the consequence of establishing a European Union legal order that is built on the rule of law and respect for fundamental rights.

---

104 See footnotes 32, 57 and 98, above.

105 Douwe Korff & Ian Brown, The inadequacy of UK data protection law in general and in view of UK surveillance laws - Executive Summary (footnote 98, above), section 4.1, *Implications for the UK*, at p. 8.

106 *Idem*, section 4.2, *Implications for the other "British Isles" and Gibraltar*.

107 *Idem*, section 4.3, *Implications for the other "5EYES" (and other countries that indulge in mass surveillance)*.

The European Commission – and the Council, and the European External Action Service – should be at the forefront of defending this European fundamental rights based legal order, rather than undermine it by trying to circumvent its own basic rules and the Court's judgments. They should point out to third countries that want to have trade and other cooperation with the EU that that requires respect for the rule of law and compliance with fundamental rights and data protection standards. That applies to the People's Republic of China and the Russian Federation – and if there are doubts about third countries that generally are seen as maintaining those standards, but that fall short in relation to surveillance, that should apply to them too.

There are moves towards the creation of international legal frameworks to cover state surveillance and the wider actions of states' intelligence and national security agencies in the global digital environment.[108] The EU should support such developments – but insist that any such framework must be in line with the EDPB's European Essential Guidelines. It can then also assure third countries that if they bring their general data protection laws in line with the Modernised Council of Europe Data Protection Convention (Convention 108+), and their surveillance laws and practices in line with these EEGs – that they can then in all probability be held to provide "adequate"/"essentially equivalent" protection compared to the EU GDPR.

Until then, they cannot be held to provide such protection.

**ii. Implications for the EU Member States:**

According to Article 4(2) of the Treaty on the Functioning of the European Union (TFEU):

> The Union … shall respect [the Member States'] essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. **In particular, national security remains the sole responsibility of each Member State.**
>
> (emphasis added)

**Consequently, EU law – including the Treaties and the Charter of Fundamental Rights – simply does not apply, *at all*, to any actions taken by the Member States in the area of national security.**

In line with the principles discussed in section 2, above, the Court of Justice has interpreted this exemption from EU law (and the Charter), and its reflections in the EU data protection

---

108 In 2017, the UN Special Rapporteur on Privacy, Prof. Joe Cannataci, called for "*a legal instrument regulating surveillance in cyberspace [as] a complementary step to other pieces of existing cyberlaw, such as the [Council of Europe's] Convention on Cybercrime, and one which could do much to provide concrete safeguards to privacy on the Internet*." See the Report of the Special Rapporteur on the right to privacy, Human Rights Council Thirty-fourth session 27 February-24 March 2017, A/HRC/34/60, para. 69, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/260/54/PDF/G1726054.pdf?OpenElement
And in September 2020, in a joint statement, the chair of the Council of Europe's data protection "Convention 108" committee, Alessandra Pierucci, and the Council of Europe's Data Protection Commissioner, Jean-Philippe Walter, urged states to strengthen the protection of personal data in the context of digital surveillance carried by intelligence services, by joining the Council of Europe convention on data protection "Convention 108+" and by promoting a new international legal standard to provide democratic and effective safeguards in this field. See:
https://www.coe.int/en/web/portal/-/digital-surveillance-by-intelligence-services-states-must-take-action-to-better-protect-individuals

rules (Article 3(2) of the 1995 Data Protection Directive; Article 1(3) of the e-Privacy Directive; Article 2(2)(d) GDPR) restrictively, by holding that the exemption does not apply to actions required of private sector actors such as e-communication companies that are subject to EU law (in particular EU data protection law) by EU Member States under national or EU law, even if those actions are imposed on those actors in order to protect national security.

Consequently:[109]

> national legislation [of a Member State] which requires providers of electronic communications services to retain traffic and location data for the purposes of protecting national security and combating crime, such as the legislation at issue in the main proceedings, falls within the scope of Directive 2002/58 [the e-Privacy Directive]
>
> [and, one may add, of the GDPR].

