Oslo Law Review

SCIENTIFIC PUBLICATION

Universitetsforlaget

Volume 10, No. 1-2023, p. 1–34
ISSN online: 2387-3299
DOI: https://doi.org/10.18261/olr.10.1.2

Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective

Christopher Docksey
Honorary Director-General, European Data Protection Supervisor; Visiting Fellow and Board Member, European Centre on Privacy and Cybersecurity, Faculty of Law, University of Maastricht
christopher.docksey@maastrichtuniversity.nl

Kenneth Propp
Senior Fellow, Europe Center of the Atlantic Council; Senior Fellow, Cross-Border Data Forum; Adjunct Professor of European Law, Georgetown University
proppkr@gmail.com

Abstract
This article applies the principle of 'accountability' to the issue of international transfers of personal data and government requirements for access to that data. It argues that accountability provides a common language for the data privacy and intelligence communities and embodies in practice the necessary norms and mechanisms to satisfy the requirements of both privacy and national security and thus facilitate greater interoperability of international data flows. The principle of accountability has been developed in the privacy and data protection area by various international organisations, together with the laws of a growing number of countries across the world. It may be applied to the state itself, to address the issue of government access to personal information.

As background, the case law of the EU Court of Justice on surveillance and international transfers is briefly described, together with the main elements of the EU-US Data Privacy Framework (DPF). In this context, state accountability for processing for national security purposes is discussed according to three rubrics: trust and transparency, legality and proportionality, and independent oversight. The accountability features of the DPF are considered in order to illustrate the interface between the EU and US legal orders and to demonstrate the elements of a possible accountability-based international code of practice.

Keywords
Accountability, interoperability, government access, national security, trust, transparency, oversight, redress

1. Introduction

This article appears in the context of greater international efforts toward achieving interoperability of privacy and data protection frameworks in order to facilitate international transfers of personal data. It considers the problem for data flows caused by government access to personal data imported by private operators from states with a high level of data protection.

Governments access personal data for important public interests, most notably criminal law enforcement and national security. In respect of criminal law enforcement, authorities operate under formal and transparent standards and procedures. In this area, there has

already been significant progress on formal international cooperation,[1] and law enforcement authorities may compel access in the context of cross-border data transfers by relying on formal legal process.

Governments accessing data for the purpose of national security may also rely on formal orders to private entities to produce data within their possession or control, on the basis of a judicial authorisation.[2] However, intelligence agencies also engage in opaque processes based on executive measures,[3] and covertly obtain data from private actors.[4] Such surveillance has become a worldwide issue,[5] with 'extensive evidence that governments around the world have been collecting data on a very large scale'.[6] In view of the specific issues raised by processing for national security purposes, and the increasing attention being paid to them, this article concentrates on this dimension of government access.

At present, there is concern in both the data protection and intelligence communities about the level of data protection requirements and the lack of legally binding standards at international level for national security processing of personal data.[7] For one group, it is a problem for the protection of the fundamental right to data protection, for the other a problem for the effective protection of public security. Messaging services are increasingly adopting end-to-end encryption, hampering access to information by government agencies.[8] In addition, there is a problem for organisations exporting personal data from jurisdictions with strict privacy standards to third countries. Such controllers are under a heavy burden to assess the privacy rules and practices in those countries.[9] In 2019, the Organisation for Economic Cooperation and Development (OECD) identified 'uncertainty regarding legal privacy regimes' as the single biggest challenge to transborder personal data flows.[10]

Against this background, this article seeks to advance the principle of accountability as an internationally accepted means of reconciling the different perspectives of national security and data privacy, based on established and widely understood accountability norms and

1. See in particular the Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (Budapest Convention) (CETS No 224). See also Regulation (EU) 2023/1543 of 12 July 2023 on European Production and Preservation Orders for electronic evidence in criminal matters and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118, and Directive (EU) 2023/1544 of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [2023] OJ L 191/181.
2. For example, Section 702 of the US Foreign Intelligence Surveillance Act, 50 USC Section 1881a.
3. Ira S Rubinstein, Gregory T Nojeim and Ronald D Lee, 'Systematic government access to personal data: a comparative analysis' (2014) 4(2) *International Data Privacy Law* 96, 104 <https://doi.org/10.1093/idpl/ipu004>.
4. ibid 103 ('sometimes it is in the interests of both governments and companies to proceed quietly, and the companies are often prohibited from public comment').
5. Office of the High Commissioner for Human Rights (OHCHR), *The Right to Privacy in the Digital Age* (2018) UN Doc A/HRC/39/29, 5-7; OHCHR, *The Right to Privacy in the Digital Age* (2018) UN Doc A/HRC/51/17, 2-13.
6. Fred H Cate and James X Dempsey, 'Introduction' in Fred H Cate and James X Dempsey (eds), *Bulk Collection, Systematic Government Access to Private-Sector Data* (Oxford University Press 2017) xxviii.
7. See the discussion of international standards and principles in section 6.1 below.
8. Tom Uren, 'The future of assistance to law enforcement in an end-to-end encrypted world', Issues paper, Report No 58/2022 (ASPI) 6. See also 'International Statement: End-To-End Encryption and Public Safety' by Australia, Canada, India, Japan, New Zealand, the United Kingdom (UK) and the United States (U.S.) (also referring to Conclusions of the Council of the EU) 11 October 2020, available at: <www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety>, accessed 10 October 2023. All other URLs cited in this article were last accessed on the same date.
9. Theodore Christakis, 'After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe', *European Law Blog* (21 July 2020) <https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe>.
10. Lisa Robinson, Kosuke Kizawa and Elettra Ronchi, 'Interoperability of privacy and data protection frameworks, Toolkit note' (OECD 2021) 8, highlighted in Figure 1 ('Main challenges to transborder flows of personal data, OECD Countries, 2019').

mechanisms. First, the principle can function as a 'Rosetta Stone' between the privacy and intelligence communities: its practical nature will be familiar to the intelligence community, whilst its proactive approach and binding nature increase respect for data privacy. Second, the basic norms of accountability are sufficiently common worldwide to permit greater privacy interoperability between democratic states in the future.

We set out the imperatives governing European Union (EU) policy on international transfers of personal information imposed by its values and fundamental rights principles. European case law on surveillance and international transfers under the Charter of Fundamental Rights of the European Union (EUCFR or Charter) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) is briefly discussed in order to explain the particular constraints applying to the transfer of personal data from Member States of the EU and European Economic Area (EEA) and Council of Europe Member States to non-European states ('third countries'), together with the scope for possible flexibility. In this respect, we consider the accountability features of the EU-US Data Privacy Framework (DPF), to examine how a legally binding and multi-layered system may satisfy concerns specifically relating to data flows and government access to personal data.

The application of the principle of accountability to government access is not novel, and we acknowledge and describe much of the important work undertaken by scholars and organisations at the international and European levels. In particular, we stress the need to apply an accountability analysis to government access according to three rubrics: (i) trust and transparency; (ii) legality and proportionality; and (iii) independent oversight. We conclude by describing recently agreed international principles for government access and suggest that an accountability-based international code of practice may be a means of realising those principles.

2. The Legal Imperatives Governing EU Policy

2.1 The EU Interest in Greater Interoperability

It is important to stress at the outset that the General Data Protection Regulation (GDPR)[11] and its predecessor, the Data Protection Directive[12], were adopted to facilitate the free flow of personal data within the EU on the basis of common fundamental rights standards;[13] they were 'not designed to prevent the processing of [personal] information or to limit the use of information technology'.[14] Article 1 GDPR sets out its objectives, to ensure the protection of natural persons with regard to the processing of personal data, with the result that the 'free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data'.[15] This fundamental objective of the GDPR was recognised at an OECD

11. 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) [2016] OJ L 119/1.
12. 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 [1995] OJ L 281/31 (repealed).
13. See recital 10 GDPR ('In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union').
14. Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' in Marise Cremona (ed), *New Technologies and EU Law* (Oxford University Press 2017) 123.
15. Article 1(3) GDPR.

Roundtable on interoperability in May 2018, which noted that the GDPR 'facilitates privacy interoperability through legislative harmonisation, allowing the flow of personal data within the European Union'.[16]

The EU has developed the concept of free data transfers from the EU to states that guarantee an 'adequate' level of protection, defined as 'essentially equivalent' by the EU Court of Justice (CJEU).[17] One common misconception is that of 'fortress Europe', which posits the GDPR as designed to build an additional barrier between the EU and the rest of the world. The EU data protection legislation is intended to *facilitate* data flows, which it does by setting the conditions for data transfers in order to ensure that the level of protection of the persons concerned is not undermined.[18]

Since its adoption, the GDPR has generated significant interest at home and abroad as a model for ensuring compliance with data protection. It has led many other jurisdictions to follow a similar approach, and the 'Brussels effect'[19] has helped spur the spread of data protection legislation across 164 countries.[20] In addition, some 73 countries assert that they carry out adequacy determinations.[21] There are also partly comparable reciprocity mechanisms in the United States.[22]

The EU Commission itself regards the adequacy approach as both sufficient and as a possible global solution for data flows. For example, it asked the European Data Protection Board (EDPB or Board) to approve the draft adequacy decisions for the UK lest 'critical opinions … show that our model is not credible as a global solution and that adequacy is basically "mission impossible" if even a former Member State that has decided to essentially keep the same data protection rules is not considered adequate'.[23]

However, we would argue that the unilateral 'adequacy' model is too limited for the EU itself, in purely practical terms. The states recognised by an EU adequacy decision only provide a small core of countries that may share data with EU/EEA Member States based on unilateral recognition of each by the EU.[24] This is because the assessment process by the Commission leading to an adequacy decision under Article 45 GDPR is slow, limited by the size of the small 'adequacy' team within its International Affairs and Data Flows Unit, which can only process a handful of draft adequacy decisions per year. Moreover, since the CJEU ruling in *Schrems II*,[25] discussed below, the Commission has

16. Robinson and others (n 10) 9.
17. Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, judgment of 16 July 2020 (Grand Chamber) (ECLI:EU:C:2020:559) para 94. The principle of 'essential equivalence' has been consolidated into recital 104 GDPR.
18. Article 44 and recital 101 GDPR.
19. Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).
20. Graham Greenleaf, 'Global Privacy Laws 2023: 162 National Laws and 20 Bills' (2023) 181 *Privacy Laws and Business International Report* 1, 2-4 <http://dx.doi.org/10.2139/ssrn.4426146>. In addition, in May and August 2023, respectively, Grenada and India adopted data protection legislation.
21. International Association of Privacy Professionals (IAPP), 'Global Adequacy Capabilities', available at: <https://iapp.org/resources/article/infographic-global-adequacy-capabilities>.
22. See Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, Section 3(c)(f), and the Judicial Redress Act 2015, section 2(d)(1), implementing the Data Protection and Privacy Agreement (the 'Umbrella Agreement').
23. Vincent Manancourt, 'Why Brussels went easy on Britain on its data deal', *Politico* (30 June 2021) <www.politico.eu/article/why-brussels-went-easy-on-britain-in-data- adequacy-deal>.
24. Note also the possibility for 'adequate' jurisdictions to recognise each other as adequate, and hence develop a larger group of states able to transfer personal data freely amongst them. See also the Joint Declaration on Privacy and the Protection of Personal Data of 23 February 2022, <https://www.eeas.europa.eu/eeas/joint-declaration-privacy-and-protection-personal-data_en>.
25. Case C-311/18, *Data Protection Commissioner v Maximilian Schrems* ('Schrems II'), judgment of 16 July 2020 (Grand Chamber) (ECLI:EU:C:2020:559).

also needed to assess government access, which has significantly extended the analysis required.

The need for a broader approach has been recognised by the former lead US negotiator on data transfers, Chris Hoff, who has commented that:

> There have been 13 adequacy decisions in the past 26 years and one [for the US] keeps getting knocked down. So interoperable frameworks … have to be the future.[26]

Moreover, the commonly used substitutes for general adequacy decisions, standard contractual clauses (SCCs) and binding corporate rules (BCRs), which have been described as 'mini adequacy decisions',[27] equally require an assessment of government access to personal data in the receiving states concerned, as discussed below.

From the EU perspective, an international solution to interoperability would be much more efficient.

2.2 European Values, Fundamental Rights and Case Law on Government Access

The standards on international transfers imposed by the CJEU and other EU bodies must be understood in the light of EU values and fundamental rights and freedoms,[28] which themselves build on the fundamental rights set out in the ECHR. The values of the EU, set out in Article 2 of the EU Treaty (TEU)—respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights[29]—are at the heart of European identity. Since the Lisbon Treaty came into force in December 2009, the Charter has served as a constitutional Bill of Rights, setting out the fundamental rights and values against which EU and national law and international treaties may be tested. Particularly relevant in the present context are the fundamental rights to privacy, protection of personal data, freedom of expression and access to an effective judicial remedy, enshrined in Articles 7, 8, 11 and 47 EUCFR.

