



Brussels, 10.7.2023
C(2023) 4745 final

COMMISSION IMPLEMENTING DECISION

of 10.7.2023

**pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
on the adequate level of protection of personal data under the EU-US Data Privacy
Framework**

(Text with EEA relevance)

COMMISSION IMPLEMENTING DECISION

of 10.7.2023

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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)¹, and in particular Article 45(3) thereof,

Whereas:

1. INTRODUCTION

- (1) Regulation (EU) 2016/679² sets out the rules for the transfer of personal data from controllers or processors in the Union to third countries and international organisations to the extent that such transfers fall within its scope of application. The rules on international data transfers are laid down in Chapter V of that Regulation. While the flow of personal data to and from countries outside the European Union is essential for the expansion of cross-border trade and international cooperation, the level of protection afforded to personal data in the Union must not be undermined by transfers to third countries or international organisations³.
- (2) Pursuant to Article 45(3) of Regulation (EU) 2016/679, the Commission may decide, by means of an implementing act, that a third country, a territory or one or more specified sectors within a third country, ensure(s) an adequate level of protection. Under this condition, transfers of personal data to a third country may take place without the need to obtain any further authorisation, as provided for in Article 45(1) and recital 103 of Regulation (EU) 2016/679.
- (3) As specified in Article 45(2) of Regulation (EU) 2016/679, the adoption of an adequacy decision has to be based on a comprehensive analysis of the third country's legal order, covering both the rules applicable to data importers and the limitations and safeguards as regards access to personal data by public authorities. In its assessment, the Commission has to determine whether the third country in question guarantees a level of protection 'essentially equivalent' to that ensured within the Union (recital

¹ OJ L 119, 4.5.2016, p. 1.

² For ease of reference, a list of abbreviations used in this Decision is included in Annex VIII.

³ See recital 101 of Regulation (EU) 2016/679.

104 of Regulation (EU) 2016/679). Whether this is the case is to be assessed against Union legislation, notably Regulation (EU) 2016/679, as well as the case law of the Court of Justice of the European Union (the Court of Justice)⁴.

- (4) As clarified by the Court of Justice in its judgment of 6 October 2015 in Case C-362/14, *Maximilian Schrems v Data Protection Commissioner*⁵ (*Schrems*), this does not require finding an identical level of protection. In particular, the means to which the third country in question has recourse for protecting personal data may differ from the ones employed in the Union, as long as they prove, in practice, effective for ensuring an adequate level of protection⁶. The adequacy standard therefore does not require a point-to-point replication of Union rules. Rather, the test is whether, through the substance of privacy rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection⁷. Furthermore, according to that judgment, when applying this standard, the Commission should notably assess whether the legal framework of the third country in question provides rules intended to limit interferences with the fundamental rights of the persons whose data is transferred from the Union, which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security, and provides effective legal protection against interferences of that kind⁸. The ‘Adequacy Referential’ of the European Data Protection Board, which seeks to further clarify this standard, also provides guidance in this regard⁹.
- (5) The applicable standard with respect to such interference with the fundamental rights to privacy and data protection was further clarified by the Court of Justice in its judgment of 16 July 2020 in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems (Schrems II)*, which invalidated Commission Implementing Decision (EU) 2016/1250¹⁰ on a previous transatlantic data flow framework, the EU-U.S. Privacy Shield (Privacy Shield). The Court of Justice considered that the limitations to the protection of personal data arising from U.S. domestic law on the access and use by U.S. public authorities of data transferred from the Union to the United States for national security purposes were not circumscribed in a way that satisfies requirements that are essentially equivalent to those under Union law, as regards the necessity and proportionality of such interferences with the right to data protection¹¹. The Court of Justice also considered that no cause of action was available before a body which offers the persons whose data was transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter on the right to an effective remedy¹².

⁴ See, most recently, Case C-311/18, *Facebook Ireland and Schrems (Schrems II)* ECLI:EU:C:2020:559.

⁵ Case C-362/14, *Maximilian Schrems v. Data Protection Commissioner (Schrems)*, ECLI:EU:C:2015:650, paragraph 73.

⁶ *Schrems*, paragraph 74.

⁷ See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017)7 of 10.1.2017, section 3.1, pp. 6-7.

⁸ *Schrems*, paragraph 88-89.

⁹ European Data Protection Board, Adequacy Referential, WP 254 rev. 01. available at the following link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

¹⁰ 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 (OJ L 207, 1.8.2016, p. 1).

¹¹ *Schrems II*, paragraph 185.

¹² *Schrems II*, paragraph 197.

- (6) Following the *Schrems II* judgment, the Commission entered into talks with the U.S. government with a view to a possible new adequacy decision that would meet the requirements of Article 45(2) of Regulation (EU) 2016/679 as interpreted by the Court of Justice. As a result of these discussions, the United States on 7 October 2022 adopted Executive Order 14086 ‘Enhancing Safeguards for US Signals Intelligence Activities’ (EO 14086), which is complemented by a Regulation on the Data Protection Review Court issued by the U.S. Attorney General (AG Regulation)¹³. In addition, the framework that applies to commercial entities processing data transferred from the Union under the present Decision – the ‘EU-U.S. Data Privacy Framework’ (EU-U.S. DPF or DPF) – has been updated.
- (7) The Commission has carefully analysed U.S. law and practice, including EO 14086 and the AG Regulation. Based on the findings set out in recitals 9-200, the Commission concludes that the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. DPF from a controller or a processor in the Union¹⁴ to certified organisations in the United States.
- (8) This Decision has the effect that personal data transfers from controllers and processors in the Union¹⁵ to certified organisations in the United States may take place without the need to obtain any further authorisation. It does not affect the direct application of Regulation (EU) 2016/679 to such organisations where the conditions regarding the territorial scope of that Regulation, laid down in its Article 3, are fulfilled.

2. THE EU-U.S. DATA PRIVACY FRAMEWORK

2.1 Personal and material scope

2.1.1 Certified organisations

- (9) The EU-U.S. DPF is based on a system of certification by which U.S. organisations commit to a set of privacy principles - the ‘EU-U.S. Data Privacy Framework Principles’, including the Supplemental Principles (together: the Principles) - issued by the U.S. Department of Commerce (DoC) and contained in Annex I to this Decision¹⁶. To be eligible for certification under the EU-U.S. DPF, an organisation must be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DoT)¹⁷. The Principles

¹³ 28 CFR Part 302.

¹⁴ This Decision has EEA relevance. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Joint Committee Decision incorporating Regulation (EU) 2016/679 into Annex XI of the EEA Agreement was adopted by the EEA Joint Committee on 6 July 2018 and entered into force on 20 July 2018. The Regulation is thus covered by that agreement. For the purposes of the decision, references to the EU and EU Member States should thus be understood as also covering the EEA States.

¹⁵ This Decision does not affect the requirements of Regulation (EU) 2016/679 that apply to the entities (controllers and processors) in the Union transferring the data, for instance on purpose limitation, data minimisation, transparency and data security (see also Article 44 of Regulation (EU) 2016/679).

¹⁶ See in this respect *Schrems*, paragraph 81, in which the Court of Justice confirmed that a system of self-certification can ensure an adequate level of protection.

¹⁷ Annex I, Section I.2. The FTC has broad jurisdiction over commercial activities, with some exceptions, e.g. with respect to banks, airlines, the business of insurance and common carrier activities of telecommunications service providers (although the decision of the U.S. Court of Appeals for the Ninth Circuit of 26 February 2018 in *FTC v. AT&T* has confirmed that the FTC has jurisdiction over non-

apply immediately upon certification. As explained in more detail in recitals 48-52, EU-U.S. DPF organisations are required to re-certify their adherence to the Principles on an annual basis¹⁸.

2.1.2 Definition of personal data and concepts of controller and ‘agent’

- (10) The protection afforded under the EU-U.S. DPF applies to any personal data transferred from the Union to organisations in the U.S. that have certified their adherence to the Principles with the DoC, with the exception of data that is collected for publication, broadcast or other forms of public communication of journalistic material and information in previously published material disseminated from media archives¹⁹. Such information can therefore not be transferred on the basis of the EU-U.S. DPF.
- (11) The Principles define personal data/personal information in the same way as Regulation (EU) 2016/679, i.e. as “data about an identified or identifiable individual that are within the scope of the GDPR received by an organization in the United States from the EU, and recorded in any form”²⁰. Accordingly, they also cover pseudonymised (or “key-coded”) research data (including where the key is not shared with the receiving U.S. organisation)²¹. Similarly, the notion of processing is defined as “any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination and erasure or destruction”²².
- (12) The EU-U.S. DPF applies to organisations in the U.S. that qualify as controllers (i.e. as a person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data)²³ or processors (i.e. agents acting on behalf of a controller)²⁴. U.S. processors must be contractually bound to act only on instructions from the EU controller and assist the latter in responding to individuals exercising their rights under the Principles²⁵. In addition, in the case of sub-processing, a processor must conclude a contract with the sub-processor guaranteeing the same level of protection as provided by the Principles and take steps to ensure its proper implementation²⁶.

2.2 EU-U.S. Data Privacy Framework Principles

2.2.1 Purpose limitation and choice

common carrier activities of such entities). See also Annex IV, footnote 2. The DoT is competent to enforce compliance by airlines and ticket agents (for air transportation), see Annex V, under section A.

¹⁸ Annex I, Section III.6.

¹⁹ Annex I, Section III.2.

²⁰ Annex I, Section I.8.a.

²¹ Annex I, Section III.14.g.

²² Annex I, Section I.8.b.

²³ Annex I, Section I.8.c.

²⁴ See e.g. Annex I, Section II.2.b and Section II.3.b and 7.d, which make clear that agents act on behalf of a controller, subject to the latter’s instructions and under specific contractual obligations.

²⁵ Annex I, Section III.10.a. See also the guidance prepared by the DoC, in consultation with the European Data Protection Board, under the Privacy Shield, which clarified the obligations of US processors receiving personal data from the Union under the framework. As these rules have not changed, this guidance/FAQ remains relevant under the EU-U.S. DPF (<https://www.privacyshield.gov/article?id=Processing-FAQs>).

²⁶ Annex I, Section II.3.b.

- (13) Personal data should be processed lawfully and fairly. It should be collected for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of processing.
- (14) Under the EU-U.S. DPF, this is ensured through different Principles. Firstly, under the *Data Integrity and Purpose Limitation Principle*, similarly as under Article 5(1)(b) of Regulation (EU) 2016/679, an organisation may not process personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorised by the data subject²⁷.
- (15) Secondly, before using personal data for a new (changed) purpose that is materially different but still compatible with the original purpose, or disclosing it to a third party, the organisation must provide data subjects with the opportunity to object (opt-out), in accordance with the *Choice Principle*²⁸, through a clear, conspicuous and readily available mechanism. Importantly, this Principle does not supersede the express prohibition on incompatible processing²⁹.

2.2.2 *Processing of special categories of personal data*

- (16) Specific safeguards should exist where ‘special categories’ of data are processed.
- (17) In accordance with the *Choice Principle*, specific safeguards apply to the processing of ‘sensitive information’, i.e. personal data specifying medical or health conditions,

²⁷ Annex I, Section II.5.a. Compatible purposes may include auditing, fraud prevention, or other purposes consistent with the expectations of a reasonable person given the context of the collection (see Annex I, footnote 6).

²⁸ Annex I, Section II.2.a. This does not apply when an organisation provides personal data to a processor acting on its behalf and under its instructions (Annex I, Section II.2.b). That said, in this case the organisation needs to have a contract in place and ensure compliance with the *Accountability for Onward Transfer Principle*, as described in further detail in recital 43. In addition, the *Choice Principle* (as well as the *Notice Principle*) may be restricted when personal data is processed in the context of due diligence (as part of a potential merger or takeover) or audits, to the extent and for as long as necessary to meet statutory or public interest requirements, or to the extent and for as long as the application of these Principles would prejudice the legitimate interests of the organisation in the specific context of due diligence investigations or audits (Annex I, Section III.4). Supplemental Principle 15 (Annex I, Section III.15.a and b) also foresees an exception to the *Choice Principle* (as well as to the *Notice* and *Accountability for Onward Transfer Principles*) for personal data from publicly available sources (unless the EU data exporter indicates that the information is subject to restrictions that require application of those principles) or personal data collected from records open to consultation by the public in general (as long as it is not combined with non-public record information and any conditions for consultation are respected). Similarly, Supplemental Principle 14 (Annex I, Section III.14.f) provides an exception to the *Choice Principle* (as well as to the *Notice* and *Accountability for Onward Transfer Principles*) for the processing of personal data by a pharmaceutical or medical device company for product safety and efficacy monitoring activities, to the extent that adherence to the Principles interferes with compliance with regulatory requirements.

²⁹ This applies to all data transfers under the EU-U.S. DPF, including where these concern data collected in the context of the employment relationship. While a certified U.S. organisation may therefore in principle use human resources data for different, non-employment-related purposes (e.g. certain marketing communications), it must respect the prohibition on incompatible processing and moreover may do so only in accordance with the *Notice* and *Choice Principles*. Exceptionally, an organisation may use personal data for an additional compatible purpose without providing *Notice* and *Choice*, but only to the extent and for the period necessary to avoid prejudicing the ability of the organisation in making promotions, appointments, or other similar employment decisions (See Annex I, Section III.9.b.(iv)). The prohibition on the U.S. organisation to take any punitive action against the employee for exercising such choice, including any restriction of employment opportunities, will ensure that, despite the relationship of subordination and inherent dependency, the employee will be free from pressure and thus can exercise a genuine free choice. See Annex I, Section III.9.b.(i).

racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, information on the sex life of the individual or any other information received from a third party that is identified and treated by that party as sensitive³⁰. This means that any data that is considered sensitive under Union data protection law (including data on sexual orientation, genetic data and biometric data) will be treated as sensitive under the EU-U.S. DPF by certified organisations.

- (18) As a general rule, organisations must obtain affirmative express consent (i.e. opt-in) from individuals to use sensitive information for purposes other than those for which it was originally collected or subsequently authorised by the individual (through opt-in), or to disclose it to third parties³¹.
- (19) Such consent does not have to be obtained in limited circumstances similar to comparable exceptions provided under Union data protection law, e.g. where the processing of sensitive data is in the vital interest of a person; is necessary for the establishment of legal claims; or is required to provide medical care or diagnosis³².

2.2.3 *Data accuracy, minimisation and security*

- (20) Data should be accurate and, where necessary, kept up to date. It should also be adequate, relevant and not excessive in relation to the purposes for which it is processed, and in principle be kept for no longer than is necessary for the purposes for which the personal data is processed.
- (21) Under the *Data Integrity and Purpose Limitation Principle*³³, personal data must be limited to what is relevant for the purpose of the processing. In addition, organisations must, to the extent necessary for the purposes of the processing, take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current.
- (22) Moreover, personal information may be retained in a form identifying or rendering an individual identifiable (and thus in the form of personal data)³⁴ only for as long as it serves the purpose(s) for which it was initially collected or subsequently authorised by the individual pursuant to the *Choice Principle*. This obligation does not prevent organisations from continuing to process personal information for longer periods, but only for the time and to the extent such processing reasonably serves one of the following specific purposes similar to comparable exceptions provided under Union data protection law: archiving in the public interest, journalism, literature and art, scientific and historical research and statistical analysis³⁵. Where personal data is retained for one of these purposes, its processing is subject to the safeguards provided by the Principles³⁶.
- (23) Personal data should also be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing and against accidental loss,

³⁰ Annex I, Section II,2.c.