However:[110]

> By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only, subject to the application of [the Law Enforcement Directive], with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR.

In other words, if under a Member State's national security laws, a Member State orders an e-communications provider to retain data beyond the normal retention periods and to build a "back door" into its systems through which the Member State's intelligence agencies can secretly access the personal data of users of the service, this can be assessed by the CJEU for its compatibility with EU law and the Charter (and in *LQDN* the Court found that French law in that respect did not meet the EU standards).[111]

But if a Member State's intelligence agencies directly "hack" into an e-communication service provider's systems – without the provider's knowledge or involvement – then that action is outside of the scope of EU law, and of the Charter, and of the Court's jurisdiction. Rather, as the last-quoted paragraph of the judgment makes clear, such action is only subject to the

---

109 CJEU Grand Chamber judgment in *La Quadrature du Net (LQDN)* of 6 October 2020, para. 104.

110 *Idem*, para. 103.

111 It was on this very issue that the French Government wanted the *Conseil d'État* to rule: the government felt that such orders too should be regarded as outside the scope of EU law. See footnote 95, above. However, in its judgment of 21 April 2021, the Court refused to assess whether the European Union authorities, notably the Court of Justice, had exceeded their powers ("ultra vires" review). Rather, it held that in relation to national security, the French data retention law was compatible with the CJEU judgments because the compulsory data retention related to an existing (continuing) real threat to national security. (On the other hand, the Court held that with regard to the use of retained data for intelligence purposes, the prior review of such access by the National Commission for the Control of Intelligence Techniques (CNCTR) is not binding, and that that had to be changed.) See:
https://www.politico.eu/wp-content/uploads/2021/04/21/393099.pdf (judgment)
https://www.conseil-etat.fr/en/news/connection-data-the-council-of-state-conciliates-the-implementation-of-european-union-law-and-the-effectiveness-of-the-fight-against-terrorism-and (summary in English)
Whether this judgment is actually in line with the CJEU case-law is doubtful, but this cannot be further discussed here. There will undoubtedly be extensive comment on the judgment in the near future.

Member State's own national law – and the European Convention on Human Rights, to which all EU Member States are a party.

The latter may constitute some form of a safety net. However:[112]

> In the absence of a European consensus [on a matter before the Court of Human Rights], the Court has tended to reflect national law by applying a lowest common denominator approach or to accommodate variations in state practice through the margin of appreciation doctrine …

This can be seen in the ECtHR's case-law on national security issues and surveillance. For instance, in its *Big Brother Watch (BBW)* judgment, it held that:[113]

> the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation.

Although the Strasbourg Court nevertheless laid down a series of "six minimum requirements" that surveillance laws should comply with,[114] it would still appear that in relation to state surveillance in general, and bulk communication interception in particular, compliance with the ECHR is less demanding than compliance with the EU Charter of Fundamental Rights (as applied by the CJEU). Unless this changes when the Grand Chamber of the Strasbourg Court rules on the *BBW* case (which is still pending there), there are therefore at the moment in the EU different standards that apply to "indirect" surveillance that relies on orders issued to private sectors and to "direct", surreptitious surveillance carried out through secret "hacking" by a Member State's intelligence agencies.

The USA was therefore right when it noted that:[115]

> under *LQDN* no EU legislation governs direct access by Member State authorities to personal data for national security purposes—not the e-Privacy Directive, not GDPR, and not the Law Enforcement Directive.

And that:[116]

> … EU law provides no privacy protections relating to EU Member State governments' direct access to personal data for national security purposes …

But it was not quite right when it claimed that:[117]

---

112 Harris, O'Boyle and Warbrick, Law of the European Convention on Human Rights (footnote 17, above), p. 9.

113 European Court of Human Rights First Section judgment of 13 September 2018 in the case of *Big Brother Watch and Others v. the United Kingdom*, para. 314. The case has been referred to the Grand Chamber where it is still pending.