With regard to international transfers, Article 44 GDPR makes it clear that its aim is to 'ensure that the level of protection of natural persons guaranteed by [that regulation] is not undermined'.[30] Moreover, the CJEU has applied the Charter to require that EU data receive a high level of protection when they are transferred to third countries,[31] whether in the context of EU international agreements,[32] Commission adequacy decisions[33] or standard contractual clauses.[34]

---

26. Manancourt (n 23).
27. Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (*European Law* Blog 17 July 2020) <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation>.
28. See generally Friedrich Erlbacher and Katarzyna Herrmann, 'Fundamental Values of the European Union: from principles to legal obligations' in European Commission, Legal Service, *70 Years of EU Law – A Union for its Citizens* (Publications Office of the EU 2022) Part 1, 30-53 <https://data.europa.eu/doi/10.2880/02622>.
29. The principles in the second sentence of Article 2 are equally regarded as values: ibid 34.
30. *Schrems II* (n 25) para 94.
31. Christopher Kuner, 'Protecting EU Data outside EU Borders under the GDPR' (2023) 60 *Common Market Law Review* 77, 95-96 <https://doi.org/10.54648/cola2023004>.
32. Opinion 1/15 ('EU-Canada PNR Agreement'), judgment of 26 July 2017 (Grand Chamber) (ECLI:EU:C:2017:592) paras 119-231.
33. Case C-362/14, *Maximilian Schrems v Data Protection Commissioner*, judgment of 6 October 2015 (Grand Chamber) ('Schrems') (ECLI:EU:C:2015:650) paras 38–40.
34. *Schrems II* (n 25) para 99.

2.3 Government Access for National Security Purposes

It has been argued that the processing of personal information by intelligence agencies falls outside the scope of EU law,[35] on the basis of Article 4(2) final sentence TEU ('national security remains the sole responsibility of each member state').[36] This is in contrast to the ECHR, which fully applies to such processing. However, the limitation in Article 4(2) TEU applies to the activities that intelligence agencies carry out themselves, by the exercise of sovereign authority. It does not apply to information collected by organisations under EU law which is then accessed for intelligence purposes, in which case it must respect the requirements laid down by EU law.[37] The CJEU has reiterated this point in multiple rulings,[38] including *Schrems II* concerning international transfers.[39]

In this context, the CJEU and the European Court of Human Rights (ECtHR) have both taken particular care with regard to government surveillance and the profiling of citizens. In 1984, the ECtHR handed down its famous ruling in *Malone v UK*, in which Judge Pettiti warned:

> The danger threatening democratic societies … stems from the temptation facing public authorities to 'see into' the life of the citizen. … public authorities seek … to build up a 'profile' of each citizen… Through use of the 'mosaic' technique, a complete picture can be assembled of the life-style of even the 'model' citizen.[40]

In 2014, the CJEU struck down the EU Data Retention Directive[41] in its *Digital Rights Ireland* ruling. The Directive required providers of publicly available electronic communications services or of public communications networks to retain traffic and location data so that they might be available to the authorities for the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism. However, it was not sufficiently circumscribed to ensure that it was actually limited to what was strictly necessary, and was found to be a 'wide-ranging and particularly serious interference' with the fundamental rights of privacy and data protection enshrined in Articles 7 and 8 EUCFR.[42]

---

35. Stewart Baker, 'How Can the U.S. Respond to Schrems II?', *Lawfare* (21 July 2020) <www.lawfareblog.com/how-can-us-respond-schrems-ii>.
36. The scope of the GDPR is correspondingly limited under Article 2(2) paras (a) and (d) GDPR.
37. See Article 23(1) paragraphs (a) to (d) GDPR; Article 15 of the ePrivacy Directive (Directive 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37, as amended); and Article 25(1)(a) of Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('EUDPR') [2018] OJ L 295/39.
38. See most recently Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministres*, judgment of 21 June 2022 (Grand Chamber) (ECLI:EU:C:2022:491) paras 66-68.
39. *Schrems II* (n 25) para 86. The CJEU also referred to Article 45(2)(a) GDPR, which obliges the Commission, 'when assessing the adequacy of the level of protection afforded by a third country', to take account, inter alia, of '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.' See also the detailed reasoning and case law cited in the Opinion of Advocate General Saugmandsgaard Øe in the same case (ECLI:EU:C:2019:1145) paras 203-226.
40. *Malone v United Kingdom* [Plenary] no 8691/79, 2 August 1984, Concurring Opinion of Judge Pettiti, 38.
41. Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54 (repealed).
42. Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others*, judgment of 8 April 2014 (Grand Chamber) (EU:C:2014:238) para 65.

This ruling was followed by *Tele2 Sverige and Watson* in 2016, concerning national provisions in Sweden and the UK adopted for the purpose of combating serious crime, in particular organised crime and terrorism. As in *Malone*, the CJEU noted that metadata alone, without regard to the content of communications, are 'liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained' and provide in particular the means of 'establishing a profile of the individuals concerned'.[43] Moreover, the Court found that such surveillance is liable to 'deter users of electronic communications systems from exercising their freedom of expression, guaranteed in Article 11' EUCFR.[44] As a result, the CJEU held that the general and indiscriminate retention of traffic and location data was a disproportionate interference with Charter rights under Articles 7, 8 and 11 (freedom of association).[45]

In *La Quadrature du Net*, the Court addressed national security in addition to serious crime. It affirmed *Tele2* to the effect that normally only targeted surveillance (for example, on the basis of a geographic criterion) is acceptable for combating serious crime. However, the Court considered that the 'importance of the objective of safeguarding national security … goes beyond that of the other objectives … of combating crime in general, even serious crime, and of safeguarding public security.' In consequence, it ruled that in the case of a 'serious threat' to national security that proves to be 'genuine and present or foreseeable', an order for general and indiscriminate data retention can be made, so long as it is subject to effective and binding review by a court or independent body.[46]

After these CJEU decisions, the ECtHR Grand Chamber handed down rulings on national security in *Centrum för rättvisa*[47] and *Big Brother Watch*.[48] Unlike the CJEU, which accepted bulk collection in the specific circumstances described above, the ECtHR accepted bulk surveillance in principle, subject to the necessary safeguards (equally important to the CJEU) that surveillance must be based on legislation, and that access to retained data should be subject to 'end-to-end safeguards' from independent *ex ante* authorisation to *ex post* supervision and review by a court or by an independent administrative body.[49] This approach partly affirms the Court's settled requirement for 'continuous control'[50] at every stage of surveillance,[51] and partly reflects the greater readiness of the Strasbourg Court to accept the margin

43. Joined Cases C-203/15 and C-698/1, *Tele2 Sverige and Watson*, judgment of 21 December 2016 (Grand Chamber) (ECLI:EU:C:2016:970) para 99.
44. ibid para 101.
45. ibid paras 103-107.
46. Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v Premier ministre and Others* and *Ordre des barreaux francophones and germanophone and Others*, judgment of 6 October 2020 (Grand Chamber) (ECLI:EU:C:2020:791) paras 136-139. The Court has consistently applied this approach in subsequent cases: see eg Case C-140/20, *GD v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, judgment of 5 April 2022 (Grand Chamber) (ECLI:EU:C:2022:258) para 67.
47. *Centrum för rättvisa v Sweden* [GC] no 35252/08, 25 May 2021.
48. *Big Brother Watch and Others v The United Kingdom* [GC] nos 58170/13, 62322/14 and 24960/15, 25 May 2021.
49. ibid § 350.
50. *Roman Zakharov v Russia* [Grand Chamber], no 47143/06, § 275, 4 December 2015.
51. ibid § 233. See EU Fundamental Rights Agency (FRA), *Surveillance by Intelligence Services, Fundamental Rights Safeguards and Remedies in the EU, Volume. II: Field Perspectives and Legal Update* (Luxembourg Publications Office 2017) ch 10, 93.

of appreciation allowed for national courts.[52] In any event, it has drawn a line between the approaches of the two courts.[53]

In parallel, the issue of government access to personal data has bedevilled negotiations between the European Union and the United States for more than two decades. The EU instruments underlying three adequacy regimes agreed between the EC/EU and the US—the original 2004 Passenger Name Record (PNR) Agreement,[54] the Safe Harbor and the Privacy Shield—have been invalidated by the CJEU. To these should be added the CJEU ruling on the draft EU-Canada PNR Agreement, discussed further below.

The catalyst for the latest negotiations between the EU and the US was *Schrems II*, invalidating the Commission decision recognising the adequacy of the Privacy Shield. The Court offered no comment on the Privacy Shield's commercial aspects and its system of self-certification, which have been updated alongside the DPF, as described below. Instead, the CJEU criticised the lack of proportionality in government access to transferred data and the failure to provide for effective judicial redress. Moreover, it emphasised that the requirement of 'essential equivalence' applies equally to all the transfer mechanisms in Chapter V GDPR, and thus also transfers under an SCC or BCR.[55]

The EDPB swiftly published a set of FAQs[56] and set up a task force to advise on supplementary measures that data exporters might take to ensure adequate protection. The Board set out its considered analysis in two Recommendations which specified the conditions under which international transfers under Articles 45 and 46 GDPR may be carried out, namely Recommendations 01/2020 on measures that supplement transfer tools (the STT Recommendations)[57] and Recommendations 02/2020 on European Essential Guarantees for surveillance measures (the EEG Recommendations).[58]

The STT Recommendations set out a 'roadmap' of six steps that a data exporter should take in order to find out whether it needs to put in place supplementary measures to be able to legally transfer data outside the EEA. Step three requires an assessment whether that

52. See Jean-Pierre Cot, 'Margin of Appreciation' in *Max Planck Encyclopedia of Public International Law* (June 2007) paras 7 and 16-24.
53. See Juraj Sajfert, 'The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?', *European Law Blog* (8 June 2021) <https://europeanlawblog.eu/2021/06/08/big-brother-watch-and-centrum-for-rattvisa-judgments-of-the-grand-chamber-of-the-european-court-of-human-rights-altamont-of-privacy>.
54. Joined Cases C-317/04 and C-318/04, *European Parliament v Council and Commission*, judgment of 30 May 2006 (Grand Chamber) (ECLI:EU:C:2006:346). See further Christopher Docksey, 'The European Court of Justice and the Decade of Surveillance' in Hielke Hijmans and Herke Kranenborg (eds), *Data Protection anno 2014: How to Restore Trust?* (Intersentia 2014) 97. For the current EU-US PNR Agreement, see <www.dhs.gov/publication/passenger-name-records-agreements>.
55. Normally, the systemic provisions under Articles 45 and 46 GDPR should be used, not the *ad hoc* derogation under Article 49. In *Schrems II* (n 25), the CJEU referred to the reserve role of Article 49 'in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR' (para 202), but this may be interpreted in light of the requirement under Article 44 that all provisions in Chapter V should be applied in such a way as to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined: see EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (25 May 2018) 3. Cf Rob van Eijk and Gabriela Zanfir-Fortuna, 'Schrems II: Article 49 derogations may not be so narrow after all?', *Future of Privacy Forum blog* (4 February 2021) <https://fpf.org/blog/schrems-ii-article-49-gdpr-derogations-may-not-be-so-narrow-and-restrictive-after-all>.
56. EDPB, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (23 July 2020).
57. EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (version 2, 18 June 2021).
58. EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (10 November 2020).

mechanism is effective to ensure compliance in the context of the national law of the third state. The EEG Recommendations are devoted to providing guidance in that respect on how to assess a third country's national security measures.

3. The EU-US Data Privacy Framework

On 25 March 2022, the EU and the United States announced that they had agreed in principle on a new Data Privacy Framework (DPF), which has both commercial and governmental aspects and was finalised in 2023.

On the commercial side, the DPF maintains the 'voluntary but binding' approach of the Safe Harbor and the Privacy Shield towards organisations importing personal information from the EU. Such organisations may self-certify that they comply with the revised and updated commercial data protection principles inherited from the predecessor Privacy Shield, and, if so certified, may freely transfer personal data from EU territory to the United States.[59]

On the US government side,[60] it consists of Presidential Executive Order 14086 of 7 October 2022 on *Enhancing Safeguards for United States Signals Intelligence Activities* (EO 14086), together with an Attorney General Regulation on the Data Protection Review Court.[61] The privacy and civil liberties safeguards in EO 14086 are further implemented by Intelligence Community Procedures.[62]

On the EU side, the Commission adopted an Adequacy Decision on 10 July 2023.[63]

With regard to proportionality, EO 14086 limits US signals intelligence activities to what is necessary and proportionate. To this end, there is a list of twelve 'legitimate objectives' for collection and four 'prohibited objectives'. Collection of data within the US (ie all the data that is transferred to the US) must be targeted. Collection of data outside the US must prioritise targeted collection, and bulk collection is limited to situations where a validated objective cannot reasonably be obtained by targeted collection, and only to the extent and in a manner that is proportionate to the validated intelligence priority.