³¹ Annex I, Section II.2.c.

³² Annex I, Section III.1.

³³ Annex I, Section II.5.

³⁴ See Annex I, footnote 7, which clarifies that an individual is considered ‘identifiable’ as long as an organisation or third party could reasonably identify that individual, taking into account the means of identification reasonably likely to be used (considering, among other things, the cost and the amount of time required for identification and the available technology at the time of the processing).

³⁵ Annex I, Section II.5.b.

³⁶ *Ibid.*

destruction or damage. To that end, controllers and processors should take appropriate technical or organisational measures to protect personal data from possible threats. These measures should be assessed taking into consideration the state of the art, related costs and the nature, scope, context and purposes of processing, as well as the risks for the rights of individuals.

- (24) Under the EU-U.S. DPF, this is ensured by the *Security Principle*, which requires, similarly to Article 32 Regulation (EU) 2016/679, to take reasonable and appropriate security measures, taking into account the risks involved in the processing and the nature of the data³⁷.

2.2.4 Transparency

- (25) Data subjects should be informed of the main features of the processing of their personal data.
- (26) This is ensured through the *Notice Principle*³⁸, which, similarly to the transparency requirements under Regulation (EU) 2016/679, requires organisations to inform data subjects about, inter alia, (i) the participation of the organisation in the DPF, (ii) the type of data collected, (iii) the purpose of the processing, (iv) the type or identity of third parties to which personal data may be disclosed and the purposes for doing so, (v) their individual rights, (vi) how to contact the organisation and (vii) available redress avenues.
- (27) This notice must be provided in a clear and conspicuous language when individuals are first asked to provide the personal data or as soon as practicable thereafter, but in any event before the data is used for a materially different (but compatible) purpose than the one for which it was collected, or before it is disclosed to a third party³⁹.
- (28) In addition, organisations must make their privacy policies reflecting the Principles public (or, in the case of human resources data, make them readily available to the concerned individuals) and provide links to the DoC's website (with further details on certification, the rights of data subjects and available recourse mechanisms), the Data Privacy Framework List (DPF List) of participating organisations and the website of an appropriate alternative dispute settlement provider⁴⁰.

2.2.5 Individual rights

³⁷ Annex I, Section II.4.a. In addition, as regards human resources data, the EU-U.S. DPF requires employers to accommodate the privacy preferences of employees by restricting access to the personal data, anonymising certain data or assigning codes or pseudonyms (Annex I, Section III.9.b.(iii)).

³⁸ Annex I, Section II.1.

³⁹ Annex I, Section II.1.b. Supplemental Principle 14 (Annex I, Section III.14.b and c) lays down specific provisions for the processing of personal data in the context of health research and clinical trials. In particular, this Principle allows organisations to process clinical trial data even after a person withdraws from the trial, if this was made clear in the notice provided when the individual agreed to participate. Similarly, where an EU-U.S. DPF organisation receives personal data for health research purposes, it may only use it for a new research activity in accordance with the *Notice* and *Choice* principles. In this case, the notice to the individual should in principle provide information about any future specific uses of the data (e.g. related studies). Where it is not possible to include from the outset all future uses of the data (because a new research use could arise from new insights or medical/research developments), an explanation that the data may be used in future unanticipated medical and pharmaceutical research activities must be included. If such further use is not consistent with the general research purposes for which the data was collected (i.e. if the new purposes are materially different, but still compatible with the original purpose, see recitals 14-15), new consent (i.e. opt-in) needs to be obtained. See in addition the specific restrictions/exceptions to the *Notice* Principle described in footnote 28.

⁴⁰ Annex I, Section III.6.d.

- (29) Data subjects should have certain rights which can be enforced against the controller or processor, in particular the right of access to data, the right to object to the processing and the right to have data rectified and erased.
- (30) The *Access Principle*⁴¹ of the EU-U.S. DPF provides individuals with such rights. In particular, data subjects have the right, without the need for justification, to obtain from an organisation confirmation of whether it is processing personal data related to them; have the data communicated to them; and obtain information about the purpose of the processing, the categories of personal data being processed and the (categories of) recipients to whom the data is disclosed⁴². Organisations are required to respond to access requests within a reasonable period of time⁴³. An organisation may set reasonable limits to the number of times within a given period that access requests from a particular individual will be met and may charge a fee that is not excessive, e.g. where requests are manifestly excessive, in particular because of their repetitive character⁴⁴.
- (31) The right of access may only be restricted in exceptional circumstances similar to the ones provided under Union data protection law, in particular where the legitimate rights of others would be violated; where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the circumstances of the case (although expense and burden are not controlling factors in determining whether providing access is reasonable); to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security, public security or defence; the information contains confidential commercial information; or the information is processed solely for research or statistical purposes⁴⁵. Any denial of, or limitation to a right has to be necessary and duly justified, with the organisation bearing the burden of demonstrating that these requirements are fulfilled⁴⁶. In carrying out that assessment, the organisation must take particularly into account the individual's interests⁴⁷. Where it is possible to separate information from other data to which a restriction applies, the organisation must redact the protected information and disclose the remaining information⁴⁸.
- (32) In addition, data subjects have the right to obtain rectification or amendment of inaccurate data, and to obtain deletion of data that has been processed in violation of the Principles⁴⁹. Moreover, as explained in recital 15, individuals have a right to object/opt-out to the processing of their data for materially different (but compatible) purposes than those for which the data was collected and to the disclosure of their data to third parties. When personal data is used for direct marketing purposes, individuals have a general right to opt-out from the processing at any time⁵⁰.
- (33) The Principles do not specifically address the issue of decisions affecting the data subject based solely on the automated processing of personal data. However, as

⁴¹ See also the Supplemental Principle on 'Access' (Annex I, Section III.8).

⁴² Annex I, Section III.8.a.(i)-(ii).

⁴³ Annex I, Section III.8.i.

⁴⁴ Annex I, Section III.8.f.(i)-(ii) and g.

⁴⁵ Annex I, Section III.4; 8.b, c, e; 14.e, f and 15.d.

⁴⁶ Annex I, Section III.8.e.(ii). The organisation must inform the individual of the reasons for the denial/restriction and provide a contact point for any further inquiries, Section III.8.a.(iii).

⁴⁷ Annex I, Section III.8.a.(ii)-(iii).

⁴⁸ Annex I, Section III.8.a.(i).

⁴⁹ Annex I, Section II.6 and III.8.a.(i).

⁵⁰ Annex I, Section III.8.12.

regards personal data that has been collected in the Union, any decision based on automated processing will typically be taken by the controller in the Union (which has a direct relationship with the concerned data subject) and is thus directly subject to Regulation (EU) 2016/679⁵¹. This includes transfer scenarios where the processing is carried out by a foreign (for instance U.S.) business operator acting as an agent (processor) on behalf of the controller in the Union (or as a sub-processor acting on behalf of the Union processor having received the data from a Union controller that collected it) which on this basis then takes the decision.

- (34) This was confirmed by a study commissioned by the Commission in 2018 in the context of the second annual review of the functioning of the Privacy Shield⁵², which concluded that, at the time, there was no evidence suggesting that automated decision-making was normally being carried out by Privacy Shield organisations on the basis of personal data transferred under the Privacy Shield.
- (35) In any event, in areas where companies most likely resort to the automated processing of personal data to take decisions affecting the individual (e.g. credit lending, mortgage offers, employment, housing and insurance), U.S. law offers specific protections against adverse decisions⁵³. These acts typically provide that individuals have the right to be informed of the specific reasons underlying the decision (e.g. the rejection of a credit), to dispute incomplete or inaccurate information (as well as reliance on unlawful factors), and to seek redress. In the area of consumer credit, the Fair Credit Reporting Act (FCRA) and Equal Credit Opportunity Act (ECOA) contain safeguards that provide consumers with some form of a right to explanation and a right to contest the decision. These Acts are relevant in a wide range of areas, including credit, employment, housing and insurance. In addition, certain anti-discrimination laws, such as Title VII of the Civil Rights Act and the Fair Housing Act, provide individuals with protections with respect to models used in automated decision-making that could lead to discrimination on the basis of certain characteristics, and grant individuals rights to challenge such decisions, including automated ones. With respect to health information, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule creates certain rights that are similar to those of Regulation (EU) 2016/679 with respect to accessing personal health information. In addition, guidance from the U.S. authorities require medical providers to receive information

⁵¹ Conversely, in the exceptional case where the U.S. organisation has a direct relationship with the Union data subject, this will typically be a consequence of it having targeted the individual in the Union by offering him or her goods or services or monitoring his or her behaviour. In this scenario, the U.S. organisation will itself fall within the scope of application of Regulation (EU) 2016/679 (Article 3(2)) and thus has to directly comply with Union data protection law.

⁵² SWD(2018)497final, section 4.1.5. The study focused on (i) the extent to which Privacy Shield organisations in the U.S. take decisions affecting individuals based on automated processing of personal data transferred from companies in the EU under the Privacy Shield; and (ii) the safeguards for individuals that U.S. federal law provides for this kind of situations and the conditions for these safeguards to apply.

⁵³ See e.g. the Equal Credit Opportunity Act (15 U.S.C. 1691 et seq.), Fair Credit Reporting Act (15 USC § 1681 et seq.), or the Fair Housing Act (42 U.S.C. 3601 et seq.). In addition, the United States has subscribed to the Organisation for Economic Cooperation and Development Artificial Intelligence Principles, which inter alia include principles on transparency, explain ability, security and accountability.

that allow them to inform individuals of automated decision-making systems used in the medical sector⁵⁴.

- (36) Therefore, these rules offer protections similar to those provided under Union data protection law in the unlikely situation in which automated decisions would be taken by the EU-U.S. DPF organisation itself.

2.2.6 *Restrictions on onward transfers*

- (37) The level of protection afforded to personal data transferred from the Union to organisations in the United States must not be undermined by the further transfer of such data to a recipient in the United States or another third country.

- (38) Under the *Accountability for Onward Transfer Principle*⁵⁵, special rules apply for so-called ‘onward transfers’, i.e. transfers of personal data from an EU-U.S. DPF organisation to a third party controller or processor, irrespective of whether the latter is located in the United States or a third country outside the United States (and the Union). Any onward transfer can only take place (i) for limited and specified purposes, (ii) on the basis of a contract between the EU-U.S. DPF organisation and the third party⁵⁶ (or comparable arrangement within a corporate group⁵⁷) and (iii) only if that contract requires the third party to provide the same level of protection as the one guaranteed by the Principles.

- (39) This obligation to provide the same level of protection as guaranteed by the Principles, read in combination with the *Data Integrity and Purpose Limitation Principle*, notably means that the third party may only process the personal information transmitted to it for purposes that are not incompatible with the purposes for which it was collected or subsequently authorised by the individual (in accordance with the *Choice Principle*).

- (40) The *Accountability for Onward Transfer Principle* should also be read in conjunction with the *Notice Principle* and, in the case of an onward transfer to a third party controller⁵⁸, with the *Choice Principle*, according to which data subjects must be informed (among others) about the type/identity of any third party recipient, the purpose of the onward transfer and the choice offered, and can object (opt out) or, in the case of sensitive data, have to give “affirmative express consent” (opt in) for the onward transfer.

⁵⁴ See e.g. the guidance available at [2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/2013-08-16-what-personal-health-information-do-individuals-have-a-right-under-hipaa-to-access-from-their-health-care-providers-and-health-plans/).

⁵⁵ See Annex I, Section II.3 and Supplemental Principle ‘Obligatory contracts for Onward Transfers’ (Annex I, Section III.10).

⁵⁶ As an exception to this general principle, an organisation may onward transfer personal data of a small number of employees without entering into a contract with the recipient for occasional employment-related operational needs, e.g. the booking of a flight, hotel room, or insurance coverage. However, also in this case, the organisation still has to comply with the *Notice* and *Choice* Principles (see Annex I, Section III.9.e).

⁵⁷ See Supplemental Principle ‘Obligatory contracts for Onward Transfers’ (Annex I, Section III.10.b). While this principle allows for transfers based also on non-contractual instruments (e.g. intra-group compliance and control programs), the text makes clear that these instruments must always “ensur[e] the continuity of protection of personal information under the Principles”. Moreover, given that the certified U.S. organisation will remain responsible for compliance with the Principles, it will have a strong incentive to use instruments that are indeed effective in practice.

⁵⁸ Individuals will have no opt-out right where the personal data is transferred to a third party that is acting as an agent to perform tasks on behalf of and under the instructions of the U.S. organisation. However, this requires a contract with the agent and the U.S. organisation will bear the responsibility to guarantee the protections provided under the Principles by exercising its powers of instruction.

- (41) The obligation to provide the same level of protection as required by the Principles applies to any and all third parties involved in the processing of the data so transferred irrespective of their location (in the U.S. or another third country) as well as when the original third party recipient itself transfers those data to another third party recipient, for example for sub-processing purposes.
- (42) In all cases, the contract with the third-party recipient must provide that the latter will notify the EU-U.S. DPF organisation if it makes a determination that it can no longer meet its obligation. When such a determination is made, the processing by the third party must cease or other reasonable and appropriate steps must be taken to remedy the situation⁵⁹.
- (43) Additional protections apply in the case of an onward transfer to a third party agent (i.e. a processor). In such a case, the U.S. organisation must ensure that the agent only acts on its instructions and take reasonable and appropriate steps (i) to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organisation's obligations under the Principles and, (ii) to stop and remediate unauthorised processing, upon notice⁶⁰. The organisation may be required by the DoC to provide a summary or representative copy of the privacy provisions of the contract⁶¹. Where compliance problems arise in a (sub-)processing chain, the organisation acting as the controller of the personal data will in principle face liability, as specified in the *Recourse, Enforcement and Liability Principle*, except if it proves that it is not responsible for the event giving rise to the damage⁶².

2.2.7 Accountability

- (44) Under the accountability principle, entities processing data are required to put in place appropriate technical and organisational measures to effectively comply with their data protection obligations and be able to demonstrate such compliance, in particular to the competent supervisory authority.
- (45) Once an organisation has voluntarily decided to certify⁶³ under the EU-U.S. DPF, its effective compliance with the Principles is compulsory and enforceable. Under the *Recourse, Enforcement and Liability Principle*⁶⁴, EU-U.S. DPF organisations must provide effective mechanisms to ensure compliance with the Principles. Organisations must also take measures to verify⁶⁵ that their privacy policies conform to the Principles and are in fact complied with. This can be done either through a system of self-assessment, which must include internal procedures ensuring that employees receive training on the implementation of the organisation's privacy policies and that compliance is periodically reviewed in an objective manner, or outside compliance reviews, the methods of which may include auditing, random checks or use of technology tools.

⁵⁹ The situation is different depending on whether the third party is a controller or a processor (agent). In the first scenario, the contract with the third party must provide that the latter ceases processing or takes other reasonable and appropriate steps to remedy the situation. In the second scenario, it is for the EU-U.S. DPF organisation - as the one controlling the processing under whose instructions the agent operates - to take these measures. See Annex I, Section II.3.