114 *Idem*, para. 423, summarising the more detailed overview of the six requirements in para. 307.

115 USA Comments on the European Data Protection Board (EDPB)'s proposed Recommendations 01/2020 on measures that may supplement transfer tools listed in Article 46 of the General Data Protection Regulation (GDPR) to ensure compliance with EU standards on protection of personal data, 21 December 2020, p. 9, available at: https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/2020.12.21_-_us_comments_on_edpb_supp_measures_final.pdf

116 *Idem*.

117 *Idem*.

> a data exporter would [therefore] have no comparative standard by which to assess whether privacy protections offered by a destination country for the same type of activities are "essentially equivalent" to protections required by EU law.

Rather, as Christakis points out, the data exporter could at least look at the Strasbourg case-law:[118]

> **Failure to take into consideration the ECHR dimension**
>
> As we have seen, the US submissions are based on the argument that "EU Member State direct access measures are not subject to EU law at all" and "a data exporter would have no comparative standard by which to assess whether privacy protections offered by a destination country for the same type of activities are "essentially equivalent" to protections required by EU law". …
>
> While this is true in relation to "EU law" *stricto sensu* (due to the scope of national security exceptions in EU data protection law), this reasoning neglects the fact that the European Convention on Human Rights (ECHR) and its Article 8 on privacy (amongst others) are applicable to surveillance laws. Of course, the ECHR is not binding in EU law as the EU has not acceded to it. However, the ECHR is binding upon all EU Member States and forms part of European law *lato sensu*.
>
> Consequently, principles such as legality (the need for a clear legal basis for meeting certain quality requirements); necessity and proportionality; independent oversight; and effective remedies/redress etc. do govern EU Member States' surveillance laws. The European Court of Human Rights (ECtHR) has issued a great number of surveillance judgments, and the issue of whether methods used by governments constitute "direct" or "indirect" surveillance (in terms of requests to service providers) seems of little relevance to the underlying principles concerning protection.
>
> In his Opinion in Schrems II, Advocate General Saugmandsgaard ØE stressed that "the provisions of the ECHR will constitute the relevant reference framework for the purpose of evaluating whether the limitations that the implementation of EO 12333 might entail — in that it authorises the intelligence authorities to collect personal data themselves, without the assistance of private operators — call into question the adequacy of the level of protection afforded in the United States" (§ 229).
>
> The importance of this ECHR dimension is also shown by the reference to ECtHR case law in the November 10, 2020 EDPB "Recommendations on the European Essential Guarantees for Surveillance Measures" (EDPB EEG Recommendations). In a similar way, the draft GDPR decision on UK adequacy published by the European Commission heavily emphasises the fact that the UK has ratified the ECHR and that "all public authorities in the UK are required to act in compliance with the Convention" (§ 116).

It nevertheless remains true that in the EU different standards apply to surveillance carried out by Member States under orders issued to providers of e-communication services (the higher standards set by the CJEU in *Schrems II* and *LQDN*), and to surveillance carried out by their national security agencies through direct, surreptitious "hacking" into the providers' systems (the somewhat lower ECHR standards) – while in relation to surveillance carried out

---

[118] Theodore Christakis, Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations, Part 1, *Countering the US arguments*, 12 April 2021, available at: https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/
(For Part 2, see footnote 13, above.)

by third countries it would appear they have to "essentially" meet the higher (CJEU) standards in relation to both kinds of surveillance. In chart form:

| | **EU Member States:** | **Third country:** |
|---|---|---|
| **Indirect access:*** | EU CJEU *Schrems II* & *LQDN* standards | "Essentially equivalent" standards to the EU CJEU *Schrems II* & *LQDN* standards |
| **Direct access:**** | ECHR standards | |

* Indirect access = access under orders issued to providers.