With regard to governance, EO 14086 and the accompanying Regulations lay down a two-layered redress mechanism to consider complaints against intelligence activities and provide any necessary remediation, subject to the supervision role of the Privacy and Civil Liberties Oversight Board (PCLOB). In the first layer, the Civil Liberties Protection Officer (CLPO) of the Office of the Director of National Intelligence investigates complaints[64] and can make

59. As from 10 July 2023, EDPB, Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023, pt 1 <https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf>.
60. In addition to existing safeguards such as Section 702 of the Foreign Intelligence Surveillance Act ('FISA 702'), in particular the supervisory role of the Foreign Intelligence Surveillance Court ('FISC'): see US White Paper of September 2020 on US Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-US Data Transfers after Schrems II; and Adequacy Decision of 10 July 2023, recitals 142-150.
61. Federal Register Vol 87, No 198 (14 October 2022) 62303-62308.
62. See *ODNI Releases Intelligence Community Procedures Implementing New Safeguards in Executive Order 14086*, available at <www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086>.
63. Commission Implementing Decision of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU-US Data Privacy Framework (C(2023) 4745 final). Full details of the DPF may be found in the Adequacy Decision.
64. The EDPB advises that data subjects located in the EU may complain to their national DPA, which will hand the complaint to the EDPB, which will in turn transmit the complaint to the competent US authority: EDPB (n 59) pt 4.

decisions binding on intelligence agencies. In the second layer, the decisions of the CLPO can be appealed to the Data Protection Review Court (DPRC), created by a regulation issued by the Attorney General. The members of the DPRC are independent, appointed for fixed terms, and its decisions are legally binding.

Both bodies operate in secret, and claimants' interests are represented before the DPRC by a special advocate with access to the same classified material as the judges. The decisions of both the CPLO and the DPRC simply state that either no violations were identified or that a 'determination requiring appropriate remediation' was made.

The adoption of the Adequacy Decision of 10 July 2023 brought into effect a designation by the Attorney General that the EU and the three EEA/EFTA Member States are 'qualifying states' for purposes of implementing the redress mechanism.[65]

4. The Role of Accountability

4.1 The Principle of Accountability

The term 'accountability' is generally used to indicate responsibility, answerability and good governance, and this concept may be found in the larger literature on accountability which is separate to, but feeds into, the data privacy principle termed 'accountability'.[66]

In order to facilitate clearer discussions of its precise meaning, which is a 'core issue' of political science, Koppel has developed an influential and useful typology of five conceptions of accountability. These are *transparency* (an accountable organisation must explain or account for its actions); *liability* (individuals and organisations should be held liable for their actions); *controllability* (did the organisation do what its principal desired); *responsibility* (fidelity to the rules); and *responsiveness* (an organisation's attention to direct expressions of the needs and desires of its constituents or clients).[67] Under this typology, the term accountability was originally used in data protection law in the sense of responsibility, a controller being responsible for ensuring compliance with the data protection rules, particularly those on data quality. This can be found in Article 6(2) of the Data Protection Directive, now Article 5(2) GDPR.[68]

However, behavioural science suggests that an approach based on enforcement of compliance, is insufficient.[69] Hodges has convincingly argued that effective respect for data privacy has to be based on 'cultures, relationships of trust, evidence of who can or cannot be trusted, and ways of demonstrating what the ethical quality of actual behaviour is'.[70]

---

65. Attorney General Designation Pursuant to Section 3(f) of Executive Order 14086 <www.justice.gov/d9/2023-07/Attorney%20General%20Designation%20Pursuant%20to%20Section%203%28f%29%20of%20Executive%20Order%2014086%20of%20the%20EU%20EEA.pdf>. See also the Memorandum in Support of Designation, available at <www.justice.gov/d9/2023-07/Supporting%20Memorandum%20for%20the%20Attorney%20General%27s%20designation%20of%20EU-EEA.pdf>.
66. For the history and development of accountability as a data privacy principle, see Christopher Docksey, 'Article 24' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (Oxford University Press 2020) 555–570.
67. Jonathan GS Koppell, 'Pathologies of Accountability: ICANN and the Challenge of Multiple Accountabilities Disorder' (2005) 65(1) *Public Administration Review* 94, 96–99 <https://doi.org/10.1111/j.1540-6210.2005.00434.x>.
68. Misleadingly entitled 'accountability': see Christopher Docksey, 'Article 24' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary, 2021 Update* (Oxford University Press 2021) 115–116 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839645>.
69. See generally Christopher Hodges and Ruth Steinholtz, *Ethical Business Practice and Regulation. A Behavioural and Values-Based Approach to Compliance and Enforcement* (Hart 2017).
70. Christopher Hodges, 'Delivering Data Protection: Trust and Ethical Culture' (2018) 1 *European Data Protection Law Review* 79 <https://doi.org/10.21552/edpl/2018/1/9>.

The modern concept of accountability must be understood in this sense, as a proactive and demonstrable commitment by the individuals in an organisation to respect the ethical and legal framework. It has become one of the fundamental innovations of modern data protection law,[71] figuring in the updated OECD Guidelines[72] and Modernised Convention 108 (Convention 108+),[73] the GDPR and the Law Enforcement Directive (LED),[74] as well as constituting the guiding principle in the APEC Cross-Border Privacy Rules (CBPR) system.

Within EU law, the principle of accountability may be found in Articles 5(2) and 24 GDPR. Article 5(2) imposes a legal responsibility for compliance with the data protection principles of Article 5(1), and Article 24 requires that controllers implement appropriate technical and organisational measures to ensure such compliance. Both provisions require the controller to be able to demonstrate compliance to external stakeholders. Article 24(1) emphasises that these internal policies and accountability mechanisms should be scaled appropriately, according to a risk-based approach which takes into account the 'nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons'. This risk-focused wording is echoed in the various accountability mechanisms of data protection by design,[75] security of processing,[76] data breach notifications,[77] data protection impact assessments (DPIA),[78] the tasks of the DPO,[79] as well as in the assessment of administrative fines.[80]

Under the APEC CBPR system, there is an accountability mechanism focussed on ensuring compliance of international transfers of personal data with the 2005 APEC Privacy Framework, updated in 2015, and its nine Privacy Principles,[81] based on the 1980 OECD Guidelines.[82] In 2022, seven APEC CBPR participating economies established the Global CBPR Forum[83] for the purpose of transforming CBPR into a global transfer mechanism, and invited countries from other regions to join.[84]

---

71. Case C-340/21, *Natsionalna agentsia za prihodite*, Opinion of AG Pitruzzella of 27 April 2023 (ECLI:EU:C:2023:353) para 21.
72. The updated OECD Privacy Guidelines of 2013 add the new meaning of accountability, in the sense of proactive and demonstrable compliance, in a new Part Three on 'Implementing Accountability'.
73. See Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No 223), 10 October 2018 (Convention 108+). Article 10 Convention 108+ on 'additional obligations' provides for a modern accountability obligation that 'controllers and, where applicable, processors take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate … that the data processing under their control is in compliance'.
74. Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.
75. Article 25(1) GDPR.
76. Article 32(1) GDPR.
77. Articles 33(1) and 34(1) GDPR.
78. Article 35(1) GDPR.
79. Article 39(2) GDPR.
80. Article 83(2)(a) GDPR.
81. Asia Pacific Economic Cooperation, APEC Privacy Framework (2015) <https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1>.
82. OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) <https://doi.org/10.1787/9789264196391-en>.
83. See Center for Information Policy Leadership (CIPL), 'Cross-Border Privacy Rules, Privacy Recognition for Processors, and Global CBPR and PRP, Frequently Asked Questions' (26 June 2020) 3 <www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_cpbr_and_prp_faq_jun23.pdf>.
84. The United Kingdom was accepted on 3 June 2023 as an Associate of the Forum.

To participate in the APEC CBPR system, companies must implement data privacy policies consistent with the APEC Privacy Framework, carry out a self-assessment, and have these assessed as compliant by an independent Accountability Agent. Once assessed as compliant, a company can display a seal or Trustmark indicating its participation in the CBPR system. The CBPR system is thus an interesting combination of voluntary self-regulation and binding regulation. It has been found to ensure effective accountability in specific cases, although it does not ensure the basic standards for EU law transfers.[85]

4.2 Accountability as the 'Rosetta Stone' for Increased Interoperability

Accountability may serve as a possible means of reconciling privacy and security for the purposes of data transfers and interoperability, by providing a 'Rosetta Stone' for mutual comprehension between the intelligence and data protection communities. We elaborate this viewpoint as follows.

First, accountability is a universal principle, familiar to the legal systems which would be interested in interoperability. In its modern form, it is a key part of specific privacy and/or data protection legislation[86] or regulatory guidance[87] in every continent, facilitating compliance in those jurisdictions.

Second, accountability is both practical and familiar to national security professionals. It is common sense and moves data protection from 'theory to practice'[88] by providing a practical list of matters that should be considered and documented when processing personal information.[89] It can be seen as a dynamic and ongoing roadmap or checklist, which requires the controller to map its data processing and to assess precisely what are the outcomes and risks involved in its processing of personal information, to develop measures to deal with those risks throughout the processing, and to document its decisions. It is familiar to security or audit professionals, since for the most part it is sim-

85. European Commission, Directorate-General for Justice and Consumers, G Bodea, K Stuurman, M Brewczyńska and others, *Data protection certification mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report – Study and Annexes* (2019) <https://doi.org/10.2838/115106>; Article 29 Working Party (WP29), Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents (WP212, 27 February 2014).

86. In Africa, accountability has been considered as the ability of a data subject to hold a data controller accountable, the ability of the regulatory authority to hold a data controller accountable, and the ability of the public to hold the regulatory authority accountable: see Data Protection in Africa: A Look at OGP Member Progress (August 2021), Open Government Network, August 2021, at 7. However, it can be found in the sense of this article in Section 24(3) of the recent Nigeria Data Protection Act 2023. In Asia, accountability elements can be found in the legislation in South Korea and, to a lesser extent, Japan: see the Commission adequacy decisions for Japan (Decision (EU) 2019/419 of 23 January 2019 [2019] OJ L76/1, pt 2.3.8) and for South Korea (Decision 2022/254 of 17 December 2021 [2022] OJ L 44/1, pt. 2.3.10). In North America, the Canadian Personal Information Protection and Electronic Documents Act ('PIPEDA') of 2000 (last revision November 2018), requires organisations to comply with a set of legal obligations that are based on ten Fair Information Principles, of which accountability is the first (see Schedule 1). In South America, Mexico included accountability elements in Article 44 III and V of the Regulations of 22 December 2011 to the Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) of 2010, and Brazil included an accountability approach in Article 6(X) of the General Data Protection Law (Lei Geral de Proteção de Dados) of 2018.

87. See eg the Privacy Management Framework published in 2015 by the Australian Information Commissioner on the Australian Privacy Principles ('APPs') laid down in Schedule 1 of the federal Privacy Act of 1988. The first APP covers the open and transparent management of personal information including having a privacy policy. See further Docksey (n 66) 559-560.

88. WP29, Opinion 3/2010 on the principle of accountability (WP173, 13 July 2010) 2-3.

89. See eg the guidance on data governance in the ASEAN Data Management Framework of January 2021.

ply good practice.[90] Practical measures include the development of internal policies, staff training and education,[91] audit, systems for internal and external oversight, and transparency.

Third, accountability provides a toolkit for compliance, based on a number of key mechanisms which can be found, for example, in the GDPR[92] and the LED.[93] Accountability tools which are most relevant for government agencies include privacy or data protection by design,[94] record keeping, security and data breach preparation, privacy or data protection impact assessments (PIAs or DPIAs) and related ways to identify and address privacy issues, and logging.[95]

Fourth, from a data protection perspective, an accountable controller will have taken responsibility for its processing of personal data: it will have applied an effective accountability analysis to that processing, and it will be using accountability mechanisms to address the identified outcomes and risks. Data protection will have been integrated into its regular control, support and core processes. For example, data mapping is a precondition for purpose limitation[96] and data minimisation,[97] enabling an accountable controller to comply with these principles.[98] Moreover, they not only protect privacy but also limit the amount of data that has to be collected and the amount that has to be given human attention.

---

90. See eg Rebecca Richards, Civil Liberties and Privacy Office, NSA, 'Privacy interests identified and addressed by government privacy officials', prepared remarks for PCLOB of 12 November 2014, available at: <https://media.defense.gov/2021/Aug/18/2002834229/-1/-1/0/PCLOB_REMARKS_20141112.PDF>.
91. 'Training is a … key instrument for the promotion of a professional institutional culture within intelligence services': UN Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (UN Document A/HRC/14/46, 17 May 2010) Practice 19, para 26. See also the references to awareness raising in the BND in Germany and instruction and training in GCHQ in the UK in FRA (n 51) 59.
92. Docksey (n 66) 565-566. For more detailed analysis of these mechanisms, see the comments by Christopher Kuner on the individual Articles in Chapter IV GDPR in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (Oxford University Press 2020) 571-754.
93. The word 'accountability' is only used once in the LED—in recital 61, which states that it is unnecessary to notify a data breach to a supervisory authority where 'the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons'. However, the key elements of accountability are equally applicable to law enforcement under the LED, by virtue of Articles 4 ('Principles') and 19 ('Obligations of the controller'), together with many of the same tools in the accountability toolbox.
94. As well as security by design: see Lee A Bygrave, 'Security by Design: Aspirations and Realities in a Regulatory Context' (2021) 8(3) *Oslo Law Review* 126 <https://doi.org/10.18261/olr.8.3.2>.
95. The obligation to keep logs is an accountability mechanism which is particularly related to government activity. It is not mentioned in the GDPR but has been consolidated in Article 25 LED, which refers to six processing operations, namely collection, alteration, consultation, disclosure including transfers, combination and erasure, and which assigns particular importance to consultation and disclosure. See further Juraj Sajfert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities' (December 2018) 15-17 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873>. The ECtHR has similarly stressed the need for recording and restricting access to health and medical files in *I v Finland*, no 20511/03, 17 July 2008. Most recently, the CJEU has linked log data to the right of access under Article 15(1) GDPR: see Case C-579/21, *Pankki S*, judgment of 22 June 2023 (ECLI:EU:C:2023) paras 69-75.
96. Data must be collected for 'specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes' under Articles 5(1)(b) GDPR and 4(1)(b) LED. See also UN Compilation (n 91) 'Management and use of Personal data', Practices 23 and 24, 21-22.
97. Data must be 'adequate, relevant and not excessive in relation to the purposes for which they are processed' under Articles 5(1)(c) GDPR and 4(1)(c) LED.
98. The refusal by Europol to respect the principle of data minimisation, consolidated into specific provisions of the updated Europol Regulation, led to the challenge by the EDPS in Case T-578/22, *European Data Protection Supervisor v European Parliament and Council of the European Union.* The General Court has ruled that the application was inadmissible: Order of 6 September 2023 (ECLI:EU:T:2023:522). An appeal to the CJEU is pending.