⁶⁰ Annex I, Section II.3.b.

⁶¹ *Ibid.*

⁶² Annex I, Section II.7.d.

⁶³ See also Supplemental Principle 'Self-Certification' (Annex I, Section III.6).

⁶⁴ See also Supplemental Principle 'Dispute Resolution and Enforcement' (Annex I, Section III.11).

⁶⁵ See also Supplemental Principle 'Verification' (Annex I, Section III.7).

- (46) In addition, organisations must retain records on the implementation of their EU-U.S. DPF practices and make them available upon request in the context of an investigation or a complaint about non-compliance to an independent dispute resolution body or competent enforcement authority⁶⁶.

2.3 Administration, oversight and enforcement

- (47) The EU-U.S. DPF will be administered and monitored by the DoC. The Framework provides for oversight and enforcement mechanisms in order to verify and ensure that EU-U.S. DPF organisations comply with the Principles and that any failure to comply is addressed. These mechanisms are set out in the Principles (Annex I) and the commitments undertaken by the DoC (Annex III), the FTC (Annex IV) and the DoT (Annex V).

2.3.1 (Re-)certification

- (48) To certify under the EU-U.S. DPF (or re-certify on an annual basis), organisations are required to publicly declare their commitment to comply with the Principles, make their privacy policies available and fully implement them⁶⁷. As part of their (re-)certification application, organisations have to submit information to the DoC on, inter alia, the name of the relevant organisation, a description of the purposes for which the organisation will process personal data, the personal data that will be covered by the certification, as well as the chosen verification method, the relevant independent recourse mechanism and the statutory body that has jurisdiction to enforce compliance with the Principles⁶⁸.
- (49) Organisations can receive personal data on the basis of the EU-U.S. DPF from the date they are placed on the DPF list by the DoC. To ensure legal certainty and avoid ‘false claims’, organisations certifying for the first time are not allowed to publicly refer to their adherence to the Principles before the DoC has determined that the organisation’s certification submission is complete and added the organisation to the DPF List⁶⁹. To be allowed to continue to rely on the EU-U.S. DPF to receive personal data from the Union, such organisations must annually re-certify their participation in the framework. When an organisation leaves the EU-U.S. DPF for any reason, it must remove all statements implying that the organisation continues to participate in the Framework⁷⁰.
- (50) As reflected in the commitments set out in Annex III, the DoC will verify whether organisations meet all certification requirements and have put in place a (public) privacy policy containing the information required under the *Notice Principle*⁷¹. Building on the experience with the (re-)certification process under the Privacy Shield, the DoC will carry out a number of checks, including to verify whether organisations’ privacy policies contain a hyperlink to the correct complaint form on the website of the relevant dispute resolution mechanism and, when several entities and subsidiaries of one organisation are included in a certification submission, whether the privacy policies of each of those entities meet the certification requirements and are readily

⁶⁶ Annex I, Section III.7.

⁶⁷ Annex I, Section I. 2.

⁶⁸ Annex I, Section III.6.b and Annex III, see section ‘Verify Self-Certification Requirements’.

⁶⁹ Annex I, footnote 12.

⁷⁰ Annex I, Section III.6.h.

⁷¹ Annex I, Section III.6.a and footnote 12, as well as and Annex III, see section ‘Verify Self-Certification Requirements’.

available to data subjects⁷². In addition, where necessary, the DoC will carry out cross-checks with the FTC and DoT to verify that the organisations are subject to oversight body identified in their (re-)certification submissions, and will work with alternative dispute resolution bodies to verify that the organisations are registered for the independent recourse mechanism identified in their (re-)certification submission⁷³.

- (51) The DoC will inform organisations that, in order to complete the (re-)certification, they must address all issues identified during its review. In case an organisation fails to respond within a timeframe set by the DoC (for example, as regards re-certification the expectation would be that the process is completed within 45 days)⁷⁴ or otherwise fails to complete its certification, the submission will be considered abandoned. In that case, any misrepresentation about participation or compliance with the EU-U.S. DPF may be subject to enforcement action by the FTC or DoT⁷⁵.
- (52) To ensure the proper application of the EU-U.S. DPF, interested parties, such as data subjects, data exporters and the national data protection authorities (DPAs), must be able to identify those organisations adhering to the Principles. To ensure such transparency at the ‘entry point’, the DoC has committed to maintain and make available to the public the list of organisations that have certified their adherence to the Principles and fall within the jurisdiction of at least one of the enforcement authorities referred to in Annexes IV and V to this Decision⁷⁶. The DoC will update the list on the basis of an organisation’s annual re-certification submission and whenever an organisation withdraws or is removed from the EU-U.S. DPF. Furthermore, to guarantee transparency also at the ‘exit point’, the DoC will maintain and make available to the public a record of organisations that have been removed from the list, in each case identifying the reason for such removal⁷⁷. Finally, it will provide a link to the FTC’s webpage on the EU-U.S. DPF, which will list the FTC’s enforcement action under the Framework⁷⁸.

2.3.2 *Compliance monitoring*

- (53) The DoC will monitor on an ongoing basis the effective compliance with the Principles by EU-U.S. DPF organisations through different mechanisms⁷⁹. In particular, it will carry out ‘spot checks’ of randomly selected organisations, as well as ad hoc spot checks of specific organisations when potential compliance issues are identified (e.g. reported to the DoC by third parties) to verify whether (i) point(s) of contact for handling complaints and data subject requests are available and responsive; (ii) the organisation’s privacy policy is readily available, both on its website and via a

⁷² Annex III, section ‘Verify Self-Certification Requirements’.

⁷³ Similarly, the DoC will work with the third party that will serve as the custodian of the funds collected through a fee for the DPA panel (see recital 73) to verify that organisations choosing the DPAs as their independent recourse mechanism have paid the fee for the relevant year. See Annex III, section ‘Verify Self-Certification Requirements’.

⁷⁴ Annex III, footnote 2.

⁷⁵ See Annex III, section ‘Verify Self-Certification Requirements’.

⁷⁶ Information about the management of the DPF List can be found in Annex III (see the introduction under ‘Administration and Supervision of the Data Privacy Framework Program by the Department of Commerce’) and Annex I (Section I.3, Section I.4, III.6.d, and Section III.11.g).

⁷⁷ Annex III, see the introduction under ‘Administration and Supervision of the Data Privacy Framework Program by the Department of Commerce’.

⁷⁸ See Annex III, section ‘Tailor the Data Privacy Framework Website to Targeted Audiences’.

⁷⁹ See Annex III, section ‘Conduct Periodic ex officio Compliance Reviews and Assessments of the Data Privacy Framework Program’.

hyperlink on the DoC's website; (iii) the organisation's privacy policy continues to comply with the certification requirements and (iv) the organisations' chosen independent dispute resolution mechanism is available to handle complaints⁸⁰.

- (54) If there is credible evidence that an organisation does not comply with its commitments under the EU-U.S. DPF (including if the DoC receives complaints or the organisation does not respond satisfactorily to inquiries of the DoC), the DoC will require the organisation to complete and submit a detailed questionnaire⁸¹. An organisation that fails to satisfactorily and timely reply to the questionnaire will be referred to the relevant authority (the FTC or DoT) for possible enforcement action⁸². As part of its compliance monitoring activities under the Privacy Shield, the DoC regularly conducted the spot checks mentioned in recital 53 and continuously monitored public reports, which allowed it to identify, address and resolve compliance issues⁸³. Organisations that persistently fail to comply with the Principles will be removed from the DPF List and must return or delete the personal data received under the Framework⁸⁴.
- (55) In other cases of removal, such as voluntary withdrawal from participation or failure to recertify, the organisation must either delete or return the data, or may retain it, provided it affirms to the DoC on an annual basis its commitment to continue to apply the Principles or provides adequate protection for the personal data by another authorized means (e.g. by using a contract that fully reflects the requirements of the relevant standard contractual clauses approved by the Commission)⁸⁵. In this case, an organisation also has to identify a contact point within the organisation for all EU-U.S. DPF-related questions.

2.3.3 Identifying and addressing false claims of participation

- (56) The DoC will monitor any false claims of EU-U.S. DPF participation or the improper use of the EU-U.S. DPF certification mark, both ex officio and on the basis of complaints (e.g. received from DPAs)⁸⁶. In particular, the DoC will on an ongoing basis verify that organisations that (i) withdraw from participation in the EU-U.S. DPF, (ii) fail to complete the annual re-certification (i.e. either started, but failed to complete the annual re-certification process in a timely manner or did not even start

⁸⁰ As part of its monitoring activities, the DoC may use different tools, including to check for broken links to privacy policies or actively monitor the news for reports that provide credible evidence of non-compliance.

⁸¹ See Annex III, section 'Conduct Periodic ex officio Compliance Reviews and Assessments of the Data Privacy Framework Program'.

⁸² See Annex III, section 'Conduct Periodic ex officio Compliance Reviews and Assessments of the Data Privacy Framework Program'.

⁸³ During the second annual review of the Privacy Shield, the DoC informed that it had conducted spot checks on 100 organisations and sent compliance questionnaires in 21 cases (after which the detected issues were rectified), see Commission SWD (2018) 497 final, p. 9. Similarly, the DoC reported during the third annual review of the Privacy Shield that it had detected three incidents through its monitoring of public reports and started the practice of carrying out spot checks on 30 companies each month, which led to follow-up with compliance questionnaires in 28% of the cases (after which the detected issues were immediately rectified, or, in three cases, were resolved after a warning letter), see Commission SWD (2019) 495 final, p. 8.

⁸⁴ Annex I, Section III.11.g. A persistent failure to comply arises, in particular, where an organisation refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or enforcement authority.

⁸⁵ Annex I, Section III.6.f.

⁸⁶ Annex III, section 'Search for and Address False Claims of Participation'.

the annual re-certification process), (iii) are removed as a participant, notably for “persistent failure to comply,” or (iv) fail to complete an initial certification (i.e. started, but failed to complete the initial certification process in a timely manner), remove from any relevant published privacy policy references to the EU-U.S. DPF that imply that the organisation actively participates in the Framework⁸⁷. The DoC will also conduct internet searches to identify references to the EU-U.S. DPF in organisations’ privacy policies, including to identify false claims by organisations that never participated in the EU-U.S. DPF⁸⁸.

- (57) Where the DoC finds that references to the EU-U.S. DPF have not been removed or are improperly used, it will inform the organisation about a possible referral to the FTC/DoT⁸⁹. If an organisation fails to respond satisfactorily, the DoC will refer the matter to the relevant agency for potential enforcement action⁹⁰. Any misrepresentation to the general public by an organisation concerning its adherence to the Principles in the form of misleading statements or practices is subject to enforcement action by the FTC, DoT or other relevant U.S. enforcement authorities. Misrepresentations to the DoC are enforceable under the False Statements Act (18 U.S.C. § 1001).

2.3.4 Enforcement

- (58) In order to ensure that an adequate level of data protection is guaranteed in practice, an independent supervisory authority tasked with powers to monitor and enforce compliance with the data protection rules should be in place.
- (59) EU-U.S. DPF organisations must be subject to the jurisdiction of the competent U.S. authorities – the FTC and DoT – which have the necessary investigatory and enforcement powers to effectively ensure compliance with the Principles⁹¹.
- (60) The FTC is an independent authority composed of five Commissioners, who are appointed by the President with the advice and consent of the Senate⁹². Commissioners are appointed for a seven-year term and may only be removed by the President for inefficiency, neglect of duty, or malfeasance in office. The FTC may not have more than three Commissioners of the same political party and Commissioners may not, during their appointment, engage in any other business, vocation, or employment.
- (61) The FTC can investigate compliance with the Principles, as well as false claims of adherence to the Principles or participation in the EU-U.S. DPF by organisations which either are no longer on the DPF List or have never certified⁹³. The FTC can

⁸⁷ *Ibid.*

⁸⁸ *Ibid.*

⁸⁹ *Ibid.*

⁹⁰ Under the Privacy Shield, the DoC reported during the third annual review of the framework that it had identified 669 cases of false claims of participation (between October 2018 and October 2019), most of which were resolved after the DoC’s warning letter, with 143 cases being referred to the FTC (see recital 62 below). See Commission SWD (2019) 495 final, p. 10.

⁹¹ An EU-U.S. DPF organisation has to publicly declare its commitment to comply with the Principles, disclose its privacy policies in line with these Principles and fully implement them. Failure to comply is enforceable under Section 5 of the FTC Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. §45) and 49 U.S.C. §41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice in air transportation or the sale of air transportation.

⁹² 15 U.S.C. § 41.

⁹³ Annex IV.

enforce compliance by seeking administrative or federal court orders (including ‘consent orders’ achieved via settlements)⁹⁴ for preliminary or permanent injunctions or other remedies, and will systematically monitor compliance with such orders⁹⁵. Where organisations fail to comply with such orders, the FTC may seek civil penalties and other remedies, including for any injury caused by the unlawful conduct. Each consent order issued to an EU-U.S. DPF organisation will have self-reporting provisions⁹⁶, and organisations will be required to make public any relevant EU-U.S. DPF-related sections of any compliance or assessment report submitted to the FTC. Finally, the FTC will maintain an online list of organisations subject to FTC or court orders in EU-U.S. DPF cases⁹⁷.

- (62) With respect to the Privacy Shield, the FTC took enforcement action in around 22 cases, both with respect to violations of specific requirements of the framework (e.g. failure to affirm to the DoC that the organisation continued to apply the Privacy Shield protections after it left the framework, failure to verify, through a self-assessment or outside compliance review, that the organisation complied with the framework)⁹⁸ and false claims of participation in the framework (e.g. by organisations that failed to complete the necessary steps to obtain certification, or allowed their certification to lapse but misrepresented their continued participation)⁹⁹. This enforcement action inter alia resulted from the proactive use of administrative subpoenas to obtain materials from certain Privacy Shield participants to check to check for substantive violations of the Privacy Shield obligations¹⁰⁰.
- (63) More generally, the FTC has in the past years taken enforcement action in a number of cases concerning compliance with specific data protection requirements that are also provided under the EU-U.S. DPF, e.g. as regards the principles of purpose limitation and data retention¹⁰¹, data minimisation¹⁰², data security¹⁰³ and data accuracy¹⁰⁴.

⁹⁴ According to information from the FTC, it has no power to conduct on-site inspections in the area of privacy protection. However, it has the power to compel organisations to produce documents and provide witness statements (see Section 20 of the FTC Act), and may use the court system to enforce such orders in case of non-compliance.

⁹⁵ See Annex IV, section ‘Seeking and Monitoring Orders’.

⁹⁶ FTC or court orders may require companies to implement privacy programs and to regularly make compliance reports or independent third-party assessments of those programs available to the FTC.

⁹⁷ Annex IV, section ‘Seeking and Monitoring Orders’.

⁹⁸ Commission SWD (2019) 495 final, p. 11.

⁹⁹ See the cases listed on the FTC’s website, available via <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>. See also Commission SWD (2017) 344 final, p.17; Commission SWD (2018) 497 final, p. 12 and Commission SWD (2019) 495 final, p. 11.

¹⁰⁰ See e.g. see [Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review \(ftc.gov\)](#).