** Direct access = access through surreptitious "hacking" into providers' systems.

In the Executive Summary of our submissions to the EU on UK (in)adequacy, Ian Brown and I commented on this as follows:[119]

> A decision by the Commission to not issue a positive adequacy decision on the UK would not have any immediate legal implications for the EU Member States or the activities of their intelligence agencies – which would remain outside the scope of EU law.
>
> However, if the decision not to issue a positive adequacy decision on the UK were to be based, at least in part, on the fact that the UK law and practices fail to meet the standards set by the CJEU in relation to third country agencies (as reflected in the European Essential Guarantees for surveillance issued by the EDPB), as presumably it would be – then the EU and its Member States could not avoid the accusation of hypocrisy and double standards. That is because several of them have laws and practices that also clearly do not meet those standards.[120]
>
> Moreover, the intelligence agencies of several other EU Member States have been shown to have been cooperating with the US NSA in very much the same way as the UK (albeit as much more junior partners than the UK – often *de facto* little more than tools used by the NSA), including in the gathering of satellite communications[121] and tapping into underseas cables.[122]

---

119 Douwe Korff & Ian Brown, The inadequacy of UK data protection law in general and in view of UK surveillance laws - Executive Summary (footnote 98, above), section 4.4.1, *Implications for [EU] Member States' national security activities*.

120 Cf. the short country sections on France and Germany in Douwe Korff et al., Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, January 2017, pp. 57 – 58 (and the references to these countries in the body of this report, *passim*), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894490 [original footnote]
See also the reference in the US Comments on the EDPB Guidelines on supplementary measures (footnote 123, above) to "*allegations [that] have been repeatedly made in leading French newspapers that intelligence agencies of the government of France have been intercepting international communications data by tapping submarine telecommunications cables.*" (footnote 22 in the US Comments paper).

121 "*Deutschland hat in enger Zusammenarbeit mit den amerikanischen Nachrichtendiensten über Jahrzehnte nicht nur mehr als 100 Staaten, darunter auch Freunde und Verbündete, belauscht.*" ("*For decades, Germany [read: the German Federal Intelligence Service, BND] has, in close cooperation with the American Intelligence Service [CIA] spied on more than 100 countries including friends and allies*"), in: "*Operation 'Rubikon' - #Cryptoleaks: Wie BND und CIA alle täuschten*" ("*Operation 'Rubikon' – How the BND and the CIA covered everything up*"), ZDF TV, 11 February 2020, available at: https://www.zdf.de/nachrichten/politik/cryptoleaks-bnd-cia-operation-rubikon-100.html [original footnote]

122 *Danish military intelligence uses XKEYSCORE to tap cables in cooperation with the NSA*, Electrospaces, 28 October 2020, available at:

> It is long overdue that the EU – or at least, given the regrettable hole in the EU legal order when it comes to national security, the EU Member States – and other states that are supposed to be democracies that uphold and adhere to the Rule of Law, give serious attention to the urgent need to rein in their intelligence agencies. However, as noted in Part Two of our submission, until now only some tentative steps are being taken to adopt an international-legal framework for such agencies, such as the "intelligence codex" proposed by a former head of the German external intelligence service, the *Bundesnachrichtendienst* (BND), Mr Hansjörg Geiger (but even that was five years ago).[123]
>
> It is notable that the European Data Protection Board, in its very recent recommendation on the kinds of "supplementary measures" that should be taken to protect personal data transferred from the EU to third countries, said that controllers and processors should adopt the same kinds of measures in relation to EU Member States ...
>
> **In our opinion, the *Schrems II* judgment, the EDPB European Essential Guarantees, and the difficult issues raised in relation to the UK after Brexit, should now also urgently spur on the EU Member States to bring their own houses in order in relation to mass surveillance and bulk collection of personal data including (but far from limited to) communications metadata.**
>
> (emphasis and box added).

Here, it must suffice to reiterate that call.

- o – O – o -

Douwe Korff
Cambridge, UK, April 2021

https://www.electrospaces.net/2020/10/danish-military-intelligence-uses.html [original footnote]

[123] See Part Two [of the Korff-Brown submissions (footnote 57, above)], section 2.2.1, footnote 7. [original footnote]