Experience has shown that the two most essential conditions for effective accountability in any organisation processing personal information are the commitment of top management and the appointment of a 'person with expert knowledge of data protection law and practices [to] assist the controller or processor',[99] that is, a DPO or Privacy Officer, discussed below. The role of the leadership of the organisation is crucial, both for creating an effective ethical culture[100] and for supporting the privacy team,[101] since '(c)ontrol led by the executive is in fact a pre-condition for setting up efficient oversight frameworks'.[102]

Indeed, even if other mechanisms are in place, the lack of management commitment can be determinative. This can be seen in the ruling in January 2023 of the UK Investigatory Powers Tribunal[103] that there had been a widespread corporate failure in MI5 and the Home Office, and 'serious failings in compliance with the statutory obligations of MI5 from late 2014 onwards'.[104] From an accountability perspective, this case underlines the need for top management commitment to ensure that the necessary procedure and safeguards are implemented. In the absence of such commitment, the safeguards in the system at question in the case all seem to have failed.[105]

This case also confirms the widely accepted need for confidential external oversight of intelligence activity, for the situation when other safeguards fail. In her 2017 High Court ruling in the *Schrems II* litigation, Justice Caroline Costello underlined that an adjudicative remedy has to be available when the administrative safeguards fail.[106]

In this respect, accountability is increasingly being recognised in CJEU jurisprudence.[107] The CJEU has consistently followed an 'accountability' approach in its case law, and its President, Koen Lenaerts, has observed that accountability is the 'central theme' of the GDPR[108], stressing the responsibility for processing of personal data.[109] It is likely that the CJEU would be open to an EU policy that promotes the accountability of government controllers.

99. Recital 97 GDPR.
100. EDPS Factsheet, 'EDPS launches Accountability Initiative' (7 June 2016) 2 ('Accountability goes beyond compliance with the rules—it implies culture change … endorsed by the highest level of the organisation's management … [and] … [r]esponsibility at the highest level'). See also Hodges (n 70) 74-75.
101. Alex Joel, 'Seek and Speak the Truth', *Just Security* (16 April 2020): 'Leaders and policymakers have a corresponding obligation to support those who speak the truth'. Available at <www.justsecurity.org/69706/seek-and-speak-the-truth>.
102. FRA (n 51) 59.
103. The Investigatory Powers Tribunal (IPT) is an independent court with jurisdiction over UK government access to personal data: see <www.ipt-uk.com/content.asp?id=10>.
104. *Liberty and Privacy International v Security Service and Secretary of State for the Home Department* [2023] UKIPTrib1, 30 January 2023, para 160.
105. The incident in the UK was not unique. See eg Andre Meister, 'German Federal Intelligence Service BND Violates Laws And Constitution By The Dozen' *Netzpolitik* (2 September 2016) <https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-and-constitution-by-the-dozen>.
106. *The Data Protection Commissioner v Facebook Ireland Limited & anor* [2017] IEHC 545 (3 October 2017) para 261.
107. Case C-129/21, *Proximus NV v Gegevensbeschermingsautoriteit*, judgment of 27 October 2022 (ECLI:EU:C:2022:833) para 81. See also Case C-340/21 *Natsionalna agentsia* (n 71).
108. CJEU President Koen Lenaerts, 'The EU General Data Protection Regulation five months on', speech at the 40th International Conference of Data Protection and Privacy Commissioners (25 October 2018) <www.youtube.com/watch?v=fZaKPaGbXNg>.
109. See Christopher Docksey and Hielke Hijmans, 'The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law' (2019) 5 *European Data Protection Law Review* 300 <https://doi.org/10.21552/edpl/2019/3/6>.

Finally, accountability is now extremely well-researched. Multiple reports and papers deal with how an organisation may develop an effective data management programme.[110]

In practice, work on accountability has mainly been applied to the private sector, including state processing for non-sovereign purposes,[111] although there has been criticism that it has not been sufficiently exploited with regard to transfers.[112] However, accountability is arguably even more important in the law enforcement and national security sectors, where individuals have no choice as to the processing of their personal information, often sensitive[113] and carried out in secret,[114] by public authorities in the exercise of sovereign power.

In 2017, Cate and Dempsey published their research on national practices and laws regarding systematic government access to personal information held by private-sector companies. The volume included for the first time the

> special insight … that the principles and practices of accountability that have been developed around corporate handling of personal information collected in commercial contexts are directly applicable to data governance within police and intelligence agencies and are especially relevant when those agencies demand disclosure of data held by the private sector'.[115]

5. The Essential Elements of Interoperability from an Accountability Perspective

From an accountability perspective, there are three basic elements for greater interoperability at international level with regard to government access to personal information: (i) trust and transparency; (ii) legality and proportionality; and (iii) independent oversight, both internal, external, administrative and judicial.[116] In the following, we examine the DPF under these rubrics.

5.1 Trust and Transparency

With accountability comes trust. The GPA has pointed out that 'strong data protections and privacy safeguards are vital for the preservation of public trust, the promotion of market

110. See eg Information Accountability Foundation (IAF), 'The Essential Elements of Accountability' (January 2019) <https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2020/04/Data-Stewardship-Elements-002-1.pdf>; CIPL, 'What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework' (May 2020) <www.information-policycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_report__27_may_2020_.pdf>. The original elements for accountability were set out by the Galway Project in 'Data Protection Accountability: The Essential Elements, A Document for Discussion' (October 2009) <www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00059/544506-00059.pdf>.

111. For example, the use of websites in Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, judgment of 19 October 2016 (ECLI:EU:C:2016:779).

112. See Kuner (n 31) 81 ('EU bodies have failed to adopt a consistent view of the principles underlying the cross-border protection of personal data, such as accountability').

113. EDPS, Opinion 3/2019 regarding the participation in negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention (2 April 2019) 3 ('Data protection principles … are as relevant for public bodies as they are for private companies. These basic principles are all the more important considering the sensitivity of the data required for criminal investigations').

114. FRA (n 51) 9 ('In a field dominated by secrecy … oversight is crucial: it helps ensure that intelligence services are held accountable for their actions'); UN Compilation (n 91) Practice 6, para 13 ('An effective system of oversight is particularly important in the field of intelligence because these services conduct much of their work in secret and hence cannot be easily overseen by the public').

115. Dempsey, Cate and Abrams, 'Organizational Accountability, Government Use of Private-Sector Data, National Security, and Individual Privacy' in *Bulk Collection* (n 6) 321.

116. The principles of legality, proportionality and accountability are discussed in Recommendations for Government and Industry in *Bulk Collection* (n 6) 426 et seq.

interoperability and the support for international sharing of personal data and cross-border data flow'.[117] The Roundtable of the data protection and privacy authorities of the G7 member countries (G7 DPAs Roundtable) has recently 'emphasize(d) that trust is a vital component to the flow of data on a global scale'.[118]

Normally, trust refers to the confidence of a data subject that a particular organisation to which they provide data about themselves will process that data lawfully and fairly. For most individuals, whose knowledge and time is limited, trust is assumed, and it has fallen to data protection authorities and, increasingly, NGOs to ensure that controllers are responsible for their processing of personal information.

Accountability mechanisms enabling trust in international transfers include SCCs[119] and BCRs. With regard to BCRs, Article 47(2)(e) GDPR refers to the specific safeguards of the right to complain to a DPA and to obtain judicial redress.

With regard to SCCs, the CJEU has spelled out in *Schrems II* the specific implications of accountability for controllers wishing to use this mechanism to transfer personal data outside the EU:

> It is therefore, above all, for that controller or processor to verify, on a case-by-case basis … whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.[120]

Following the ruling in *Schrems II*, the EDPB's STT Recommendations specifically applied the principle of accountability to international data transfers:

> The right to data protection has an active nature. It requires exporters and importers (whether they are controllers and/or processors) to go beyond an acknowledgement or passive compliance with this right. Controllers and processors must seek to comply with the right to data protection in an active and continuous manner by implementing legal, technical and organisational measures that ensure its effectiveness. Controllers and processors must also be able to demonstrate these efforts to data subjects, the general public and data protection supervisory authorities.

This accountability requirement, to be able to demonstrate compliance, enables verification.[121] Since the individuals subject to government surveillance cannot carry out verification themselves, the EDPB has stressed the 'importance of comprehensive supervision by independent supervisory authorities … in circumstances where, due to the nature of secret

117. Global Privacy Assembly (GPA), Resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes (25 October 2021).
118. G7 Data Protection and Privacy Authorities' Action Plan 2023, relating to Data Free Flow with Trust (DFFT).
119. See Not-So-Standard Clauses: Examining Three Regional Contractual Frameworks for International Data Transfers, Future of Privacy Forum (30 March 2023), available at <https://fpf.org/wp-content/uploads/2023/03/FPF-SCC-Not-So-Standard-Clauses-Report-FINAL-single-pages-1.pdf>.
120. *Schrems II* (n 25) para 134; see also para 142.
121. In a very different context, President Reagan reportedly made the rhyming Russian proverb 'Доверяй, но проверяй' ('Doveryay, no proveryay'; 'trust, but verify') a key part of the negotiations on the Intermediate-Range Nuclear Forces (INF) Treaty.

surveillance, the individual is prevented from seeking review or from taking a direct part in any review proceedings'.[122]

In 2015, the Venice Commission reported on bulk collection and stressed the importance of oversight, in particular a general complaints procedure to an independent, external body, especially in the absence of other safeguards such as prior judicial authorisation[123] or notification of data subjects.[124]

In addition, trust requires transparency, although this cannot be the same for national security as it is for civil matters.[125] The EU Fundamental Rights Agency (FRA) has pointed out that, in view of the secret nature of intelligence techniques and operations, 'it is beyond dispute that full transparency of oversight is neither possible nor desirable'.[126] Equally, however, the GPA has stressed that

> transparency, including both information to the public and the provision of information to individually affected data subjects, subject to necessary and proportionate limitations, is an essential element of both government accountability and citizens' ability to exercise their rights in a democratic society.[127]

To provide the necessary confidence in how personal information is acquired, and in the purposes for which it is used and retained, the rules governing access and use of personal information must be published. This is not to say that the specific operations carried out must be public, but rather the general legal framework governing surveillance activities.[128] Moreover, experience has shown, notably following the Snowden revelations,[129] that a complete absence of transparency by intelligence agencies can lead to a 'deep well of distrust',[130] which can have significant political and legal consequences.

Moreover, transparency is a key distinguisher between democratic and authoritarian jurisdictions. In principle, an accountability analysis would require controllers to follow a more demanding approach to safeguard measures for transfers to jurisdictions which are

122. EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (28 February 2023) para 164. The EU General Court has accepted that there is no obligation on Europol to give individuals the opportunity to be heard before their personal data is included in a report, because such an obligation could undermine the practical effect of the Europol Regulation and the actions of given police authorities and law enforcement agencies: Case T-436/21, *Veen v Europol*, judgment of 27 April 2022 (ECLI:EU:T:2022:261) paras 43-44 and 48 (on appeal to the CJEU in Case C-444/22 P).
123. The absence of 'independent prior authorisation' for bulk collection under the DPF has been criticised by the European Parliament (EP): Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-U.S. Data Privacy Framework (2023/2501(RSP)) paras 3 and 4.
124. European Commission for Democracy through Law, Report on the Democratic Oversight of Signals Intelligence Agencies (15 December 2015).
125. See also Koppell (n 67) 96 (noting the 'literal value of accountability, the idea that an accountable bureaucrat and organization must explain or account for its actions').
126. FRA (n 51) 87.
127. GPA Resolution (n 117) 2-3. See also WP29 (n 88) 14 ('Transparency is an integral element of many accountability measures').
128. *Zakharov* (n 50) § 229. See also Lorna Woods, 'Zakharov v. Russia (Eur. Ct. H.R.)' (2016) 55(2) *International Legal Materials* 207-208. In the US, see the compilation of legal materials in ODNI Office of General Counsel, *Intelligence Community Legal Reference Book* (Winter 2020).
129. Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (Vintage Books 2014); Timothy H Edgar, *Beyond Snowden: Privacy, Mass Surveillance and the Struggle to Reform the NSA* (Brookings Institution Press 2017).
130. Privacy & Civil Liberties Oversight Board (PCLOB), Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (23 January 2014) 15.

unable to demonstrate compliance with the accountability principles. A study by the University of Leuven on government access to data in third countries commissioned by the EDPB has underlined the problem of permitting data exports to China and Russia, and illustrated the difficulties of recognising an adequate level of protection in India,[131] where a relatively comprehensive data protection law was finally adopted in August 2023 following the 2017 seminal ruling by the Indian Supreme Court in the famous Puttuswamy case.[132]

Transparency is also required to prevent mission creep. The most egregious examples include the self-authorised use by local authorities in the UK of 'surveillance powers in circumstances that seemed disproportionate' to investigate whether families actually lived in the catchment area (jurisdiction) of schools to which their children were applying and whether dog walkers were permitting their dogs to foul the streets[133].