¹⁰¹ See e.g. the FTC’s order in Drizly, LLC., inter alia requiring the company (1) to destroy any personal data it collected that is not necessary for it to provide products or services to consumers, (2) refrain from collecting or storing personal information unless it is necessary for specific purposes outlined in a retention schedule.

¹⁰² See e.g. the FTC order in CafePress (24 March 2022) requiring inter alia to minimize the amount of data that is collected.

¹⁰³ See e.g. the FTC’s enforcement action in Drizzly, LLC and CafePress, where it required the relevant companies to put in place a dedicated security program or specific security measures. In addition, as regards data breaches, see also the FTC order of 27 January 2023 in Chegg, the settlement reached with Equifax in 2019 (<https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>)

¹⁰⁴ See e.g. the case of RealPage, Inc (16 October 2018), where the FTC took enforcement action under the FCRA against a tenant screening company that provided background reports on individuals to property

- (64) The DoT has exclusive authority to regulate the privacy practices of airlines, and shares jurisdiction with the FTC with respect to the privacy practices of ticket agents in the sale of air transportation. DoT officers first aim at reaching a settlement and, if this is not possible, may initiate enforcement proceedings involving an evidentiary hearing before a DoT administrative law judge who has the authority to issue cease-and-desist orders and civil penalties¹⁰⁵. Administrative law judges benefit from several protections under the Administrative Procedure Act (APA) to ensure their independence and impartiality. For example, they can only be dismissed for good cause; are assigned to cases in rotation; may not perform duties inconsistent with their duties and responsibilities as administrative law judges; are not subject to supervision by the investigative team of the authority they are employed by (in this case the DoT); and must conduct their adjudicative/enforcement function impartially¹⁰⁶. The DoT has committed to monitor enforcement orders and ensure that orders resulting from EU-U.S. DPF cases are available on its website¹⁰⁷.

2.4 Redress

- (65) In order to ensure adequate protection and in particular the enforcement of individual rights, the data subject should be provided with effective administrative and judicial redress.
- (66) The EU-U.S. DPF, through the *Recourse, Enforcement and Liability Principle*, requires organisations to provide recourse for individuals who are affected by non-compliance and thus the possibility for Union data subjects to lodge complaints regarding non-compliance by EU-U.S. DPF organisations and to have these complaints resolved, if necessary by a decision providing an effective remedy¹⁰⁸. As part of their certification, organisations must satisfy the requirements of this Principle by providing for effective and readily available independent recourse mechanisms by which each individual's complaints and disputes can be investigated and expeditiously resolved at no cost to the individual¹⁰⁹.
- (67) Organisations may choose independent recourse mechanisms in either the Union or in the United States. As explained in more detail in recital 73, this includes the possibility to voluntarily commit to cooperate with the EU DPAs. Where organisations process human resources data, such commitment to cooperate with EU DPAs is mandatory. Other alternatives include independent alternative dispute resolution or private-sector developed privacy programs that incorporate the Principles into their rules. The latter must include effective enforcement mechanisms in accordance with the requirements of the *Recourse, Enforcement and Liability Principle*.
- (68) Consequently, the EU-U.S. DPF provides data subjects with a number of possibilities to enforce their rights, lodge complaints regarding non-compliance by EU-U.S. organisations and to have their complaints resolved, if necessary by a decision

owners and property management companies, based on information from rental histories, public record information (including criminal and eviction histories) and credit information, which were used as a factor in determining eligibility for housing. The FTC found that the company did not take reasonable measures to ensure the accuracy of the information that it provided on the basis of its auto-decision tool.

¹⁰⁵ See Annex V, section 'Enforcement Practices'.

¹⁰⁶ See 5 U.S.C. §§ 3105, 7521(a), 554(d) and 556(b)(3).

¹⁰⁷ Annex V, see section 'Monitoring and Making Public Enforcement Orders Concerning EU-U.S. DPF Violations'.

¹⁰⁸ Annex I, Section II.7.

¹⁰⁹ Annex I, Section III.11.

providing an effective remedy. Individuals can bring a complaint directly to an organisation, to an independent dispute resolution body designated by the organisation, to national DPAs, the DoC or to the FTC. In cases where their complaints have not been resolved by any of these recourse or enforcement mechanisms, individuals also have a right to invoke binding arbitration (Annex I of Annex I to this Decision). Except for the arbitral panel, which requires certain remedies to be exhausted before it can be invoked, individuals are free to pursue any or all of the redress mechanisms of their choice, and are not obliged to choose one mechanism over the other or to follow a specific sequence.

- (69) Firstly, Union data subjects may pursue cases of non-compliance with the Principles through direct contacts with the EU-U.S. DPF organisations¹¹⁰. To facilitate resolution, the organisation must put in place an effective redress mechanism to deal with such complaints. An organisation's privacy policy must therefore clearly inform individuals about a contact point, either within or outside the organisation, that will handle complaints (including any relevant establishment in the Union that can respond to inquiries or complaints), as well as on the designated independent dispute resolution body (see recital 70). Upon receipt of an individual's complaint, directly from the individual or through the DoC following referral by a DPA, the organisation must provide a response to the Union data subject within a period of 45 days¹¹¹. Likewise, organisations are required to respond promptly to inquiries and other requests for information from the DoC or from a DPA¹¹² (where the organisation has committed to cooperate with the DPA) relating to their adherence to the Principles.
- (70) Secondly, individuals can also bring a complaint directly to the independent dispute resolution body (either in the United States or in the Union) designated by an organisation to investigate and resolve individual complaints (unless they are obviously unfounded or frivolous) and to provide appropriate recourse free of charge to the individual¹¹³. Sanctions and remedies imposed by such a body must be sufficiently rigorous to ensure compliance by organisations with the Principles and should provide for a reversal or correction by the organisation of the effects of non-compliance and, depending on the circumstances, the termination of the further processing of the personal data at stake and/or their deletion, as well as publicity for findings of non-compliance¹¹⁴. Independent dispute resolution bodies designated by an organisation are required to include on their public websites relevant information regarding the EU-U.S. DPF and the services they provide under it¹¹⁵. Each year, they must publish an annual report providing aggregate statistics regarding these services¹¹⁶.
- (71) As part of its compliance review procedures, the DoC may verify that EU-U.S. DPF organisations are actually registered with the independent recourse mechanisms they

¹¹⁰ Annex I, Section III.11.d.(i).

¹¹¹ Annex I, Section III.11.d.(i).

¹¹² This is the handling authority designated by the panel of DPAs provided for in the Supplemental Principle on 'The Role of the Data Protection Authorities' (Annex I, Section III.5).

¹¹³ Annex I, Section III.11.d.

¹¹⁴ Annex I, Section II.7 and III.11.e.

¹¹⁵ Annex I, Section III.11.d.(ii).

¹¹⁶ The annual report must include: (1) the total number of EU-U.S. DPF-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed.

claim they are registered with¹¹⁷. Both the organisations and the responsible independent recourse mechanisms are required to respond promptly to inquiries and requests by the DoC for information relating to the EU-U.S. DPF. The DoC will work with independent recourse mechanisms to verify that they include information on their websites regarding the Principles and the services they provide under the EU-U.S. DPF and that they publish annual reports¹¹⁸.

- (72) In cases where the organisation fails to comply with the ruling of a dispute resolution or self-regulatory body, the latter must notify such non-compliance to the DoC and the FTC (or another U.S. authority with jurisdiction to investigate non-compliance by the organisation), or a competent court¹¹⁹. If an organisation refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution or government body, or where such a body determines that an organisation frequently fails to comply with the Principles, this may be considered as a persistent failure to comply with the result that the DoC, after first providing 30 days' notice and an opportunity to respond to the organisation that has failed to comply, will strike the organisation off the DPF List¹²⁰. If, after removal from the list, the organisation continues to make the claim of EU-U.S. DPF certification, the DoC will refer it to the FTC or other enforcement agency¹²¹.
- (73) Thirdly, individuals may also bring their complaints to a national DPA in the Union, which may make use of their investigatory and remedial powers under Regulation (EU) 2016/679. Organisations are obliged to cooperate in the investigation and the resolution of a complaint by a DPA either when it concerns the processing of human resources data collected in the context of an employment relationship or when the respective organisation has voluntarily submitted to the oversight by DPAs¹²². Notably, organisations have to respond to inquiries, comply with the advice given by the DPA, including for remedial or compensatory measures, and provide the DPA with written confirmation that such action has been taken¹²³. In cases of non-compliance with the advice given by the DPA, the DPA will refer such cases to the DoC (which may remove organisations from the EU-U.S. DPF list) or, for possible enforcement action, to the FTC or the DoT (failure to cooperate with the DPAs or to comply with the Principles is actionable under U.S. law)¹²⁴.
- (74) To facilitate cooperation for an effective handling of complaints, both the DoC and the FTC have put in place a dedicated point of contact that is responsible for liaising directly with DPAs¹²⁵. Those points of contact assist with DPA enquiries regarding an organisation's compliance with the Principles.

¹¹⁷ Annex I, Section 'Verify Self-Certification Requirements'.

¹¹⁸ See Annex III, section 'Facilitate Cooperation with Alternative Dispute Resolution Bodies That Provide Principles-Related Services'. See also Annex I, Section III.11.d.(ii)-(iii).

¹¹⁹ See Annex I, Section III.11.e.

¹²⁰ See Annex I, Section III.11.g, in particular points (ii) and (iii).

¹²¹ See Annex III, section on 'Search for and Address False Claims of Participation'.

¹²² Annex I, Section II.7.b.

¹²³ Annex I, Section III.5.

¹²⁴ Annex I, Section III.5.c.(ii).

¹²⁵ Annex III (see section 'Facilitate Cooperation with DPAs') and Annex IV (see sections 'Referral Prioritization and Investigation' and 'Enforcement Cooperation with EU DPAs').

- (75) The advice provided by the DPAs¹²⁶ is issued after both sides in the dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel may deliver advice as quickly as the requirement for due process allows, and as a general rule within 60 days after receiving a complaint¹²⁷. If an organisation fails to comply within 25 days of delivery of the advice and has offered no satisfactory explanation for the delay, the panel may give notice of its intention either to submit the matter to the FTC (or other competent U.S. enforcement authority), or to conclude that the commitment to cooperate has been seriously breached. In the first alternative, this may lead to enforcement action based on Section 5 of the FTC Act (or similar statute)¹²⁸. In the second alternative, the panel will inform the DoC which will consider the organisation's refusal to comply with the advice of the DPA panel as a persistent failure to comply that will lead to the organisation's removal from the DPF List.
- (76) If the DPA to which the complaint has been addressed has taken no or insufficient action to address a complaint, the individual complainant has the possibility to challenge such (in-)action in the national courts of the respective EU Member State.
- (77) Individuals may also bring complaints to DPAs even when the DPA panel has not been designated as an organisation's dispute resolution body. In these cases, the DPA may refer such complaints either to the DoC or the FTC. In order to facilitate and increase cooperation on matters relating to individual complaints and non-compliance by EU-U.S. DPF organisations, the DoC will establish a dedicated contact point to act as a liaison and to assist with DPA inquiries regarding an organisation's compliance with the Principles¹²⁹. Likewise, the FTC has committed to establish a dedicated point of contact¹³⁰.
- (78) Fourthly, the DoC has committed to receive, review and undertake best efforts to resolve complaints about an organisation's non-compliance with the Principles¹³¹. To this end, the DoC provides special procedures for DPAs to refer complaints to a dedicated contact point, track them and follow up with organisations to facilitate resolution¹³². In order to expedite the processing of individual complaints, the contact point liaises directly with the respective DPA on compliance issues and in particular updates it on the status of complaints within a period of not more than 90 days following referral¹³³. This allows data subjects to bring complaints of non-compliance by EU-U.S. DPF organisations directly to their national DPA and have them channelled to the DoC as the U.S. authority administering the EU-U.S. DPF.
- (79) Where, on the basis of its ex officio verifications, complaints or any other information, the DoC concludes that an organisation has persistently failed to comply with the Principles it may remove such an organisation from the DPF list¹³⁴. Refusal to comply with a final determination by any privacy self-regulatory, independent dispute

¹²⁶ The rules of procedure of the informal DPA panel should be established by the DPAs based on their competence to organise their work and cooperate among each other.

¹²⁷ Annex I, Section III.5.c.(i).

¹²⁸ Annex I, Section III.5.c.(ii).

¹²⁹ See Annex III, section 'Facilitate Cooperation with DPAs'.

¹³⁰ See Annex IV, sections 'Referral Prioritization and Investigation' and 'Enforcement Cooperation with EU DPAs'.

¹³¹ Annex III, see e.g. section 'Facilitate Cooperation with DPAs'.

¹³² Annex I, Section II.7.e and Annex III, section 'Facilitate Cooperation with DPAs'.

¹³³ *Ibid.*

¹³⁴ Annex I, Section III.11.g.

resolution or government body, including a DPA, will be regarded as a persistent failure to comply¹³⁵.

- (80) Fifthly, an EU-U.S. DPF organisation must be subject to the jurisdiction of U.S. authorities, in particular the FTC¹³⁶, which have the necessary investigatory and enforcement powers to effectively ensure compliance with the Principles. The FTC gives priority consideration to referrals of non-compliance with the Principles received from independent dispute resolution or self-regulatory bodies, the DoC and DPAs (acting on their own initiative or upon complaints) to determine whether Section 5 of the FTC Act has been violated¹³⁷. The FTC has committed to create a standardised referral process, to designate a point of contact at the agency for DPA referrals, and to exchange information on referrals. In addition, it may accept complaints directly from individuals and undertake EU-U.S. DPF investigations on its own initiative, in particular as part of its wider investigation of privacy issues.
- (81) Sixthly, as a recourse mechanism of ‘last resort’ in case none of the other available redress avenues has satisfactorily resolved an individual's complaint, the Union data subject may invoke binding arbitration by the ‘EU-U.S. Data Privacy Framework Panel’ (EU-U.S. DPF Panel)¹³⁸. Organisations must inform individuals about their possibility to invoke binding arbitration and they are obliged to respond once an individual has invoked this option by delivering notice to the concerned organisation¹³⁹.
- (82) This EU-U.S. DPF Panel consists of a pool of at least ten arbitrators that will be designated by the DoC and the Commission based on their independence, integrity, as well as experience in U.S. privacy and Union data protection law. For each individual dispute, the parties select from this pool a panel of one or three¹⁴⁰ arbitrators.
- (83) The International Centre for Dispute Resolution (ICDR), the international division of the American Arbitration Association (AAA), was selected by the DoC to administer arbitrations. Proceedings before the EU-U.S. DPF Panel will be governed by a set of agreed arbitration rules and a code of conduct for appointed arbitrators. The ICDR-AAA website provides clear and concise information to individuals about the arbitration mechanism and the procedure to file for arbitration.
- (84) The arbitration rules agreed between the DoC and the Commission supplement the EU-U.S. DPF which contains several features which enhance the accessibility of this mechanism for Union data subjects: (i) in preparing a claim before the panel, the data subject may be assisted by his or her national DPA; (ii) while the arbitration will take place in the United States, Union data subjects may choose to participate through video or telephone conference, to be provided at no cost to the individual; (iii) while the language used in the arbitration will as a rule be English, interpretation at the arbitral hearing and translation will in principle be provided upon a reasoned request and at no cost to the data subject; (iv) finally, while each party has to bear its own

¹³⁵ Annex I, Section III.11.g.

¹³⁶ An EU-U.S. DPF organisation has to publicly declare its commitment to comply with the Principles, publicly disclose its privacy policies in line with these Principles and fully implement them. Failure to comply is enforceable under Section 5 of the FTC Act prohibiting unfair and deceptive acts in or affecting commerce.

¹³⁷ See also the similar commitments undertaken by the DoT, Annex V.

¹³⁸ See Annex I, Annex I ‘Arbitral Model’.

¹³⁹ See Annex I, Section II.1.a.(xi) and II.7.c.

¹⁴⁰ The number of arbitrators on the panel will have to be agreed between the parties.

attorney's fees, if represented by an attorney before the panel, the DoC will maintain a fund supplied with annual contributions by the EU-U.S. DPF organisations, which are to cover the costs of the arbitration procedure up to maximum amounts to be determined by the U.S. authorities in consultation with the Commission¹⁴¹.

- (85) The EU-U.S. DPF Panel has the authority to impose individual-specific, non-monetary equitable relief¹⁴² necessary to remedy non-compliance with the Principles. While the panel takes into account other remedies already obtained by other EU-U.S. DPF mechanisms when making its determination, individuals may still resort to arbitration if they consider these other remedies to be insufficient. This allows Union data subjects to invoke arbitration in all cases where the action or inaction of EU-U.S. DPF organisations, independent recourse mechanisms or the competent U.S. authorities (for instance the FTC) has not satisfactorily resolved their complaints. Arbitration may not be invoked if a DPA has the legal authority to resolve the claim at issue with respect to the EU-U.S. DPF organisation, namely in those cases where the organisation is either obliged to cooperate and comply with the advice of the DPAs as regards the processing of human resources data collected in the employment context, or has voluntarily committed to do so. Individuals can enforce the arbitration decision in the U.S. courts under the Federal Arbitration Act, thereby ensuring a legal remedy in case an organisation fails to comply.
- (86) Seventh, where an organisation does not comply with its commitment to respect the Principles and published privacy policy, additional avenues for judicial redress are available under U.S. law, including to obtain compensation for damages. For example, individuals can under certain conditions obtain judicial redress (including compensation for damages) under State consumer laws in cases of fraudulent misrepresentation, unfair or deceptive acts or practices¹⁴³, and under tort law (in particular under the torts of intrusion upon seclusion¹⁴⁴, appropriation of name or likeness¹⁴⁵ and public disclosure of private facts¹⁴⁶).
- (87) Together, the various redress avenues described above ensure that each complaint regarding non-compliance with the EU-U.S DPF by certified organisations will be effectively adjudicated and remedied.

3. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE UNITED STATES

¹⁴¹ Annex I of Annex I, Section G.6.

¹⁴² Individuals may not claim damages in arbitration, but invoking arbitration does not foreclose the option to seek damages in the ordinary U.S. courts.

¹⁴³ See e.g. state consumer protection laws in California (Cal. Civ. Code §§ 1750 - 1785 (West) Consumers Legal Remedies Act); District of Columbia (D.C. Code §§ 28-3901); Florida (Fla. Stat. §§ 501.201 - 501.213, Deceptive and Unfair Trade Practices Act); Illinois (815 Ill. Comp. Stat. 505/1 - 505/12, Consumer Fraud and Deceptive Business Practices Act); Pennsylvania (73 Pa. Stat. Ann. §§ 201-1 - 201-9.3 (West) Unfair Trade Practices and Consumer Protection Law).

¹⁴⁴ I.e. in case of an intentional interference with an individual's private affairs or concerns, in a way that would be highly offensive to a reasonable person (Restatement (2nd) of Torts, §652(b)).

¹⁴⁵ This tort commonly applies in case of the appropriation and use of an individual's name or likeness to advertise a business or product, or for some similar commercial purpose (see Restatement (2nd) of Torts, §652C).

¹⁴⁶ I.e. when information concerning the private life of an individual is made public, where this is highly offensive to a reasonable person and the information is not of legitimate concern to the public (Restatement (2nd) of Torts, §652D).

- (88) The Commission also assessed the limitations and safeguards, including the oversight and individual redress mechanisms available in United States law as regards the collection and subsequent use by U.S. public authorities of personal data transferred to controllers and processors in the U.S. in the public interest, in particular for criminal law enforcement and national security purposes (government access)¹⁴⁷. In assessing whether the conditions under which government access to data transferred to the United States under this Decision fulfil the ‘essential equivalence’ test pursuant to Article 45(1) of Regulation (EU) 2016/679, as interpreted by the Court of Justice in light of the Charter of Fundamental Rights, the Commission took into account several criteria.
- (89) In particular, any limitation to the right to the protection of personal data must be provided for by law and the legal basis which permits the interference with such a right must itself define the scope of the limitation to the exercise of the right concerned¹⁴⁸. In addition, in order to satisfy the requirement of proportionality, according to which derogations from and limitations to the protection of personal data must apply only in so far as is strictly necessary in a democratic society to meet specific objectives of general interest equivalent to those recognized by the Union, this legal basis must lay down clear and precise rules governing the scope and application of the measures in question and impose minimum safeguards so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse¹⁴⁹. Moreover, these rules and safeguards must be legally binding and enforceable by individuals¹⁵⁰. In particular, data subjects must have the possibility of bringing legal action before an independent and impartial tribunal in order to have access to their personal data, or to obtain the rectification or erasure of such data¹⁵¹.

3.1 Access and use by U.S. public authorities for criminal law enforcement purposes

- (90) As regards interference with personal data transferred under the EU-U.S. DPF for criminal law enforcement purposes, the law of the United States imposes a number of limitations on the access and use of personal data, and provides oversight and redress mechanisms which are in line with the requirements referred to in recital 89 of this Decision. The conditions under which such access can take place and the safeguards

¹⁴⁷ This is also relevant in light of Section I.5 of Annex I. Pursuant to this Section and similarly to the GDPR, compliance with data protection requirements and rights that are part of the Privacy Principles can be subject to limitations. However, such limitations are not absolute, but can only be relied on under several conditions, for example to the extent necessary to comply with a court order or meet public interest, law enforcement, or national security requirements. In this context and for the sake of clarity, this Section also refers to the conditions set out in EO 14086 that are assessed inter alia in recitals 127-141.

¹⁴⁸ See *Schrems II*, paragraphs 174-175 and the case-law cited. See also, as regards access by public authorities of Member States, Case C-623/17 *Privacy International* ECLI:EU:C:2020:790, paragraph 65; and Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791, paragraph 175.

¹⁴⁹ See *Schrems II*, paragraphs 176 and 181, as well as the case-law cited. See also, as regards access by public authorities of Member States, *Privacy International*, paragraph 68; and *La Quadrature du Net and Others*, paragraph 132.

¹⁵⁰ See *Schrems II*, paragraphs 181-182.

¹⁵¹ See *Schrems I*, paragraph 95 and *Schrems II*, paragraph 194. In that respect, the CJEU has notably stressed that compliance with Article 47 of the Charter of Fundamental Rights, guaranteeing the right to an effective remedy before an independent and impartial tribunal, “contributes to the required level of protection in the European Union [and] must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of Regulation (EU) 2016/679” (*Schrems II*, paragraph 186).

applicable to the use of those powers are assessed in detail in the following sections. In this respect, the U.S. government (through the Department of Justice, DoJ) has also provided assurances on the applicable limitations and safeguards (Annex VI to this Decision).

3.1.1 Legal bases, limitations and safeguards

3.1.1.1 Limitations and safeguards as regards the collection of personal data for criminal law enforcement purposes

- (91) Personal data processed by certified U.S. organisations that would be transferred from the Union on the basis of the EU-U.S. DPF may be accessed for criminal law enforcement purposes by U.S. federal prosecutors and federal investigative agents under different procedures, as explained in more detail in recitals 92-99. These procedures apply in the same way when information is obtained from any U.S. organisation, regardless of the nationality or place of residence of the concerned data subjects¹⁵².
- (92) Firstly, upon request of a federal law enforcement officer or an attorney for the government, a judge may issue a warrant for a search or seizure (including of electronically stored information)¹⁵³. Such a warrant may only be issued if there is ‘probable cause’¹⁵⁴ that ‘seizable items’ (evidence of a crime, illegally possessed items, or property designed or intended for use or used in committing a crime) are likely to be found in the place specified by the warrant. The warrant must identify the property or item to be seized and designate the judge to which the warrant must be returned. A person subject to a search or whose property is subject to a search may move to suppress evidence obtained or derived from an unlawful search if that evidence is introduced against that person during a criminal trial¹⁵⁵. When a data holder (e.g. a company) is required to disclose data pursuant to a warrant, it may notably challenge the requirement to disclose as unduly burdensome¹⁵⁶.
- (93) Secondly, a subpoena may be issued by a grand jury (an investigative arm of the court impanelled by a judge or magistrate) in the context of investigations of certain serious

¹⁵² See Annex VI. See for instance, with respect to the Wiretap Act, Stored Communications Act and Pen Register Act (mentioned in more detail in recital 95-98), *Suzlon Energy Ltd v. Microsoft Corp.*, 671 F.3d 726, 729 (9th Cir. 2011).

¹⁵³ Federal Rules of Criminal Procedure, 41. In a 2018 judgment, the Supreme Court confirmed that a search warrant or warrant exception is also required for law enforcement authorities to access historical cell site location records, that provide a comprehensive overview of a user’s movements and that the user can have a reasonable expectation of privacy with respect to such information (*Timothy Ivory Carpenter v. United States of America*, No. 16-402, 585 U.S. (2018)). As a result, such data generally cannot be obtained from a cellular company on the basis of a court order on the basis of reasonable grounds to believe that the information is relevant and material to an ongoing criminal investigation, but requires showing the existence of probable cause when a warrant is used.

¹⁵⁴ According to the Supreme Court, ‘probable cause’ is a “practical, non-technical” standard that calls upon the “factual and practical considerations of everyday life on which reasonable and prudent men [...] act” (*Illinois v. Gates*, 462 U.S. 213, 232 (1983)). As regards search warrants, probable cause exists when there is a fair probability that a search will result in evidence of a crime being discovered (id).

¹⁵⁵ *Mapp v. Ohio*, 367 U.S. 643 (1961).

¹⁵⁶ See *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (holding that “due process requires a hearing on the issue of burdensomeness before compelling a telephone company to provide” assistance with a search warrant) and *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

crimes¹⁵⁷, usually at the request of a federal prosecutor, to require someone to produce or make available business records, electronically stored information, or other tangible items. In addition, different statutes authorise the use of administrative subpoenas to produce or make available business records, electronically stored information, or other tangible items in investigations involving health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations¹⁵⁸. In both cases, the information must be relevant to the investigation and the subpoena cannot be unreasonable, i.e. overbroad, oppressive or burdensome (and can be challenged by the recipient of the subpoena on those grounds)¹⁵⁹.

- (94) Very similar conditions apply to administrative subpoenas issued to seek access to data held by companies in the US for civil or regulatory (“public interest”) purposes. The authority of agencies with civil and regulatory responsibilities to issue such administrative subpoenas must be established in statute. The use of an administrative subpoena is subject to a “reasonableness test”, which requires that the investigation is conducted pursuant to a legitimate purpose, the information requested under the subpoena is relevant to that purpose, the agency does not already have the information it is seeking with the subpoena, and the necessary administrative steps to issue the subpoena have been followed¹⁶⁰. Case law of the Supreme Court has also clarified the need to balance the importance of the public interest in the information being requested with the importance of personal and organisational privacy interests¹⁶¹. While the use of an administrative subpoena is not subject to prior judicial approval, it becomes subject to judicial review in case of a challenge by the recipient on the above-mentioned grounds, or if the issuing agency seeks to enforce the subpoena in court¹⁶². In addition to these general overarching limitations, specific (stricter) requirements may follow from individual statutes¹⁶³.
- (95) Thirdly, several legal bases enable criminal law enforcement authorities to obtain access to communications data. A court may issue an order authorising the collection

¹⁵⁷ The Fifth Amendment to the U.S. Constitution requires grand jury indictment for any “capital or otherwise infamous crime.” The grand jury consists of 16 to 23 members, and determines whether probable cause exists to believe a crime has been committed. To reach this conclusion, grand juries are vested with investigative powers that allow them to issue subpoenas.

¹⁵⁸ See Annex VI.

¹⁵⁹ Federal Rules of Criminal Procedure, 17.

¹⁶⁰ *United States v. Powell*, 379 U.S. 48 (1964)

¹⁶¹ *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946).

¹⁶² The Supreme Court has clarified that, in case of a challenge of an administrative subpoena, a court must consider whether (1) the investigation is for a lawfully authorized purpose, (2) the subpoena authority at issue is within the power of Congress to command, and (3) the “documents sought are relevant to the inquiry.” The Court also noted that an administrative subpoena request must be “reasonable”, i.e. requiring “specification of the documents to be produced adequate, but not excessive, for the purposes of the relevant inquiry,” including “particularity in ‘describing the place to be searched, and the persons or things to be seized.’”

¹⁶³ For example, the Right to Financial Privacy Act provides a government authority with the power to obtain financial records held by a financial institution pursuant to an administrative subpoena only if (1) there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry and (2) a copy of the subpoena or summons has been provided to the customer together with a notice stating with reasonable specificity the nature of the inquiry (12 U.S.C. §3405). Another example is the Fair Credit Reporting Act, which prohibits consumer reporting agencies from disclosing consumer reports in response to administrative subpoena requests (and only allows them to respond to grand jury subpoena requests or court orders, 15 U.S.C. §1681 et seq.). As regards access to communication information, the specific requirements of the Stored Communications Act apply, including with respect to the possibility to use administrative subpoenas (see recitals 96-97 for a detailed overview).

of real-time, non-content dialling, routing, addressing and signalling information about a phone number or e-mail (through the use of a pen register or trap and trace device), if it finds that the authority has certified that the information likely to be obtained is relevant to a pending criminal investigation¹⁶⁴. The order must, inter alia, specify the identity, if known, of the suspect; the attributes of the communications to which it applies and a statement of the offense to which the information to be collected relates. The use of a pen register or trap and trace device may be authorised for a maximum period of sixty days, which may only be extended by a new court order.

- (96) In addition, access for criminal law enforcement purposes to subscriber information, traffic data and stored content of communications held by internet service providers, telephone companies, and other third party service providers may be obtained on the basis of the Stored Communications Act¹⁶⁵. To obtain the stored content of electronic communications, criminal law enforcement authorities must in principle obtain a warrant from a judge based on probable cause to believe that the account in question contains evidence of a crime¹⁶⁶. For subscriber registration information, IP addresses and associated time stamps, and billing information, criminal law enforcement authorities may use a subpoena. For most other stored, non-content information, such as e-mail headers without the subject line, a criminal law enforcement authority must obtain a court order, which will be issued if the judge is satisfied that there are reasonable grounds to believe that the requested information is relevant and material to an ongoing criminal investigation.
- (97) Providers that receive requests under the Stored Communications Act may voluntarily notify a customer or subscriber whose information is sought, except when the relevant criminal law enforcement authority obtains a protective order prohibiting such notification¹⁶⁷. Such a protective order is a court order requiring a provider of electronic communications services or remote computing services to whom a warrant, subpoena or court order is directed, not to notify any other person of the existence of the warrant, subpoena or court order, for as long as the court deems appropriate. Protective orders are granted if a court finds that there is reason to believe that notification would seriously jeopardise an investigation or unduly delay a trial, e.g. because it would result in endangering the life or physical safety of an individual, flight from prosecution, intimidation of potential witnesses, etc. A Deputy Attorney General memorandum (which is binding on all DoJ attorneys and agents) requires prosecutors to make a detailed determination regarding the need for a protective order and provide a justification to the court on how the statutory criteria for obtaining a

¹⁶⁴ 18 U.S.C. §3123.