5.1.1 Trust and Oversight Using a Standard Response to a Complaint

The DPF provides that neither the CLPO nor the DPRC may reveal whether a complainant was subject to US signals intelligence activities. Instead, complainants are notified that the review either did not identify any covered violations or yielded a determination requiring appropriate remediation.

This approach in the DPF has been criticised by the European Parliament on the basis that 'a person bringing a case would have no chance of being informed about the substantive outcome of the case'.[134] However, the EDPB does not oppose it per se, though it is concerned that there is no provision for any exemptions to the standard response, such as 'the disclosure of a summary outlining the information's content or that of the evidence in question'.[135] In view of its concerns on this specific aspect, the EDPB relies in effect on 'assessment on this aspect by the PCLOB in future reviews of such decisions'. This reliance on the PCLOB, a trusted independent authority, shows that the use of a standard response can only work acceptably if it is based on trust. This limited form of reporting is 'widely used in Europe, including by the CNCTR' (Commission nationale de contrôle des techniques de renseignement) in France.[136] Under EU law, it is accepted when it is entrusted to an independent supervisory authority,[137] as in the case of Article 17 LED and Article 25(7) of the Regulation governing data processing by EU institutions.[138] So it is unlikely that the use of a standard

131. EDPB, Legal study on Government access to data in third countries, Final Report (8 November 2021), EDPS/2019/02-13.
132. *Justice K S Puttuswamy (Retd) and Anr vs Union Of India And Ors*, judgment of 24 August 2017 (Supreme Court), Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161.
133. 'A Question of Trust', Report of the Investigatory Powers Review by David Anderson QC (June 2015), para 9.77 and fn 51.
134. EP Resolution (n 123), para 8.
135. EDPB Opinion (n 122), paras 239-240.
136. Theodore Christakis, Kenneth Propp and Peter Swire, 'The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC', *The Privacy Advisor* (11 October 2022) <https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc>.
137. Christopher Docksey, 'Schrems II and individual redress – Where there's a will, there's a way', *Lawfare* (12 October 2020) <www.lawfareblog.com/schrems-ii-and-individual-redress-where-theres-will-theres-way>.
138. EUDPR (n 37). This is drafted in the same terms as Article 20(4) of its predecessor, Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8/1 (repealed).

response would in itself cause a problem for the European courts. The more challenging issue is whether the review process in which it is incorporated is trusted.[139]

5.2 Legality and Proportionality

The principle of proportionality is a general principle of EU law referenced in Article 52(1) EUCFR, which requires, inter alia, that any limitations to its fundamental rights and freedoms are subject to the principle of proportionality. This principle is also referenced in numerous provisions of the GDPR,[140] in particular, the data minimisation principle in Article 5(1)(c).[141] Proportionality is the final part of the following three-step analysis under Article 52 EUCFR.

First, the conduct must be authorised by law, in an express legal basis for government interference with privacy. In this respect, the various elements of the DPF have been laid down, not by Congress,[142] but by a binding presidential order, EO 14086, together with implementing regulations adopted by the Department of Justice. However, neither EU law nor the ECtHR case law upon which it builds necessarily require that legislation be adopted, so long as the 'legal situation is sufficiently precise and clear to enable the persons concerned to know the full extent of their rights and, where appropriate, to be able to rely on them before the national courts'.[143]

There is then an assessment of necessity: whether it is strictly necessary to take the action proposed.[144]

And finally, proportionality must be considered, whether the action proposed is the least intrusive way of achieving the necessary objective.[145]

The CJEU applied these principles in *La Quadrature du Net*. As pointed out earlier, the Court found that, where there is a 'genuine and present or foreseeable' 'serious threat' to national security, an order for general and indiscriminate data retention can be made, so long as it is the exception and not the rule, and is subject to effective and binding review by a court or independent body.[146]

---

139. For example, in *Centrum för rättvisa* (n 47), the ECtHR found that the system overall could be trusted despite the failure, in practice, to notify the persons concerned that they have been surveilled: §173. It concluded: 'In these circumstances, there is no reason to doubt that Swedish law and practice secure an effective supervision on signal intelligence activities in Sweden': § 353.
140. Eg, Articles 5(1)(b) and 5(1)(b), 6(1)(f), 23, 35, 83, 84, and 90 GDPR. See also Dariusz Kloza and Laura Drechsler, 'Proportionality Has Come to the GDPR' *European Law Blog* (9 December 2020) <https://europeanlawblog.eu/2020/12/09/proportionality-has-come-to-the-gdpr>.
141. Case C-708/18, *TK v Asociația de Proprietari bloc M5A Scara-A*, judgment of 11 December 2019 (ECLI:EU:C:2019) paras 48-49; Case C-268/21, *Norra Stockholm Bygg v Lycander*, judgment of 2 March 2023 (ECLI:EU:C:2023:145) para 54.
142. The European Parliament has criticised the absence of Congressional legislation and the ability of the President to amend or withdraw the Executive Order at any time: see EP Resolution (n 123) para 12. However, it is argued that in the national security area 'executive orders and presidential directives are built to last': Alex Joel, 'Protect Privacy. That's an Order' *Lawfare* (6 April 2021) <https://www.lawfaremedia.org/article/protect-privacy-thats-order>.
143. Case 29/84, *Commission v Germany*, judgment of 23 May 1985 (ECLI:EU:C:1985:229) para 23. See also Theodore Christakis, Kenneth Propp and Peter Swire, 'EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an "Essentially Equivalent" Solution', *European Law Blog* (31 January 2022) Part C <https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution>.
144. See EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit (11 April 2017) pt 4.
145. See EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19 December 2019).
146. *La Quadrature du Net* (n 46) paras 136-139.

In its Adequacy Decision, the Commission takes the view that the US approach to bulk collection of signals intelligence in the Executive Order responds to these requirements. First, 'collection of data within the United States … must always be targeted'. The Commission points out that this type of data collection is the 'most relevant' because it concerns data that has been transferred to organisations in the US.

Second, 'bulk collection' may apply to data collection that takes place outside the US, but 'targeted collection must be prioritised' and bulk collection is only allowed where the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection,[147] and only to the extent and in a manner that is proportionate to the validated intelligence priority'.[148]

The European Parliament acknowledged that the inclusion of the principles of necessity and proportionality in EO 14086 constituted a 'significant step forward,' though it was not persuaded that the US would be using the same substantive definitions of these principles.[149] However, the EDPB recalled that the CJEU has not *excluded* the principle of bulk collection for international transfers.[150] It welcomed the fact that that 'the EO provides that targeted collection should be prioritised over bulk collection,' and concluded that '[i]n principle these provisions constitute a guarantee to ensure the necessity of the collection of data'.[151]

5.3 Independent Oversight

The need for appropriate, effective and independent oversight of the intelligence services[152] tends to be accepted by all stakeholders, but they differ as to what must necessarily constitute such oversight.[153] From an accountability perspective there are three distinct levels of oversight.[154] First, as noted above, a *sine qua non* of accountability is internal oversight and expertise. Second, because modern accountability is a *legal standard*, it has to be under-

147. Adequacy Decision (n 63) recital 141.
148. ibid recital 131; see also recital 133.
149. EP Resolution (n 123) recital J and para 2. For the CJEU approach, see Lorenzo Dalla Corte, 'On proportionality in the data protection jurisprudence of the CJEU' (2022) 12(4) *International Data Privacy Law* 259 <https://doi.org/10.1093/idpl/ipac014>. For the US, see generally Vicki S Jackson, 'Constitutional Law in an Age of Proportionality' (2015) 124(8) *Yale Law Journal*, 3094. Jackson criticises the 'relative absence of proportionality from U.S. constitutional law': ibid 3121. However, she notes the use of 'structured' proportionality in 'some areas of U.S. constitutional law': ibid 3096-3097. Moreover, she argues in favour of 'greater use of proportionality, as a principle and as a structured form of review': ibid 3194. For a specific assessment of necessity and proportionality in the national security area, see Alex Joel, 'Necessity, Proportionality, and Executive Order 14086' (2023) *Joint PIJIP/TLS Research Paper Series*, no 99, 12-18 and 24-26 <https://digitalcommons.wcl.american.edu/research/99>.
150. EDPB Opinion 5/2023 (n 122), paras 133 and 134
151. ibid para 130.
152. WP29 Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes (WP215, 10 April 2014) 13.
153. A broad definition of the term 'oversight' includes 'the various ways of holding government agencies accountable before the public and the government: internal oversight by the responsible minister, parliamentary oversight, judicial oversight, and external independent oversight': Nico Van Eijk, 'Standards for Independent Oversight' in *Bulk Collection* (n 6) 383. See also the seven standards for independent oversight of intelligence services: ibid 388-392.
154. The literature, reports and decisions refer to two more accountability elements, internal control and parliamentary supervision. Internal control consists of control within the services and by the executive, as opposed to internal oversight by the DPO or CPO: see FRA (n 51) 59. Parliamentary supervision is part of parliamentary oversight of the executive, and forms a significant part of the oversight structure in several jurisdictions. Within the EU, see the five models of oversight in FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Update 2023* (24 May 2023) 20-23 <https://doi.org/10.2811/382910> and, more globally, see the country reports in *Bulk Collection* (n 6). Congressional oversight in the US is described in the Adequacy Decision (n 63) recitals 168-170, and is emphasised by Joel (n 149) 29-30.

pinned by external oversight, which is quite different to internal oversight.[155] External oversight consists of independent, legally binding administrative supervision. Third, there must be the possibility to seek redress before a court or comparable body. In the same way, the main international texts addressing government access to personal data separately address the requirements for independent oversight and legal redress.[156]

5.3.1 Internal Oversight – the DPO /CPO

As noted above, the role of the internal privacy adviser, the DPO or Privacy Officer, is central to the principle of accountability. Like accountability itself, this core function can be found in many different systems[157] and is widespread worldwide.[158] The internal privacy expert or team is embedded within the organisation of the data controller and must be directly responsible to top management so as to be able to effectively advise and guide, particularly with regard to privacy by design and data minimisation when designing new systems or retrofitting existing ones.

In the EU, the DPO plays a crucial role in ensuring compliance with the fundamental right to data protection, and has been described as the cornerstone of the principle of accountability.[159] Under Articles 37-39 GDPR, DPOs have the right and duty to act independently in carrying out their role,[160] but are normally part of the organisation of the data controller[161] and thus may fulfil other tasks and duties, so long as these do not result in a conflict of interests.[162] Because of their 'essential role', the EDPB decided that its 2023 coordinated enforcement action should address the designation and position of DPOs.[163] In the context of national intelligence, the FRA has characterised internal control, including a reference to the work of the DPO of the Federal Intelligence Service (BND), as 'imperative.'[164]

In the US federal administration, the EDPB has pointed out that '(a)ll intelligence community elements have oversight and compliance officials, which conduct periodic oversight of signals intelligence activities, including Privacy and Civil Liberties Officers and Inspectors General'.[165] The privacy and civil liberties officers (PCLOs) are sometimes combined

155. The first CPO of the Department of Homeland Security stressed that she was 'part of the leadership team--to inform decisions, to advise and counsel, to debate and argue when necessary, but to be perceived as an ally, an element, not only as an outsider, or a watchdog'. See Privacy Office, First Annual Report to Congress (April 2003-June 2004) Appendix D 7-8.
156. See Points 6 and 8 of the GPA Resolution (n 117); Principles VI and VII of the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, OECD/LEGAL/0487 (14 December 2022); and Guarantees C and D of the EDPB Essential Guarantees (n 58).
157. For example, Question 40 under the Accountability rubric of the Intake Questionnaire, which a company applying for CBPR certification must provide, asks whether an individual(s) has been appointed to be responsible for overall compliance with the APEC Privacy Principles.
158. IAPP, Data Protection Officer Requirements by Country: <https://iapp.org/media/pdf/resource_center/dpo_requirements_by_country.pdf>.
159. WP29 Guidelines on Data Protection Officers ('DPOs') (WP243 rev.01, 5 April 2017).
160. Article 38(3) and Recital 97 GDPR. See Case C-534/20, *Leistritz AG v LH*, judgment of 22 June 2022 (ECLI:EU:C:2022:495) paras 26-28.
161. Although Article 37 GDPR does provide for the possibility of using a shared DPO or an external contractor to act as DPO.
162. Article 38(6) GDPR. See Case C-453/21, *X-FAB Dresden v FC*, judgment of 9 February 2023 (ECLI:EU:C:2023:79).
163. See <https://edpb.europa.eu/news/news/2023/launch-coordinated-enforcement-role-data-protection-officers_en>.
164. FRA Volume II 2017 (n 51) 59. See also the earlier discussion of internal controls in various EU Member State intelligence agencies in Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Volume I: Member States' Legal Frameworks (Luxembourg, Publications Office 2015) 30-31.
165. EDPB Opinion 5/2023 (n 122), para 183. See also Adequacy Decision (n 63) recitals 107-110.

with, sometimes complemented by, a Chief Privacy Officer (CPO). These are senior officers with statutory responsibility for investigating and addressing complaints about violations of privacy and civil liberties. Taken as a whole, they constitute a 'complex and comprehensive' system for the protection of personal information within the US intelligence and law enforcement communities.[166]

In addition to these officials in the various intelligence and law enforcement agencies, the DPF relies for the handling of complaints concerning EU personal data on the Civil Liberties Protection Officer (CLPO) based in the Office of the Director of National Intelligence (ODNI). The ODNI is a legally separate organisation from the other agencies, and reports directly to the President. The CLPO coordinates, advises and supervises the various US intelligence agencies and their Strategic Goals include, inter alia, ensuring that complaints indicating possible abuses of civil liberties and privacy are reviewed, assessed, investigated, responded to, and resolved.

The DPF positions the CLPO as the first part of a 'two layered' approach to providing an effective external judicial-style remedy.[167] The CLPO is charged with first hearing complaints and making administrative decisions thereon. The decisions of the CLPO can then be appealed to a new second layer, the Data Protection Review Court ('DPRC').

From one point of view the CLPO 'will function analogously to a data protection officer for the U.S. intelligence community,'[168] and indeed this was the case at the time of the Privacy Shield, when the CLPO was merely one of a number of '(m)ultiple oversight layers … in place' which did 'not meet the required level of independence.'[169] The question arises, however, whether the CLPO's heightened oversight role under the DPF is now closer to that of an independent regulator (DPA) rather than a DPO. From an accountability perspective, the CLPO is clearly a key element of oversight, and something of a hybrid between an internal DPO or privacy officer and an independent supervisory body, as discussed below.

5.3.2 Administrative Oversight and Independent Supervision

Independent supervision in one form or another is common across the globe: the DPAs in the EU/EEA, the Federal Trade Commission in the U.S., and the Privacy Enforcement Authorities at the core of the APEC Cross-Border Privacy Rules (CBPR) System[170] and the Global CBPR Forum.[171]

However, in some jurisdictions the regulator may be effective at encouraging accountability and at enforcement, but nonetheless functions as a part of the executive. For example, the regulator in Singapore is 'an active and apparently impartial regulator', but is also

166. Alex Joel, Protecting Privacy and Promoting Transparency in a Time of Change: My Perspective after 14 Years as Civil Liberties Protection Officer <https://privacyacrossborders.org/wp-content/uploads/2023/02/Protecting-Privacy-and-Promoting-Transparency-in-a-Time-of-Change.pdf>.
167. EDPB Opinion (n 122), para 215.
168. Christakis, Propp and Swire (n 136).
169. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, [2016] OJ L 2017/1, recitals 95-96.
170. APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines (November 2019), para 42. See the 26 PE Authorities in the 11 economies participating in the Cross-border Privacy Enforcement Arrangement (CPEA) listed at: http://<www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>.
171. In the same way as under APEC CBPR, the criteria for Membership of the Global Forum require that applicants should have 'at least one Privacy Enforcement Authority as a participant in the Global Cooperation Arrangement for Privacy Enforcement ('Global CAPE')', Global CBPR Forum Terms of Reference (2023), Annex A, para 3(b).

part of government and thus a 'non-independent regulator.'[172] Of note is that Singapore is a signatory with the EU of the Joint Declaration on Privacy and the Protection of Personal Data of 23 February 2022, which includes the core elements of 'independent oversight by a dedicated supervisory authority and effective redress'.[173]

In the regulatory framework of the Council of Europe, the element of independent supervision was not present in Convention 108, but was added in Additional Protocol No 181 of 2001. Independent supervision has now been consolidated into Article 15 of Convention 108+[174] and applies equally to processing for national security and defence purposes.[175]

In the US, the Federal Trade Commission (FTC) is an independent data protection regulator, and is a member of the Global Privacy Assembly of independent privacy and data protection commissioners. For most commercial sectors, the FTC ensures the role of independent oversight, and that role is an essential guarantee for the commercial aspects of the DPF carried over from the Privacy Shield. However, like many national DPAs in EU Member States, the FTC has no jurisdiction over state surveillance.

In the UK, there is a widely recognised DPA, the Information Commissioner (ICO),[176] together with an independent supervisory authority for intelligence oversight, the Investigatory Powers Commissioner (IPC),[177] who is supported by two Offices, the IPCO and the OCDA.[178] In addition, a team of Judicial Commissioners is responsible for prior authorisations of the most intrusive investigatory powers, as part of a 'double lock' safeguard procedure.[179] The Investigatory Powers Commissioner and the Judicial Commissioners must be serving or retired members of the senior judiciary.[180]

In the EU, DPAs implement the principle of independent supervision under both primary and secondary law, namely Article 8(3) of the Charter, Article 16(2) of the Treaty on the Functioning of the European Union (TFEU), and Article 52 GDPR.[181] The CJEU regards the requirement of independent supervision as an 'essential component' of the right to pro-

172. Graham Greenleaf, 'How far can Convention 108+ "globalise"? Prospects for Asian accessions' (2021) 40 *Computer Law & Security Review* 7 <https://doi.org/10.1016/j.clsr.2020.105414>. See also Docksey, 'Update' (n 68) 112-113.

173. In addition, Singapore and the EU have agreed to 'strengthening data free flow with trust' under the EU-Singapore Digital Partnership 2023, pt 26, by means of model data protection contracts, emerging technologies and privacy enhancing technologies.

174. The importance of independent supervision for transborder data flows has been underlined by the Council of Europe, which cites the case where a supervisory authority is no longer able to effectively exercise its functions as an example of a 'real and serious risk' which could 'significantly undermine' the protections afforded to personal data under Convention 108+. See Council of Europe, 'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data' (10 October 2018),para106<https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>.

175. See Article 11 (Exceptions and restrictions) para 3, second indent.

176. In the intelligence area, the ICO is responsible under section 244 of the Investigatory Powers Act for oversight of the integrity, security or destruction of communications data retained under Part 4 thereof.

177. The ICO and the IPC entered into a Memorandum of Understanding in December 2020 on mutual cooperation, the sharing of information and the conduct of joint audits, where appropriate: <https://ico.org.uk/media/about-the-ico/mou/2619387/ipco-ico-mou.pdf>.

178. See <www.ipco.org.uk>.

179. Report on the Operation of the Investigatory Powers Act 2016, Home Office, February 2023, at 8 <www.gov.uk/government/publications/report-on-the-operation-of-the-investigatory-powers-act-2016/home-office-report-on-the-operation-of-the-investigatory-powers-act-2016-accessible-version>.

180. See Investigatory Powers Act 2016, Part 8, Oversight Arrangements.

181. See generally Hielke Hijmans, The European Union as Guardian of Internet Privacy, The Story of Article 16 TFEU (Springer 2016) ch 7.

tection of personal data under primary EU law,[182] and has laid down a body of case law in three infringement cases and two cases relating to international transfers.[183]

In the infringement cases, the CJEU has ruled that DPAs must be free from any external influence, direct or indirect,[184] and from all suspicion of partiality, whether due to the integration of the authority within the executive,[185] or to the threat of legislation prematurely terminating the term in office of the Commissioner[186]—ie acting as a 'sword of Damocles'.[187]

This insistence on data protection authorities' complete independence has been criticised as excessive,[188] although it is fair to say that the right result was achieved on the specific facts of the three infringement cases assessing Member States' DPAs. Further, the CJEU has stressed in that context that independence is not a *right* of data protection authorities but rather a means to strengthen the protection of individuals.[189]

Advocate General Kokott has argued that control by an independent authority is one aspect of the right to data protection where a limitation should be very difficult to justify. For example, there might be a *different* authority for sensitive processing, such as law enforcement and terrorism,[190] but it would be unacceptable to have *no* authority *whatsoever*.[191]

With regard to international transfers and independent supervision, the CJEU has handed down two specific rulings. The first ruling applied the rights to privacy and data protection in the Charter to strike down the EU Data Retention Directive.[192] Although the case was purely internal in scope, the CJEU referred *obiter* to the problem that the directive did not require personal data to be retained within the EU, and hence under the supervision of a DPA, as 'explicitly required by Article 8(3) of the Charter'.[193] The second ruling was the negative Opinion of July 2017 on the draft EU-Canada PNR Agreement. Whilst independent supervision is generally ensured by the Privacy Commissioner of Canada, its remit did

182. Only for data protection supervisory authorities, in view of their status under EU primary law: compare Case C-424/15, Garai and Almendros v Administración del Estado, judgment of 19 October 2016 (ECLI:EU:C:2016:780).
183. See Herke Kranenborg, 'Article 8' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), The EU Charter of Fundamental Rights, A Commentary (Hart Publishing 2014) 277-279.
184. Case C-518/07, *Commission v Germany*, judgment of 9 March 2010 (Grand Chamber) (ECLI:EU:C:2010:125). See the criticism of 'agencies fully integrated into government' in Spiros Simitis, 'Reviewing Privacy in an Information Society' (1987) 3 *University of Pennsylvania Law Review* 135, 707, 744 <https://scholarship.law.upenn.edu/penn_law_review/vol135/iss3/3>.
185. Case C-614/10, *Commission v Austria*, judgment of 16 October 2012 (Grand Chamber) (ECLI:EU:C:2012:631).
186. Case C-288/12, *Commission v Hungary*, judgment of 8 April 2014 (Grand Chamber) (ECLI:EU:C:2014:237). This ruling forms the foundation of the EDPS' legal challenge to the EU legislator's overruling of his decisions to curb excessive data retention by Europol, in Case T-578/22, *EDPS v Parliament and Council* (n 98).
187. Case C-288/12, *Commission v Hungary*, Opinion of AG Wathelet of 10 December 2013 (ECLI:EU:C:2013:816) para 83.
188. Alexander Balthasar, 'Complete Independence' of National Data Protection Supervisory Authorities' (2013) 9(3) *Utrecht Law Review* 31 <https://doi.org/10.18352/ulr.234>. Cf Bygrave's characterisation of the criterion as 'part of a "paranoia" of European political culture': Lee A Bygrave, 'The "Strasbourg Effect" on Data Protection in Light of the "Brussels Effect": Logic, Mechanics and Prospects' (2021) 40 *Computer Law & Security Review* 1 <http://dx.doi.org/10.2139/ssrn.3617871>.
189. *Commission v Germany* (n 184), para 25.
190. The reports by the FRA show that in 18 EU Member States specific authorities supervise the intelligence community: see *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, Volume I* (Luxembourg, Publications Office 2015); FRA (n 51) and FRA (n 154) 9.
191. Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) *International Data Privacy Law* 226-227 <https://doi.org/10.1093/idpl/ipt017>.
192. See n 41.
193. *Digital Rights Ireland* (n 42) para 68.

not extend to foreign nationals not resident in Canada. To fill the gap, Canada set up an 'impartial' authority within the administration. The CJEU found that the draft agreement did not guarantee in a sufficiently clear and precise manner the oversight of data protection safeguards by an independent authority not subject to external influence.[194] This body of case law suggests that the CJEU will require there to be an 'essentially equivalent' form of independent supervision underpinning any international transfers.[195]

In brief, the independence of a DPA enables trust that its decisions will be objective and that it will not defer to a hierarchy or to external pressure.

In the intelligence area, independent oversight at the various stages of the intelligence cycle is of particular relevance, since such accountability may enable trust where many of the safeguards used in the commercial setting are not feasible.[196] This can be seen in the case law of the ECtHR, which has been flexible on safeguards such as notification[197] in light of the existence of independent oversight, both administrative and judicial.[198]

5.3.3 Independent Oversight by Way of the PCLOB and the CLPO

The documentation for the DPF shows that many of these essential accountability procedures and mechanisms have been developed within the US law enforcement and intelligence communities, as part of what the EDPB has described as a 'multi-layered oversight process'.[199] However, the question arises whether the DPF provides for the essential element of independent supervision required by Article 8(3) of the Charter.

In this respect, the Board has stressed the role of the Privacy and Civil Liberties Oversight Board (PCLOB) in the system. It characterises the PCLOB as an 'independent oversight agency'[200] and 'recognises the comprehensive supervision role of the PCLOB regarding the new redress mechanism and the implementation of the EO 14086'.[201] It concludes that the PCLOB is 'an essential element of the oversight structure'.[202] However, the findings of the PCLOB are not legally binding on the Intelligence Community.