¹⁶⁵ 18 U.S.C. §§ 2701-2713.

¹⁶⁶ 18 U.S.C. §§ 2701(a)-(b)(1)(A). If the concerned subscriber or customer is notified (either in advance or, in certain circumstances, through a delayed notification), the content information stored for longer than 180 days may also be obtained on the basis of an administrative subpoena or grand jury subpoena (18 U.S.C. §§ 2701(b)(1)(B)) or a court order (if there are reasonable grounds to believe that the information relevant and material to an ongoing criminal investigation (18 U.S.C. §§ 2701(d)). However, in accordance with a federal appeals court ruling, government investigators generally obtain search warrants from judges in order to collect the contents of private communication or stored data from a commercial communications service provider. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

¹⁶⁷ 18 U.S.C. § 2705(b).

protective order are met in the specific case¹⁶⁸. The memorandum also requires that applications for protective orders must generally not seek to delay notification for more than one year. Where, in exceptional circumstances, orders of longer duration might be necessary, such orders may only be sought with the written agreement of a supervisor designated by the U.S. Attorney or the appropriate Assistant Attorney General. In addition, a prosecutor must, when closing an investigation, immediately assess whether there is a basis to maintain any outstanding protective orders and, where this is not the case, terminate the protective order and ensure the service provider is notified thereof¹⁶⁹.

- (98) Criminal law enforcement authorities may also intercept in real time wire, oral or electronic communications on the basis of a court order in which a judge finds, inter alia, that there is probable cause to believe that the wiretap or electronic interception will produce evidence of a federal crime, or the whereabouts of a fugitive fleeing from prosecution¹⁷⁰.
- (99) Further protections are provided by various Department of Justice policies and guidelines, including the Attorney General Guidelines for Domestic FBI Operations (AGG-DOM), which, inter alia require that the Federal Bureau of Investigation (FBI) uses the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties¹⁷¹.
- (100) According to the representations made by the U.S. government, the same or higher protections described above apply to law enforcement investigations at State level (with respect to investigations carried out under State laws)¹⁷². In particular, constitutional provisions, as well as statutes and case-law at State level reaffirm the above mentioned protections against unreasonable searches and seizures by requiring the issuance of a search warrant¹⁷³. Similar to the protections afforded at the federal

¹⁶⁸ See the Memorandum issued by Deputy Attorney General Rod Rosenstein on 19 October 2017 on a more restrictive policy on applications for protective (or non-disclosure) orders, available at <https://www.justice.gov/criminal-ccips/page/file/1005791/download>.

¹⁶⁹ Memorandum issued by Deputy Attorney General Lisa Moncao on 27 May 2022 on a supplemental policy regarding applications for protective orders pursuant to 18 U.S.C. §2705(b).

¹⁷⁰ 18 U.S.C. §§ 2510-2522.

¹⁷¹ Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (September 2008), available at <http://www.justice.gov/archive/opa/docs/guidelines.pdf>. Additional rules and policies that prescribe limitations on the investigative activities of federal prosecutors are set out in the United States Attorneys' Manual, available at <http://www.justice.gov/usam/united-states-attorneys-manual>. To depart from these Guidelines, prior approval must be obtained from the FBI's Director, Deputy Director or Executive Assistant Director designated by the Director, unless such approval cannot be obtained because of the immediacy or gravity of a threat to the safety of persons or property or to national security (in which case Director or other authorising person needs to be notified as soon as practicable). Where the Guidelines are not followed, the FBI must notify the DoJ thereof, who in turn informs the Attorney General and Deputy Attorney General.

¹⁷² Annex VI, footnote 2. See also e.g., *Arnold v. City of Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) ("In the areas of individual rights and civil liberties, the United States Constitution, where applicable to the states, provides a floor below which state court decisions may not fall"); *Cooper v. California*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) ("Our holding, of course, does not affect the State's power to impose higher standards on searches and seizures than required by the Federal Constitution if it chooses to do so."); *Petersen v. City of Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) ("Although the Arizona Constitution may impose stricter standards on searches and seizures than does the federal constitution, Arizona courts cannot provide less protection than does the Fourth Amendment").

¹⁷³ The majority of states have replicated the protections of the Fourth Amendment in their constitutions. See Alabama Const. art. I, § 5); Alaska Const. art. I, § 14; 1; Arkansas Const. art. II, § 15; California

level, search warrants may be issued only upon a showing of probable cause and must describe the place to be searched and the person or thing to be seized¹⁷⁴.

3.1.1.2 Further use of the information collected

- (101) As regards the further use of data collected by federal criminal law enforcement authorities, different statutes, guidelines and standards impose specific safeguards. With the exception of the specific instruments applicable to the activities of the FBI (AGG-DOM and FBI Domestic Investigations and Operations Guide), the requirements described in this section generally apply to the further use of data by any federal authority, including to data accessed for civil or regulatory purposes. This includes the requirements following from the Office of Management and Budget memos/regulations, the Federal Information Security Management Modernization Act, the E-Government Act and the Federal Records Act.
- (102) In accordance with authority provided by the Clinger-Cohen Act (P.L. 104-106, Division E) and the Computer Security Act of 1987 (P.L. 100-235), the Office of Management and Budget (OMB) issued Circular No. A-130 to establish general binding guidance that applies to all federal agencies (including law enforcement authorities) when they handle personally identifiable information¹⁷⁵. In particular, the circular requires all federal agencies to “limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of personally identifiable information to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of authorised agency functions”¹⁷⁶. In addition, to the extent reasonably practicable, federal agencies must ensure that personally

Const. art. I, § 13; Colorado Const. art. II, § 7; Connecticut Const. art. I, § 7; Delaware Const. art. I, § 6; Florida Const. art. I, § 12; Georgia Const. art. I, § I, para. XIII; Hawaii Const. art. I, § 7; Idaho Const. art. I, § 17; Illinois Const. art. I, § 6; Indiana Const. art. I, § 11; Iowa Const. art. I, § 8; Kansas Const. Bill of Rights, § 15; Kentucky Const. § 10; Louisiana Const. art. I, § 5; Maine Const. art. I, § 5; Massachusetts Const. Decl. of Rights art. 14; Michigan Const. art. I, § 11; Minnesota Const. art. I, § 10; Mississippi Const. art. III, § 23; Missouri Const. art. I, § 15; Montana Const. art. II, § 11; Nebraska Const. art. I, § 7; Nevada Const. art. I, § 18; New Hampshire Const. pt. 1, art. 19; N.J. Const. art. II, § 7; New Mexico Const. art. II, § 10; New York Const. art. I, § 12; North Dakota Const. art. I, § 8; Ohio Const. art. I, § 14; Oklahoma Const. art. II, § 30; Oregon Const. art. I, § 9; Pennsylvania Const. art. I, § 8; Rhode Island Const. art. I, § 6; South Carolina Const. art. I, § 10; South Dakota Const. art. VI, § 11; Tennessee Const. art. I, § 7; Texas Const. art. I, § 9; Utah Const. art. I, § 14; Vermont Const. ch. I, art. 11; West Virginia Const. art. III, § 6; Wisconsin Const. art. I, § 11; Wyoming Const. art. I, § 4. Others (e.g. Maryland, North Carolina and Virginia) have enshrined in their constitutions specific language concerning warrants that has been judicially interpreted to provide similar or higher protections to the Fourth Amendment (see Maryland. Decl. of Rts. art. 26; North Carolina Const. art. I, § 20; Virginia Const. art. I, § 10, and relevant case law, e.g. *Hamel v. State*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008); *State v. Johnson*, 861 S.E.2d 474, 483 (N.C. 2021) and *Lowe v. Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985)). Finally, Arizona and Washington have constitutional provisions that protect privacy more generally (Arizona Const. art. 2, § 8; Washington Const. art. I, § 7), which have been interpreted by courts as providing more protections than the Fourth Amendment (see e.g. *State v. Bolt*, 689 P.2d 519, 523 (Ariz. 1984), *State v. Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *State v. Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984), *State v. Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

¹⁷⁴ See, e.g. California Penal Code § 1524.3(b); Rule 3.6-3.13 Alabama Rules of Criminal Procedure; Section 10.79.035; Revised Code of Washington; Section 19.2-59 of Chapter 5, Title 19.2 Criminal Procedure, Code of Virginia.

¹⁷⁵ I.e. “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual”, see OMB Circular No. A-130, p. 33 (definition of ‘personally identifiable information’).

¹⁷⁶ OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information, 81 Fed. Reg. 49,689 (28 July 2016), p. 17.

identifiable information is accurate, relevant, timely and complete, and reduced to the minimum necessary for the proper performance of an agency's functions. More generally, federal agencies must establish a comprehensive privacy program to ensure compliance with applicable privacy requirements, develop and evaluate privacy policies and manage privacy risks; maintain procedures to detect, document and report privacy compliance incidents; develop privacy awareness and training programmes for employees and contractors; and put in place policies and procedures to ensure that personnel is held accountable for complying with privacy requirements and policies¹⁷⁷.

- (103) In addition, the E-Government Act¹⁷⁸ requires all federal agencies (including criminal law enforcement authorities) to put in place information security protections that are commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction; have a Chief Information Officer to ensure compliance with information security requirements and perform an annual independent evaluation (e.g. by an Inspector General, see recital 109) of their information security program and practices¹⁷⁹. Similarly, the Federal Records Act (FRA)¹⁸⁰ and supplemental regulations¹⁸¹ require information held by federal agencies to be subject to safeguards ensuring the physical integrity of the information and protecting it against unauthorized access.
- (104) Pursuant to federal statutory authority, including the Federal Information Security Modernisation Act of 2014, the OMB and the National Institute of Standards and Technology (NIST) have developed standards which are binding on federal agencies (including criminal law enforcement authorities) and that further specify the minimum information security requirements that have to be put in place, including access controls, ensuring awareness and training, contingency planning, incident response, auditing and accountability tools, ensuring system and information integrity, conducting privacy and security risk assessments etc.¹⁸². Moreover, all federal agencies (including criminal law enforcement authorities) must, in accordance with guidelines of the OMB, maintain and implement a plan for handling data breaches, including when it comes to responding to such breaches and assessing the risks of harm¹⁸³.
- (105) As regards data retention, the FRA¹⁸⁴ requires U.S. federal agencies (including criminal law enforcement authorities) to establish retention periods for their records (after which such records must be disposed), which must be approved by the National

¹⁷⁷ Appendix II, §5(a)-(h).

¹⁷⁸ 44 U.S.C. Chapter 36.

¹⁷⁹ 44 U.S.C. §§ 3544-3545.

¹⁸⁰ FAC, 44 U.S.C. § 3105.

¹⁸¹ 36 C.F.R. §§ 1228.150, et seq., 1228.228, and Appendix A.

¹⁸² See e.g. OMB Circular No. A-130; NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (10 December 2020); and the NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems.

¹⁸³ Memorandum 17-12, 'Preparing for and Responding to a Breach of Personally Identifiable Information' available at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf and OMB Circular No. A-130. For example, the procedures for responding to data breaches of the Department of Justice, see <https://www.justice.gov/file/4336/download>.

¹⁸⁴ FRA, 44 U.S.C. §§3101 et seq.

Archives and Record Administration¹⁸⁵. The length of these retention period is fixed in light of different factors, such as the type of investigation, whether the evidence is still relevant to the investigation, etc. With respect to the FBI, AGG-DOM provides that the FBI must have in place such a records retention plan and maintain a system that can promptly retrieve the status of and basis for investigations.

- (106) Finally, OMB Circular No. A-130 also contains certain requirements for disseminating personally identifiable information. In principle, the dissemination and disclosure of personally identifiable information must be limited to what is legally authorised, relevant and reasonably deemed necessary for the proper performance of an agency's functions¹⁸⁶. When sharing personally identifiable information with other government entities, U.S. federal agencies must impose, where relevant, conditions (including the implementation of specific security and privacy controls) that govern the processing of the information through written agreements (including contracts, data use agreements, information exchange agreements and memoranda of understanding)¹⁸⁷. As regards the grounds on which information may be disseminated, the AGG-DOM and FBI Domestic Investigations and Operations Guide¹⁸⁸ for instance provide that the FBI may be under a legal requirement to do so (e.g. under an international agreement) or is allowed to disseminate information in certain circumstances, e.g. to other U.S. agencies if disclosure is compatible with the purpose for which the information was collected and it is related to their responsibilities; to congressional committees; to foreign agencies if the information is related to their responsibilities and the dissemination is consistent with the interests of the United States; the dissemination is notably necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security and the disclosure is compatible with the purpose for which the information was collected¹⁸⁹.

3.1.2 Oversight

- (107) The activities of federal criminal law enforcement agencies are subject to oversight by various bodies¹⁹⁰. As explained in recitals 92-99, in most cases this includes prior oversight by the judiciary, which has to authorise individual collection measures before they can be used. In addition, other bodies oversee different stages of the activities of criminal law enforcement authorities, including the collection and

¹⁸⁵ The National Archives and Record Administration has the authority to assess agency records management practices, and may determine whether continued retention of certain records is warranted (44 U.S.C. §§ 2904(c), 2906).

¹⁸⁶ OMB Circular No. A-130, Section 5.f.1.(d)

¹⁸⁷ OMB Circular No. A-130, Appendix I §3(d).

¹⁸⁸ See also FBI Domestic Investigations and Operations Guide (DIOG) Section 14.

¹⁸⁹ AGG-DOM, Section VI, B and C; FBI Domestic Investigations and Operations Guide (DIOG) Section 14.

¹⁹⁰ The mechanisms mentioned in this section also apply to the collection and use of data by federal authorities for civil and regulatory purposes. Federal civil and regulatory agencies are subject to scrutiny from their respective Inspectors Generals and oversight from Congress, including the Government Accountability Office, Congress's auditing and investigatory agency. Unless the agency has a designated Privacy and Civil Liberties Officer - a position typically found within agencies like the Department of Justice and the Department of Homeland Security (DHS) due to their law enforcement and national security responsibilities - these duties fall to the agency's Senior Agency Official for Privacy (SAOP). All federal agencies are legally obligated to designate an SAOP, who bears the responsibility for ensuring the agency's compliance with privacy laws and overseeing related matters. See, e.g., OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016).

processing of personal data. Together, these judicial and non-judicial bodies ensure that law enforcement authorities are subject to independent oversight.