In contrast, the determinations of the ODNI CLPO *are* legally binding, and there are specific protections for the independence of the CLPO: the office holder can only be dismissed for cause; all members of the intelligence community are prohibited from impeding or improperly influencing the ODNI CLPO's reviews, including the Director of National Intelligence, who must not interfere with the review; and the CLPO is required to act impartially when reviewing complaints.[203]

Moreover, the role of the ODNI CLPO is appreciably different to that of Privacy Officers, Privacy and Civil Liberties Officers and Inspectors General. These officials operate within

194. Opinion 1/15 (n 32), para 230.
195. See the discussion below of the EDPB Essential Guarantees (n 58), the GPA Resolution (n 117) and the OECD Declaration (n 156).
196. 'In a field dominated by secrecy, such oversight is crucial: it helps ensure that intelligence services are held accountable for their actions, and encourages the development of effective internal safeguards within the services': see FRA (n 51) Executive Summary 9.
197. *Centrum för rättvisa* (n 47) para 354.
198. 'There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively … or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken': ibid para 251.
199. EDPB Opinion (n 122) para 183.
200. ibid para 174.
201. ibid para 196
202. ibid para 201.
203. ibid paras 171-172.

their respective departments, whereas the CLPO has a general advisory and oversight role across the whole intelligence community. Most importantly, the CLPO handles complaints under the DPF, their determinations are subject to appeal to a court, the DPRC, and their handling of complaints under the DPF, together with the intelligence community's compliance with its determinations, are subject to annual review by the PCLOB.[204]

The EDPB has underlined the unique features of the CLPO role under the DPF with regard to validation of intelligence priorities[205] (save in specific cases of a derogatory procedure),[206] consultation on updated policies together with the Attorney General and the PCLOB,[207] and reporting violations to an Assistant Attorney General and thence to the Foreign Intelligence Surveillance Court (FISC).[208] Nonetheless, the CLPO remains situated within the executive branch and under the authority of the Director of National Intelligence.[209] As a result, the EDPB concluded that the CLPO is 'not vested with a sufficient degree of independence from the executive'.[210]

However, its analysis fails to take two issues into account. First, the Board found that the CLPO does not satisfy the requirements of EUCFR Article 47, that is, it is not a *tribunal*. Indeed, neither the Board nor the Commission considered whether the CLPO might qualify rather as an independent supervisory authority for the purposes of Article 8(3) EUCFR. Second, the Commission's analysis in the Adequacy Decision refers to two elements of the DPF which are highly relevant to independence. First, neither intelligence agencies nor the Director of National Intelligence, in whose office the CLPO sits, may influence or interfere with the CLPO's review.[211] Second, the CLPO is given heightened protection against dismissal, which may only be for cause.[212]

The absence of these two elements was probative in the EU-Canada PNR case.[213] This ruling confirmed that, where international transfers from the EU are concerned, the test is not absolute equivalence (between the level of protection in the third country and the level present inside the EU) but rather *essential* equivalence. In consequence, the presence of the CLPO in the executive branch is not necessarily unacceptable *per se,* so long as it may carry out its tasks under the DPF with the necessary independence and has binding powers to deal with complaints.

The solution for the CJEU may be to consider the independence of supervision *taken as a whole*. The mix of the CLPO's investigatory role, their special status and freedom to act independently within the executive, and their binding powers, together with the review role of the undoubtedly independent PCLOB, may be argued as having provided an essentially equivalent level of independent supervision.

In this respect, if the latest EU-US transfers regime is challenged before the CJEU, there are a number of factors in its favour. First, the Commission will be able to rely on the generally favourable assessment by the EDPB of the administrative oversight of the intelligence

204. ibid para 196.
205. ibid para 116.
206. ibid para 159.
207. ibid para 121.
208. ibid para 210.
209. *Commission v Austria* (n 185).
210. EDPB Opinion (n 122) para 216.
211. Adequacy Decision (n 63) recital 180.
212. ibid recital 179.
213. Opinion 1/15 (n 32) para 231. Whilst the 'impartial' administrative body in Canada would receive no directions from the other operational bodies of the latter, it continued to be 'under the direction of' the responsible Minister' and 'subject to any direction given by the Minister,' and it had no 'special status' under the legislation: see Opinion of AG Mengozzi of 8 September 2016 (ECLI:EU:C:2016:656) para 315 and fn 118.

community. The Board has cautiously approved the systems of internal oversight, based on privacy and civil liberties officers and Inspectors General,[214] and external oversight, based principally on the role of the PCLOB.[215] Commentators have argued that these mechanisms must be considered within the established multi-layered structure of privacy controls in US intelligence agencies, providing a pragmatic, holistic approach to ensuring the protection of privacy.[216]

Second, there are some indications of flexibility in the case law of the CJEU. First, the Court has slightly modified its approach with regard to national security and mass surveillance in *La Quadrature du Net* to permit bulk collection in situations of clear and present danger. Moreover, the CJEU will be aware of the acceptance by the ECtHR of bulk collection in its *Centrum för rättvisa* and *Big Brother Watch* rulings, due to the presence of a sufficient combination of safeguards, as discussed above.

Third, there are some interesting omissions in both *Schrems* and *Schrems II*, where the CJEU concentrated on the right to privacy under Article 7 EUCFR and the right to an effective judicial remedy under Article 47 EUCFR. It did not find it necessary to rule on Article 8 EUCFR and, in particular, on the alleged violation of the right to independent supervision under paragraph 3 thereof. It also made no comment on the enforcement role of the Department of Transportation under the Safe Harbor and the Privacy Shield, which might otherwise have been equated with the 'impartial' body criticised in its EU-Canada PNR Opinion.

Fourth, the CJEU has taken a pragmatic approach with regard to private-sector surveillance where there is no feasible alternative. In *GC v CNIL*, it implicitly recognised that search engines may lawfully collect even sensitive data, and it is only when that information is produced in response to a search request that the data protection requirements must be respected.[217] In effect, the Court limited its assessment to where there is a concrete outcome of the processing.

As seen above, the combined roles of the CPLO and the PCLOB may well provide an effective and binding form of independent oversight. From an accountability perspective, the CLPO has many of the features of a supervisory body. Like a DPA, and unlike a CPO or PCLO, it has an overarching advisory and supervisory role across the entire regulated community, its determinations are legally binding and subject to appeal to a court, and there are specific protections to preserve its independence. Moreover, its presence within the executive is subject to the independent review role of the PCLOB stressed by the EDPB.[218]

Whilst these elements are convincing, they still do not entirely align with the case law of the CJEU on independent supervision. However, the infringements case law relates entirely to EU Member States, which are within the scope of the Charter, rather than to third countries with their own constitutional traditions. Moreover, in none of the cases dealing with, respectively, transfers, DPAs, the Data Retention Directive and EU-Canada PNR,[219] was a multi-layered system of supervision under consideration, as under the DPF.

---

214. ibid para 193.
215. ibid paras 195 and 201.
216. See Alex Joel, 'A System of Many Layers with Many Players' (13 February 2023) <https://privacyacrossborders.org/2023/02/13/a-system-of-many-layers-with-many-players>. See also Testimony by Professor Peter Swire in Irish High Court Case, Chapter 3, Systemic Safeguards in the US System of Foreign Intelligence Surveillance Law: <www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony>.
217. Case C-136/17, *GC and Others v CNIL*, judgment of 24 September 2019 (ECLI:EU:C:2019:773) paras 46-47 and 69. The lack of a feasible alternative with regard to bulk collection by search engines was predicted by AG Jääskinen in Case C-131/12, *Google Spain v AEPD and Costeja González*, Opinion of 13 May 2014 (ECLI:EU:C:2013:424) para 90.
218. EDPB Opinion (n 122) para 196.
219. The only case that did require an evaluation of the law of a third state.

Consequently, there is a real opportunity for the CJEU to develop an external, accountability-based approach that would maintain the requirement for independent supervision but assess the essential elements of equivalence based on content and outcome. This would recognise the difference between absolute equivalence within the EU and essential equivalence in third countries. Such an approach by the CJEU would also facilitate interoperability with like-minded democracies on the basis of a more internationally accepted vision of this particular norm, for example, under Article 15 of Convention 108+, where the 'test is one of independence, not separateness'.[220] The OECD Declaration accepts both internal compliance offices and independent administrative authorities.[221]

Should, however, independent supervision be a sticking point for the Court, the role of the CLPO is already sufficiently developed that it conceivably could be reinforced further to make it into a supervisory authority that satisfies the independence requirement of Article 8(3) EUCFR. One method, for example, would be to protect the independence of the CLPO in the same way as the independence of the DPRC, described below. Another possibility might be to set up a specific body to hear complaints under the DPF. In such a situation, it would be appropriate for the Court to suspend the temporal effect of its ruling to allow time for such an amendment to be considered and implemented.[222]

5.3.4 Judicial Oversight and the Right to an Effective Judicial Remedy

Article 47 EUCFR frames the right to an effective remedy before a tribunal as an overarching fundamental right applying to the enumerated fundamental rights in the Charter.[223] Like the rights to a fair trial and an effective remedy under Articles 6 and 13 ECHR, the right to an effective remedy under the Charter is a deeply entrenched fundamental right.

The right to an effective remedy can also be found in the GDPR, specifically in recital 104 and Article 45(2) paragraphs (a) and (b). The latter provisions refer not only to 'effective administrative and judicial redress for data subjects' but also to the need for 'effective supervision by an independent regulator'. They underline the fact that administrative and judicial redress must be available separately from independent supervision—neither alone is sufficient to satisfy the standard set by the Charter.

The right to an effective remedy figures in the two *Schrems* rulings on international transfers and in internal CJEU case law on the question of whether a body by nature is a 'court or tribunal'.[224] In *Schrems II*, the Advocate General recalled the criteria laid down by the CJEU to assess whether a body is a court for the purposes of Article 47 of the Charter. The decision hinges on 'whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is *inter partes*, whether it applies rules of law and whether it is independent'.[225] The most important of these criteria is the requirement of independence. This means acting autonomously, without being subject to decisions

220. Greenleaf (n 172) 6.
221. OECD Declaration (n 156) Principle VI, Oversight, second paragraph.
222. See Joined Cases C-191/14, C-192/14, C-295/14, C-389/14 and C-391/14 to C-393/14, *Borealis Polyolefine and Others*, judgment of 28 April 2016 (ECLI:EU:C:2016:311) para 106.
223. See also the Explanations relating to the Charter: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32007X1214%2801%29>.
224. Case C-272/19, *VQ v Land Hessen*, judgment of 9 July 2020 (ECLI:EU:C:2020:535); Case C-746/18, *HK v Prokuratuur*, judgment of 2 March 2021 (Grand Chamber) (ECLI:EU:C:2021:152).
225. Opinion of Advocate General Saugmandsgaard Øe, fn 191, citing Case C-64/16, *Associação Sindical dos Juízes Portugueses*, judgment of 27 February 2018 (Grand Chamber) (ECLI:EU:C:2018:117) para 38 and the case law cited therein.

or pressure by any other body that could impair the independent judgment of its members and to influence their decisions.[226] The CJEU has accepted that an authority which is part of the executive may be regarded as a 'judicial authority' so long as it is 'capable of exercising its responsibilities objectively … without being exposed to the risk that its decision-making power be subject to external directions or instructions, in particular from the executive, such that it is beyond doubt that [its] decision … lies with that authority and not, ultimately, with the executive'.[227]

Article 13 ECHR has the same standard of independence, but its wording differs in one important respect. Article 13 enshrines the right to an 'effective remedy before a national authority' as opposed to a 'tribunal' under Article 47 of the Charter. The case law of the ECtHR confirms that, while it is preferable for a remedy to be available before a court or tribunal, an authority may be sufficient in appropriate cases. It may be a quasi-judicial or administrative body so long as it satisfies the criteria to determine that the remedy is effective—namely that it is independent, that it affords the necessary procedural safeguards to the applicant and that it has the power to hand down a legally binding decision.[228]

The case law of the two jurisdictions suggests that the difference between the Charter and the ECHR may not necessarily be significant for interoperability between the EU and third countries. Thus, in *Schrems II*, the CJEU articulated a more flexible standard for assessing the adequacy of a judicial remedy in a third country. It reiterated the need for 'an independent and impartial court', but then indicated two minimum elements required for an adequacy assessment of effective judicial protection, namely legal guarantees of independence from the executive, and the power to adopt decisions binding the intelligence services.[229]

The DPF provides for a judicial remedy before a special administrative court, the DPRC. It has been argued that the DPRC meets the criterion of independence articulated in the case law of the CJEU and the ECHR, and that its powers and procedures provide the necessary procedural safeguards and binding legal powers.[230] The European Parliament has listed a number of concerns that it feels require further negotiation (standard response, no remedy in damages or access on appeal to the federal courts).[231] In the new situation under the DPF of the handling of an administrative complaint by the DPRC, it has been argued that action by the DPRC may be subject to appeal to the federal courts under the Administrative Procedure Act, which applies broadly to action by federal agencies that is 'arbitrary, capricious,

226. Case C-64/16, *Associação Sindical dos Juízes Portugueses* (n 225) para 44.
227. Case C-509/18, *PF (Prosecutor General of Lithuania)*, judgment of 27 May 2019 (Grand Chamber) (ECLI:EU:C:2019:457) paras 30 and 51, considering the concept of a 'judicial authority' within the meaning of Article 6(1) of Framework Decision 2002/584 (European arrest warrant). Compare Joined Cases C-508/18 and C-82/19 PPU, *OG and PI (Public Prosecutor's offices)*, judgment of 27 May 2019 (Grand Chamber) (ECLI:EU:C:2019:456).
228. Guide on Article 13 of the European Convention on Human Rights, paras 23-29 <www.echr.coe.int/Documents/Guide_Art_13_ENG.pdf>.
229. *Schrems II* (n 25) paras 195-196.
230. Christakis, Propp and Swire (n 136). Korff takes an opposing standpoint: Douwe Korff, 'The inadequacy of the US Executive Order on Enhancing Safeguards For US Signals Intelligence Activities' (11 November 2022) point 4.4, 20, available at: <www.ianbrown.tech/2022/11/11/the-inadequacy-of-the-us-executive-order-on-enhancing-safeguards-for-us-signals-intelligence-activities>.
231. Resolution of 11 May 2023, para 8. See also Korff (n 230) point 4.5, 22.

an abuse of discretion, or otherwise not in accordance with law'.[232] Whilst such appeal is not provided for in the DPF, it is noteworthy that there has been no attempt to exclude it, unlike the unsuccessful statutory attempt to preclude appeals from the Investigatory Powers Tribunal in the UK.[233]

As in the case of independent supervision, this could be the opportunity for the CJEU to distinguish between essential equivalence and absolute equivalence with regard to the standard of individual redress to be applied in the specific case of international transfers. In *Schrems I*, the CJEU ruled that 'legislation not providing for *any possibility* for an individual to pursue legal remedies … does not respect the *essence* of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter' (emphasis added).[234] In this respect, there is a possibility for individuals to pursue a legal remedy before the DPRC, and a possibility for judicial appeals.

The EDPB has analysed the case law of the CJEU and the ECtHR and duly concluded that 'both courts do not base their assessment on purely formalistic criteria, but regard the substantive safeguards as decisive'.[235] Subject to a number of caveats, the Board has cautiously concluded that the DPRC redress mechanism 'is not per se insufficient' to ensure essential equivalence with the requirements of Article 47 EUCFR.[236]

Finally, the divergence between the CJEU and the ECtHR with regard to bulk collection, noted above, illustrates both the higher standard of protection required of EU Member States under the Charter and the essential equivalence of the standard required of non-EU states party to the ECHR. Jurisdictions such as Switzerland and the two Channel Islands are subject to the ECHR and enjoy adequacy decisions that are about to be updated in view of their updated GDPR-standard national legislation. Moreover, within the scope of the GDPR, the three EFTA/EEA nations (Iceland, Liechtenstein and Norway) are subject to the ECHR, not the Charter, in its interpretation and application.[237] In brief, it is possible to interpret and apply the Charter to its highest standard within the EU whilst accepting that the standard developed by the ECtHR is *essentially equivalent* to that of the Charter in third states.

232. Theodore Christakis, Kenneth Propp and Peter Swire, 'EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers', *European Law Blog* (16 February 2022) <https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers>. See also the US White Paper on Information on US Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-US Data Transfers after *Schrems II* (September 2020) 12-13 <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>. The question remains open since the US Supreme Court declined on 21 February 2023 to hear the petition of certiorari in *Wikimedia Foundation, et al v National Security Agency, et al.*
233. The UK Supreme Court narrowly interpreted a legislative provision purporting to oust the appellate jurisdiction of the higher courts ('ouster clause') in *R (on the application of Privacy International) (Appellant) v Investigatory Powers Tribunal and others (Respondents)* [2019] UKSC 22, judgment of 15 May 2019.
234. *Schrems* (n 33) para 95.
235. EDPB Opinion 5/2023 (n 122) para 218.
236. ibid para 220.
237. Joined Cases E-11/19 and E-12/19, *Adpublisher*, judgment of 10 December 2020 (EFTA Court) para 50.

6. The Way Forward Globally on the Basis of Accountability

6.1 Recently Developed Standards and Principles[238]

A number of non-binding international standards have been agreed in principle in the Global Privacy Assembly (GPA) 2021 Resolution on Government Access to Data and the OECD 2022 Declaration on access to personal data for national security and law enforcement purposes. The GPA Resolution represents a consensus of 128 data protection authorities worldwide[239] which have jurisdiction over government data access issues. The OECD Declaration represents the first intergovernmental consensus in this area, developed during exhaustive discussions between, amongst others, privacy and (for the first time) national security representatives, agreed by the thirty-eight OECD member countries and the European Union.

Both instruments set forth similar sets of principles, including legality (legal basis),[240] clear and precise legislation applying to government access,[241] necessity and proportionality,[242] together with the internal[243] and external (effective remedies and redress)[244] elements of the principle of independent oversight, discussed above. In addition, Point V of the GPA Resolution requires there to be data subject rights, and Principle IV of the OECD Declaration requires safeguards on data handling.

These principles are also comparable to the four Essential Guarantees enunciated by the EDPB in its EEG Recommendations—that is, processing should be based on clear, precise and accessible rules, necessity and proportionality with regard to legitimate objectives need to be demonstrated, and there should be independent oversight and effective remedies available to individuals.

Hence, the issue is not how to find the principles, it is how to put them into operation.

6.2 An International Agreement

There have been calls for some time for a legally binding international treaty on data protection, both in general, notably in the 2009 Madrid Resolution,[245] and in particular on government access.[246] An international instrument could set out the necessary standards and procedures and would be legally binding. Alternatively, at European level, senior Council of Europe officials have urged the development of a new international legal standard to provide democratic and effective safeguards for surveillance performed by intelligence services,

238. Bearing in mind that these initiatives follow 'decades' of discussion of 'best practices for intelligence oversight' and that '(a)pplying the broad concept of accountability to intelligence services is not new': Dempsey, Cate and Abrams (n 115).
239. The FTC and the Hong Kong Privacy Commissioner abstained, on the ground that the resolution related to matters outside their respective jurisdictions.
240. GPA Resolution Pt 1 and OECD Declaration Principle I.
241. GPA Resolution Pt 2 and OECD Declaration Principles I Legality and III Approval.
242. GPA Resolution Pt 3, OECD Declaration Principle II, Legitimate Aims.
243. GPA Resolution Pt 6, OECD Declaration Principles VI paras 1 and 2 and VII non-judicial redress.
244. GPA Resolution Pt 8 and OECD Declaration Principle VII.
245. Joint Proposal on International Standards for the Protection of Privacy, International Conference of Data Protection and Privacy Commissioners, 6 November 2009.
246. See eg WP29 (n 152) 15-16; Report of the UN Special Rapporteur on the right to privacy, Joseph A Cannataci (UN Document A/HRC/34/60, 24 February 2017) para 69; Martin Abrams, 'Time for a Global Treaty', *IAF blog* (22 July 2022) <https://informationaccountability.org/2020/07/time-for-a-global-treaty>.

based on the criteria developed by courts such as the European Court of Human Rights and the US Supreme Court.[247]

However, there does not seem to be the political will at global level for such solutions.

6.3 Data Free Flow with Trust (DFFT)

Originally launched as the 'Osaka Track' of the G7, the DFFT policy was fleshed out by the Japanese Presidency of the G7. In 2023, the G7 announced its intention of promoting regulatory cooperation for DFFT, in particular through the discussions of the G7 DPAs' Roundtable. The G7 also committed itself to 'operationalising DFFT through a new institutional arrangement for partnership'—the Institutional Arrangement for Partnership (IAP), to be launched over the course of 2023. The partnership will be based on the pre-existing work of the OECD and the Roundtable, together with other multistakeholder fora.[248]

The discussion above shows how the DPF may represent an acceptable interface between the EU and US systems. In this light, an accountability-based approach might offer a possible way forward, underpinned by the political commitment to DFFT, for a system of internationally agreed principles to which States may voluntarily accede and become bound.

6.4 An International Code of Practice

The GDPR and the APEC CBPR System specifically include accountability mechanisms as tools for transfers. In the GDPR codes of conduct[249] and certification[250] are specifically cited as additional safeguards permitting the transfer of personal data under Article 46(2) paragraphs (e) and (f) GDPR, and Kuner in particular has recommended these mechanisms as a possible solution for international transfers under the GDPR.[251] The G7 Roundtable DPAs have committed to examine certification mechanisms and model contractual clauses to assess interoperability and convergence between different transfer tools.[252]

Accountability mechanisms could similarly inspire possible solutions to the subject of this article, governmental access to personal data, for example through creation of an international Code of Practice. Such a mechanism could operate multilaterally like the CBPR system, but would not necessarily require a legally binding international agreement.[253] It could be a document agreed by experts,[254] stakeholders,[255] or the working groups of an international organisation[256] which simply sets forth the essential accountability principles as applied to the activities of national security authorities. Such a Code could be developed relatively quickly, in view of the extensive work already carried out in the GPA and the OECD.

---

247. Joint statement by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 'Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services' (Strasbourg, 7 September 2020).
248. G7 Digital and Tech Ministerial Declaration of 30 April 2023, paras 9-13 <http://www.g7.utoronto.ca/ict/2023-ministerial_declaration_dtmm.pdf>.
249. EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfers (version 2, 22 February 2022).
250. EDPB Guidelines 07/2022 on certification as a tool for transfers (14 June 2022).
251. Kuner (n 27).
252. Action Plan (n 118) Pillar I, para 6.
253. '(I)nternational cooperation and norm production are moving into other arenas and taking on 'softer', more informal manifestations than those of classical multilateralism': Bygrave (n 188) 17.
254. Eg the Principles and Model Codes published by the American Law Institute: see <www.ali.org/about-ali/how-institute-works>.
255. Eg the Toolkit on Cross-border Access to Electronic Evidence developed by the Internet & Jurisdiction Policy Network, available at <www.internetjurisdiction.net/data/toolkit>.
256. Eg the Model Laws, legal and legislative guides, and recommendations formulated by the United Nations Commission on International Trade Law (UNCITRAL): see <https://uncitral.un.org>.

To take advantage of such a Code, a State would have to have in place, or adopt, the necessary legal framework implementing the agreed principles and accountability-based procedures and safeguards, coupled with a statement committing its agencies to adhere to those principles. Building on the development of the DPF, the EU and the US could conceivably share leadership on the basis of such an approach.[257]

6.5 Caveat from the EU Perspective

In any event, each and every one of these solutions would require assurance that they do not undermine the necessary level of data protection, in view of the 'vast numbers of countries within the UN, with highly heterogeneous legal systems'.[258] In September 2022, the G7 DPAs Roundtable commended to G7 ministers the work of the GPA and the OECD with regard to government access to personal data and recalled that:

> clear and precise rules governing the scope and the conditions under which privately held data might be accessed for national security and public safety purposes need to be laid down by appropriately enacted legislation which ensures that interferences are limited to what is strictly necessary and proportionate in democratic societies.[259]

7. Conclusion

The principle of accountability offers a means of addressing the issue of government access to personal information held by the private sector. It is familiar across the world and it does not 'belong' to any particular jurisdiction. In the EU, it has become one of the central innovations of the GDPR and underlies much of the case law on the GDPR's material scope. The principle offers a common language to the privacy and intelligence communities and a toolkit of mechanisms understood by both.

The groundwork for an operational initiative now exists. The necessary basic principles have been developed at international level, notably by the GPA, the OECD and the EDPB. At the same time, the DPF offers an example of a national, accountability-based 'multi-layered' system for the lawful processing of personal data for national security purposes. As noted by the EDPB, the success of the DPF will depend heavily on the level of commitment of the US intelligence community to its full and effective implementation, as reviewed in due course by the PCLOB.

Taken together, these developments could permit like-minded democracies to develop the level of trust and transparency necessary for greater privacy interoperability in the future. They could be implemented in a number of ways: in an international agreement or a Council of Europe Convention open to third States, in a voluntary but binding system modelled on CBPR, or in a non-binding instrument such as an international code of practice based on the essential principles and guarantees developed by the GPA, the OECD and the EDPB that

257. 'The United States already leads the world in mass surveillance. It can lead the world in mass surveillance reform': Edgar (n 129) quoted in <https://www.brookings.edu/books/beyond-snowden>.

258. EDPS Opinion 9/2022 of 18 May 2022 on the Recommendation for a Council Decision authorising the negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, paras12-15.

259. G7 DPAs Roundtable, Communiqué: Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces (8 September 2022) para 10—affirmed by G7 DPAs Roundtable Action Plan 2023, Pillar I, para 8.

would have to be respected by states subscribing to those principles. In the short term, an accountability-based Code would facilitate the use of SCCs and BCRs for transfers between countries respecting the Code, and facilitate the Commission analysis required for future adequacy decisions.

For any of these initiatives to succeed, they will have to be based on the accountability of the state actors concerned. This means the assumption of responsibility for the processing of personal information by the leaders and members of the intelligence community, the development of the necessary technical and operational measures to ensure respect for the agreed principles, and the ability to demonstrate the resulting compliance, in fact and law.

Acknowledgements

Our thanks are due to Lee A Bygrave, Alex Joel, Christopher Kuner and Peter Swire for providing valuable criticism and input. Nonetheless, the usual disclaimer applies.