- (108) Firstly, Privacy and Civil Liberties Officers exist within various departments with criminal law enforcement responsibilities¹⁹¹. While the specific powers of these officers may vary somewhat depending on the authorising statute, they typically encompass the supervision of procedures to ensure that the respective department/agency is adequately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints from individuals who consider that their privacy or civil liberties have been violated. The heads of each department or agency must ensure that Privacy and Civil Liberties Officers have the material and resources to fulfil their mandate, are given access to any material and personnel necessary to carry out their functions, and are informed about and are consulted on proposed policy changes¹⁹². Privacy and Civil Liberties Officers periodically report to Congress, including on the number and nature of the complaints received by the department/agency and a summary of the disposition of such complaints, the reviews and inquiries conducted and the impact of the activities carried out by the Officer¹⁹³.
- (109) Secondly, an independent Inspector General oversees the activities of the Department of Justice, including the FBI¹⁹⁴. Inspectors General are statutorily independent¹⁹⁵ and responsible for conducting independent investigations, audits, and inspections of the Department's programs and operations. They have access to all records, reports, audits, reviews, documents, papers, recommendations or other relevant material, if need be by subpoena, and may take testimony¹⁹⁶. While Inspectors General issue non-binding recommendations for corrective action, their reports, including on follow-up action (or the lack thereof)¹⁹⁷ are generally made public and sent to Congress, which can on this basis exercise its oversight function (see recital 111)¹⁹⁸.

¹⁹¹ See 42 U.S.C. § 2000ee-1. This includes for instance the Department of Justice, the Department of Homeland Security and the FBI. In the DHS, additionally, a Chief Privacy Officer is responsible for preserving and enhancing privacy protections and promoting transparency within the Department (6 U.S.C. 142, Section 222). All DHS systems, technology, forms, and programs that collect personal data or have a privacy impact are subject to the oversight of the Chief Privacy Officer who has access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department, and if need be by subpoena. The Privacy Officer has to report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations.

¹⁹² 42 U.S.C. § 2000ee-1(d).

¹⁹³ See 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). For example, the report of the DOJ's Chief Privacy and Civil Liberties Officer and the Office of Privacy and Civil Liberties covering the period October 2020- March 2021 shows that 389 privacy reviews were carried out, including of information systems and other programs (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

¹⁹⁴ Similarly, the Homeland Security Act of 2002 established an Office of Inspector General in the Department of Homeland Security.

¹⁹⁵ Inspectors General have secure tenure and may only be removed by the President who must communicate to Congress in writing the reasons for any such removal.

¹⁹⁶ See Inspector General Act of 1978, § 6.

¹⁹⁷ See in this respect for instance the overview prepared by the DoJ Office of the Inspector General of its recommendations made and the extent to which they have been implemented through department and agency follow-up actions, <https://oig.justice.gov/sites/default/files/reports/22-043.pdf>.

¹⁹⁸ See Inspector General Act of 1978, §§ 4(5), 5. For example, the Office of the Inspector General within the Department of Justice recently published its semi-annual report to Congress (1 October 2021- 31 March 2022, <https://oig.justice.gov/node/23596>), which provides an overview of its audits, evaluations, inspections, special reviews and investigations of DOJ programs and operations. These activities

- (110) Thirdly, to the extent they carry out counter-terrorism activities, departments with criminal law enforcement responsibilities are subject to oversight by the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the executive branch composed of a bipartisan, five-member Board appointed by the President for a fixed six-year term with Senate approval¹⁹⁹. According to its founding statute, the PCLOB is entrusted with responsibilities in the field of counterterrorism policies and their implementation, with a view to protect privacy and civil liberties. In its review it can access all relevant agency records, reports, audits, reviews, documents, papers and recommendations, including classified information, conduct interviews and hear testimony²⁰⁰. It receives reports from the civil liberties and privacy officers of several federal departments/agencies²⁰¹, may issue recommendations to the government and law enforcement authorities, and regularly reports to Congressional committees and the President²⁰². Reports of the Board, including the ones to Congress, must be made publicly available to the greatest extent possible²⁰³.
- (111) Finally, criminal law enforcement activities are subject to oversight by specific Committees in the U.S. Congress (the House and Senate Judiciary Committees). The Judiciary Committees conduct regular oversight in different ways, in particular through hearings, investigations, reviews and reports²⁰⁴.

3.1.3 Redress

- (112) As indicated, criminal law enforcement authorities must in most cases obtain prior judicial authorisation to collect personal data. Although this is not required for administrative subpoenas, these are limited to specific situations and will be subject to independent judicial review at least where the government seeks enforcement in court. In particular, recipients of administrative subpoenas may challenge them in court on the grounds that they are unreasonable, i.e. overbroad, oppressive or burdensome²⁰⁵.

included an investigation of a former contractor regarding unlawful disclosure of electronic surveillance (the wiretapping of an individual) in an ongoing investigation, which led to the sentencing of the contractor. The Office of the Inspector General also conducted an investigation of the DOJ agencies' information security programmes and practices, which includes testing the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems.

¹⁹⁹ Members of the Board must be selected solely on the basis of their professional qualifications, achievements, public stature, expertise in civil liberties and privacy, and relevant experience, and without regard to political affiliation. There may in no event be more than three members of the Board that belong to the same political party. An individual appointed to the Board may not, while serving on the Board, be an elected official, officer, or employee of the Federal Government, other than in the capacity as a member of the Board. See 42 U.S.C. § 2000ee (h).

²⁰⁰ 42 U.S.C. § 2000ee (g).

²⁰¹ See 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). These include at least the Department of Justice, the Department of Defense, the Department of Homeland Security, plus any other department, agency or element of the executive branch designated by the PCLOB to be appropriate for coverage.

²⁰² 42 U.S.C. § 2000ee, (e).

²⁰³ 42 U.S.C. § 2000ee (f).

²⁰⁴ For example, the Committees organise thematic hearings (see e.g. a recent hearing of the House Judiciary Committee on “digital dragnets”, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>), as well as, regular oversight hearings, e.g. of the FBI and DoJ, see <https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation>; <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966> and <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899>.

²⁰⁵ See Annex VI.

- (113) Individuals may first of all lodge requests or complaints with criminal law enforcement authorities concerning the handling of their personal data. This includes the possibility to request access to and correction of personal data²⁰⁶. As regards activities relating to counter-terrorism, individuals may also lodge a complaint with Privacy and Civil Liberties Officers (or other privacy officials) within law enforcement authorities²⁰⁷.
- (114) Moreover, U.S. law provides for a number of judicial redress avenues for individuals, against a public authority or one of its officials, where these authorities process personal data²⁰⁸. These avenues, which include in particular the APA, the Freedom of Information Act (FOIA) and the Electronic Communications Privacy Act (ECPA), are open to all individuals irrespective of their nationality, subject to any applicable conditions.
- (115) Generally, under the judicial review provisions of the APA²⁰⁹, “any person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action”, is entitled to seek judicial review²¹⁰. This includes the possibility to ask the court to “hold unlawful and set aside agency action, findings, and conclusions found to be [...] arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law”²¹¹.
- (116) More specifically, Title II of the ECPA²¹² sets forth a system of statutory privacy rights and as such governs law enforcement access to the contents of wire, oral or electronic communications stored by third-party service providers²¹³. It criminalises the unlawful (i.e. not authorised by court or otherwise permissible) access to such communications and provides recourse for an affected individual to file a civil action in U.S. federal court for actual and punitive damages as well as equitable or declaratory relief against a government official that has wilfully committed such unlawful acts, or against the United States.
- (117) In addition, several other statutes afford individuals the right to bring suit against a U.S. public authority or official with respect to the processing of their personal data, such as the Wiretap Act²¹⁴, the Computer Fraud and Abuse Act²¹⁵, the Federal Torts

²⁰⁶ OMB Circular No. A-130, Appendix II, Section 3(a) and (f), which requires federal agencies to ensure appropriate access and correction upon request of individuals, and to establish procedures to receive and address privacy-related complaints and requests.

²⁰⁷ See 42 U.S.C. § 2000ee-1 as regards for instance the DoJ and the Department of Homeland Security. See also OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy*.

²⁰⁸ The redress mechanisms mentioned in this section also apply to the collection and use of data by federal authorities for civil and regulatory purposes.

²⁰⁹ 5 U.S.C. § 702.

²¹⁰ Generally, only “final” agency action — rather than “preliminary, procedural, or intermediate” agency action — is subject to judicial review. See 5 U.S.C. § 704.

²¹¹ 5 U.S.C. § 706(2)(A).

²¹² 18 U.S.C. §§ 2701-2712.

²¹³ The ECPA protects communications held by two defined classes of network service providers, namely providers of: (i) electronic communication services, for instance telephony or e-mail; (ii) remote computing services like computer storage or processing services.

²¹⁴ 18 U.S.C. §§ 2510 et seq. Under the Wiretap Act (18 U.S.C. § 2520), a person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used may bring a civil action for violation of the Wiretap Act, including under certain circumstances against an individual government official or the United States. For the collection of non-content information (e.g. IP address, e-mail to/from address), see also the Pen Registers and Trap and Trace Devices chapter of Title 18 (18 U.S.C. §§ 3121-3127 and, for civil action, § 2707).

Claim Act²¹⁶, the Right to Financial Privacy Act²¹⁷, and the Fair Credit Reporting Act²¹⁸.

- (118) Also, under FOIA²¹⁹, 5 U.S.C. § 552 any person has the right to obtain access to federal agency records, including where these contain the individual's personal data. After exhausting administrative remedies, an individual may invoke such right to access in court unless those records are protected from public disclosure by an exemption or special law enforcement exclusion²²⁰. In this case, the court will assess whether any exemption applies or has been lawfully invoked by the relevant public authority.

3.2 Access and use by U.S. public authorities for national security purposes

- (119) The law of the United States contains various limitations and safeguards with respect to the access and use of personal data for national security purposes, and provides oversight and redress mechanisms that are in line with the requirements referred to in recital 89 of this Decision. The conditions under which such access can take place and

²¹⁵ 18 U.S.C. § 1030. Under the Computer Fraud and Abuse Act, a person may bring suit against any person with respect to intentional unauthorised access (or exceeding authorised access) to obtain information from a financial institution, a U.S. government computer system or other specified computer, including under certain circumstances against an individual government official.

²¹⁶ 28 U.S.C. §§ 2671 et seq. Under the Federal Tort Claims Act, a person may bring suit, under certain circumstances, against the United States with respect to “the negligent or wrongful act or omission of any employee of the Government while acting within the scope of his office or employment”.

²¹⁷ 12 U.S.C. §§ 3401 et seq. Under the Right to Financial Privacy Act, a person may bring suit, under certain circumstances, against the United States with respect to the obtaining or disclosing of protected financial records in violation of the statute. Government access to protected financial records is generally prohibited unless the government makes the request subject to a lawful subpoena or search warrant or, subject to limitations, a formal written request and the individual whose information is sought receives notice of such a request.

²¹⁸ 15 U.S.C. §§ 1681-1681x. Under the Fair Credit Reporting Act, a person may bring suit against any person who fails to comply with requirements (in particular the need for lawful authorisation) regarding the collection, dissemination and use of consumer credit reports, or, under certain circumstances, against a government agency.

²¹⁹ 5 U.S.C. § 552.

²²⁰ These exclusions are, however, framed. For example, according to 5 U.S.C. § 552 (b)(7), FOIA rights are ruled out for “records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions, if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual.” Also, “[w]henver a request is made which involves access to records [the production of which could reasonably be expected to interfere with enforcement proceedings] and– (A) the investigation or proceeding involves a possible violation of criminal law; and (B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.” (5 U.S.C. § 552 (c)(1)).

the safeguards applicable to the use of these powers are assessed in detail in the following sections.

3.2.1 Legal bases, limitations and safeguards

3.2.1.1 Applicable legal framework

- (120) Personal data transferred from the Union to EU-U.S. DPF organisations may be collected by U.S. authorities for national security purposes on the basis of different legal instruments, subject to specific conditions and safeguards.
- (121) Once personal data has been received by organisations located in the United States, U.S. intelligence agencies may seek access to such data for national security purposes only as authorised by statute, specifically under the Foreign Intelligence Surveillance Act (FISA) or and statutory provisions authorising access through National Security Letters (NSL)²²¹. FISA contains several legal bases that may be used to collect (and subsequently process) the personal data of Union data subjects transferred under the EU-U.S. DPF (Section 105 FISA²²², Section 302 FISA²²³, Section 402 FISA²²⁴, Section 501 FISA²²⁵ and Section 702 FISA²²⁶), as described in more detail in recitals 142-152.
- (122) U.S. intelligence agencies also have possibilities to collect personal data outside the United States, which may include personal data in transit between the Union and the United States. The collection outside the United States is based on Executive Order 12333 (EO 12333)²²⁷, issued by the President²²⁸.
- (123) The collection of signals intelligence is the form of intelligence collection that is the most relevant for the present adequacy finding, as it concerns the collection of electronic communications and data from information systems. Such collection may be carried out by U.S. intelligence agencies both within the United States (on the basis of FISA) and while data is in transit to the United States (on the basis of EO 12333).
- (124) On 7 October 2022, the U.S. President issued EO 14086 on Enhancing Safeguards for United States Signals Intelligence setting limitations and safeguards for all U.S. signals intelligence activities. This EO replaces Presidential Policy Directive (PPD-28)

²²¹ 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; and 18 U.S.C. § 2709. See recital 153.

²²² 50 U.S.C. § 1804, which concerns traditional individualized electronic surveillance.

²²³ 50 U.S.C. §1822, which concerns physical searches for foreign intelligence purposes.

²²⁴ 50 U.S.C. § 1842 with § 1841(2) and Section 3127 of Title 18, which concerns the installation of pen registers or trap and trace devices.

²²⁵ 50 U.S.C. § 1861, which permits FBI to submit “an application for an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism.”

²²⁶ 50 U.S. Code § 1881a, which allows US Intelligence Community elements to seek access to information, including the content of internet communications, from U.S. companies, targeting certain non-U.S. persons outside the United States with the legally compelled assistance of electronic communication providers.

²²⁷ EO 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8 December 1981 as amended 30 July 2008). EO 12333 more generally defines the goals, directions, duties and responsibilities of U.S. intelligence efforts (including the role of the various Intelligence Community elements) and sets out the general parameters for the conduct of intelligence activities.

²²⁸ Under Article II of the U.S. Constitution, responsibility ensuring national security including in particular gathering foreign intelligence falls within the President's authority as Commander in Chief of the armed forces.

to a large extent²²⁹, strengthens the conditions, limitations and safeguards that apply to all signals intelligence activities (i.e. on the basis of FISA and EO 12333), regardless of where they take place²³⁰, and establishes a new redress mechanism through which these safeguards can be invoked and enforced by individuals²³¹ (see in more detail recitals 176-194). In doing so, it implements in U.S. law the outcome of the talks that took place between the EU and U.S. following the invalidation of the Commission's adequacy decision on the Privacy Shield by the Court of Justice (see recital 6). It is, therefore, a particularly important element of the legal framework assessed in this Decision.

- (125) The limitations and safeguards introduced by EO 14086 supplement those provided by Section 702 FISA and EO 12333. The requirements described below (in sections 3.2.1.2 and 3.2.1.3) must be applied by intelligence agencies when engaging in signals intelligence activities pursuant to Section 702 FISA and EO 12333, e.g. when selecting/identifying categories of foreign intelligence information to be acquired pursuant to Section 702 FISA; collecting foreign intelligence or counterintelligence pursuant to EO 12333; and making individual targeting decisions under Section 702 FISA and EO 12333.
- (126) The requirements laid down in this Executive Order issued by the President are binding on the entire Intelligence Community. They must be further implemented through agency policies and procedures that transpose them into concrete directions for day-to-day operations. In this respect, EO 14086 provides U.S. intelligence agencies with a maximum of one year to update their existing policies and procedures (i.e. by 7 October 2023) to bring them in line with the EO's requirements. Such updated policies and procedures have to be developed in consultation with the Attorney General, the Civil Liberties Protection Officer of the Director of National Intelligence (ODNI CLPO) and the PCLOB – an independent oversight body authorised to review Executive Branch policies and their implementation, with a view to protect privacy and civil liberties (see recital 110 as regards the role and status of the PCLOB) – and be made publicly available²³². In addition, once the updated policies and procedures are in place, the PCLOB will conduct a review to ensure that they are consistent with the EO. Within 180 days of completion of such a review by the PCLOB, each intelligence agency must carefully consider and implement or

²²⁹ EO 14086 supersedes a previous Presidential Directive, PPD 28, with the exception of its Section 3 and a complementing Annex, (which requires intelligence agencies to annually review their signals intelligence priorities and requirements, taking into account the benefits of signals intelligence activities for the U.S.' national interests, as well as the risk posed by those activities) and Section 6 (which contains general provisions), see the National Security Memorandum on Partial Revocation of Presidential Policy Directive 28, available at <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/>

²³⁰ See Section 5(f) EO 14086, which explains that the EO has the same scope of application as PPD-28, which, according to its footnote 3, applied to signals intelligence activities conducted in order to collect communications or information about communications, except signals intelligence activities undertaken to test or develop signals intelligence capabilities.

²³¹ See in this respect e.g. Section 5(h) of EO 14086, which clarifies that the safeguards in the EO create a legal entitlement and can be enforced by individuals through the redress mechanism.

²³² See Section 2(c)(iv)(C) EO 14086.

otherwise address all of the PCLOB’s recommendations. On 3 July 2023, the U.S. government published such updated policies and procedures²³³.

3.2.1.2 *Limitations and safeguards as regards the collection of personal data for national security purposes*

- (127) EO 14086 sets a number of overreaching requirements that apply to all signals intelligence activities (collection, use, dissemination, etc. of personal data).
- (128) Firstly, such activities must be based on statute or Presidential authorisation and undertaken in compliance with U.S. law, including the Constitution²³⁴.
- (129) Secondly, appropriate safeguards must be in place to ensure that privacy and civil liberties are integral considerations in the planning of such activities²³⁵.
- (130) In particular, any signals intelligence activity may only be carried out “following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority” (as regards the notion of ‘validated intelligence priority’, see recital 135)²³⁶.
- (131) Moreover, such activities may only be conducted “to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized”²³⁷. In other words, a proper balance must be achieved “between the importance of the intelligence priority pursued and the impact on the privacy and civil liberties of affected individuals, regardless of their nationality or wherever they might reside”²³⁸.
- (132) Finally, to ensure compliance with these general requirements - which reflect the principles of legality, necessity and proportionality - signals intelligence activities are subject to oversight (see in more detail section 3.2.2)²³⁹.
- (133) These overarching requirements are further substantiated with respect to the collection of signals intelligence through a number of conditions and limitations ensuring that the interference with the rights of individuals is limited to what is necessary and proportionate to advance a legitimate objective.
- (134) Firstly, the EO limits the grounds on which data can be collected as part of signals intelligence activities in two ways. On the one hand, the EO lays down the legitimate objectives that may be pursued by signals intelligence collection, e.g. to understand or assess the capabilities, intentions, or activities of foreign organisations, including international terrorist organisations, that pose a current or potential threat to the national security of the United States; to protect against foreign military capabilities and activities; to understand or assess transnational threats that impact global security, such as climate and other ecological change, public health risks and humanitarian

²³³ <https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086>.

²³⁴ Section 2(a)(i) EO 14086.

²³⁵ Section 2(a)(ii) EO 14086.

²³⁶ Section 2(a)(ii)(A) EO 14086. This does not always require that signals intelligence is the sole means for advancing aspects of a validated intelligence priority. For example, the collection of signals intelligence may be used to ensure alternative pathways for validation (e.g. to corroborate information received from other intelligence sources) or for maintaining reliable access to the same information (Section 2(c)(i)(A) EO 14086).

²³⁷ Section 2(a)(ii)(B) EO 14086.

²³⁸ Section 2(a)(ii)(B) EO 14086.

²³⁹ Section 2(a)(iii), in conjunction with Section 2(d) EO 14086.

threats²⁴⁰. On the other hand, the EO lists certain objectives that must never be pursued by signals intelligence activities, e.g. for the purpose of burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press; for the purpose of disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion; or to afford a competitive advantage to U.S. companies²⁴¹.

- (135) Moreover, the legitimate objectives laid down in EO 14086 cannot by themselves be relied upon by intelligence agencies to justify signals intelligence collection but must be further substantiated, for operational purposes, into more concrete priorities for which signals intelligence may be collected. In other words, actual collection can only take place to advance a more specific priority. Such priorities are established through a dedicated process aimed at ensuring compliance with the applicable legal requirements, including those relating to privacy and civil liberties. More specifically, intelligence priorities are first developed by the Director of National Intelligence (through the so-called National Intelligence Priorities Framework) and submitted to the President for approval²⁴². Before proposing intelligence priorities to the President, the Director must, in accordance with EO 14086, obtain an assessment from the ODNI CLPO for each priority as to whether it (1) advances one or more legitimate objectives listed in the EO; (2) was neither designed nor is anticipated to result in signals intelligence collection for a prohibited objective listed in the EO; and (3) was established after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside²⁴³. In case the Director disagrees with the CLPO's assessment, both views must be presented to the President²⁴⁴.
- (136) Therefore, this process notably ensures that privacy considerations are taken into account from the initial stage where intelligence priorities are developed.
- (137) Secondly, once an intelligence priority has been established, a number of requirements govern the decision as to whether and to what extent signals intelligence may be collected to advance such a priority. These requirements operationalise the overarching necessity and proportionality standards set forth by Section 2(a) of the EO.
- (138) In particular, signals intelligence may only be collected “following a determination that, based on a reasonable assessment of all relevant factors, the collection is necessary to advance a specific intelligence priority”²⁴⁵. In determining whether a specific signals intelligence collection activity is necessary to advance a validated intelligence priority, U.S. intelligence agencies must consider the availability,

²⁴⁰ Section 2(b)(i) EO 14086. Because of the circumscribed list of legitimate objectives in the EO, which does not encompass possible future threats, the EO provides for the possibility for the President to update this list if new national security imperatives emerge, such as new threats to national security. Such updates must in principle be publicly released, unless the President determines that doing so would itself pose a risk to the national security of the United States (Section 2(b)(i)(B) EO 14086).

²⁴¹ Section 2(b)(ii) EO 14086.

²⁴² Section 102A of the National Security Act and Section 2(b)(iii) EO 14086.

²⁴³ In exceptional cases (in particular, when such process cannot be carried out because of a need to address a new or evolving intelligence requirement), such priorities can be set directly by the President or the head of an element of the Intelligence Community, who in principle have to apply the same criteria as the ones described in section 2(b)(iii)(A)(1)-(3), see Section 4(n) EO 14086.

²⁴⁴ Section 2(b)(iii)(C) EO 14086.

²⁴⁵ Section 2(b) and (c)(i)(A) EO 14086.

feasibility and appropriateness of other less intrusive sources and methods, including from diplomatic and public sources²⁴⁶. When available, such alternative, less intrusive sources and methods must be prioritised²⁴⁷.

- (139) When, in the application of such criteria, the collection of signals intelligence is considered necessary, it must be as “tailored as feasible” and must “not disproportionately impact privacy and civil liberties”²⁴⁸. To ensure that privacy and civil liberties are not disproportionately affected – i.e. to strike a proper balance between national security needs and the protection of privacy and civil liberties – all relevant factors have to be duly taken into account, such as the nature of the pursued objective; the intrusiveness of the collection activity, including its duration; the probable contribution of the collection to the objective pursued; the reasonably foreseeable consequences to individuals; and the nature and sensitivity of the data to be collected²⁴⁹.
- (140) As regards the type of signals intelligence collection, collection of data within the United States, which is the most relevant for the present adequacy finding as it concerns data that has been transferred to organisations in the U.S., must always be targeted, as explained in more detail in recitals 142-153.
- (141) ‘Bulk collection’²⁵⁰ may only be carried out outside the United States, on the basis of EO 12333. Also in this case, pursuant to EO 14086, targeted collection must be prioritised²⁵¹. Conversely, bulk collection is only allowed where the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection²⁵². When it is necessary to carry out bulk collection of data outside the United States, specific safeguards under EO 14086 apply²⁵³. Firstly, methods and technical measures must be applied in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information²⁵⁴. Secondly, the EO limits the use of information

²⁴⁶ Section 2(c)(i)(A) EO 14086.

²⁴⁷ Section 2(c)(i)(A) EO 14086.

²⁴⁸ Section 2(c)(i)(B) EO 14086.

²⁴⁹ Section 2(c)(i)(B) EO 14086.

²⁵⁰ I.e. the collection of large quantities of signals intelligence that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms), see Section 4(b) EO 14086. Pursuant to EO 14086 and as further explained in recital 141, bulk collection under EO 12333 takes place only when necessary to advance specific validated intelligence priorities and is subject to a number of limitations and safeguards designed to ensure that data is not accessed on an indiscriminate basis. Bulk collection is therefore to be contrasted to collection taking place on a generalised and indiscriminate basis (‘mass surveillance’) without limitations and safeguards.

²⁵¹ Section 2(c)(ii)(A) EO 14086.

²⁵² Section 2(c)(ii)(A) EO 14086.

²⁵³ The specific rules on bulk collection of EO 14086 also apply to a targeted signals intelligence collection activity that temporarily uses data acquired without discriminants (e.g. specific selection terms or identifiers), i.e. in bulk (which is only possible outside the territory of the United States). This is not the case when such data is only used to support the initial technical phase of the targeted signals intelligence collection activity, retained only for a short period of time required to complete this phase and deleted immediately thereafter (Section 2(c)(ii)(D) EO 14086). In this case, the only purpose of the initial collection without discriminants is to allow a targeted collection of information by applying a specific identifier or selection term. In such a scenario, only data that responds to the application of a certain discriminant is inserted into government databases, while the remaining data is destroyed. Such targeted collection therefore remains governed by the general rules that apply to signals intelligence collection, including Section 2(a)-(b) and 2(c)(i) EO 14086.

²⁵⁴ Section 2(c)(ii)(A) EO 14086.

collected in bulk (including querying) to six specific objectives, including protecting against terrorism, the taking of hostages, and the holding of individuals captive by or on behalf of a foreign government, organisation or person; protecting against foreign espionage, sabotage, or assassination; protecting against threats from the development possession, or proliferation of weapons of mass destruction or related technologies and threats, etc.²⁵⁵ Finally, any querying of signals intelligence obtained in bulk may only take place where necessary to advance a validated intelligence priority, in pursuit of these six objectives and in accordance with policies and procedures that appropriately take into account the impact of the queries on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside²⁵⁶.

- (142) In addition to the requirements of EO 14086, the signals intelligence collection of data that has been transferred to an organisation in the United States is subject to specific limitations and safeguards governed by Section 702 FISA²⁵⁷. Section 702 FISA allows the collection of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States with the compelled assistance of U.S. electronic communication service providers²⁵⁸. In order to collect foreign intelligence information pursuant to Section 702 FISA, the Attorney General and the Director of National Intelligence submit annual certifications to the Foreign Intelligence Surveillance Court (FISC) which identify categories of foreign intelligence information to be acquired²⁵⁹. Certifications must be accompanied by targeting, minimization and querying procedures, which are also approved by the Court and are legally binding on U.S. intelligence agencies.
- (143) The FISC is an independent tribunal²⁶⁰ created by federal statute whose decisions can be appealed to the Foreign Intelligence Surveillance Court of Review (FISCR)²⁶¹ and, ultimately, the Supreme Court of the United States²⁶². The FISC (and FISCR) is

²⁵⁵ Section 2(c)(ii)(B) EO 14086. In case new national security imperatives emerge, such as new threats to national security, the President may update this list. Such updates must in principle be publicly released, unless the President determines that doing so would in itself pose a risk to the national security of the United States (Section 2(c)(ii)(C) EO 14086). As regards queries of data collected in bulk, see Section 2(c)(iii)(D) EO 14086.

²⁵⁶ Section 2(a)(ii)(A), in conjunction with Section 2(c)(iii)(D) EO 14086. See also Annex VII.

²⁵⁷ 50 U.S.C. § 1881.

²⁵⁸ 50 U.S.C. § 1881a (a). In particular, as noted by the PCLOB, Section 702 surveillance “consists entirely of targeting specific [non-U.S.] persons about whom an individualised determination has been made” (Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2 July 2014, Section 702 Report, p. 111). See also NSA CLPO, NSA’s Implementation of Foreign Intelligence Act Section 702, 16 April 2014. The term ‘electronic communication service provider’ is defined in 50 U.S.C. § 1881 (a)(4).

²⁵⁹ 50 U.S.C. § 1881a (g).

²⁶⁰ The FISC is comprised of judges appointed by the Chief Justice of the United States from among sitting U.S. district court judges, who previously have been appointed by the President and confirmed by the Senate. The judges, who have life tenure and can only be removed for good cause, serve on the FISC for staggered seven-year terms. FISA requires that the judges be drawn from at least seven different U.S. judicial circuits. See 50 U.S.C. § 1803 (a). The judges are supported by experienced judicial law clerks that constitute the court’s legal staff and prepare legal analysis on collection requests. See Letter from the Honourable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to the Honourable Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate (29 July 2013) (Walton Letter), p. 2, available at <https://fas.org/irp/news/2013/07/fisc-leahy.pdf>.

²⁶¹ The FISCR is composed of judges appointed by the Chief Justice of the United States and drawn from U.S. district courts or courts of appeals, serving for a staggered seven year term. See 50 U.S.C. § 1803 (b).

²⁶² See 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

supported by a standing panel of five attorneys and five technical experts that have an expertise in national security matters as well as civil liberties²⁶³. From this group the court appoints an individual to serve as *amicus curiae* to assist in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court finds that such appointment is not appropriate²⁶⁴. This ensures in particular that privacy considerations are properly reflected in the court's assessment. The court may also appoint an individual or organisation to serve as *amicus curiae*, including to provide technical expertise, whenever it deems this appropriate or, upon motion, permit an individual or organisation leave to file an *amicus curiae* brief²⁶⁵.

- (144) The FISC reviews the certifications and the related procedures (in particular targeting and minimisation procedures) for compliance with the requirements of FISA. If it considers that the requirements are not fulfilled, it can deny the certification in full or in part and request the procedures to be amended²⁶⁶. In this respect, the FISC has repeatedly confirmed that its review of Section 702 targeting and minimization procedures is not confined to the procedures as written, but also includes how the procedures are implemented by the government²⁶⁷.
- (145) Individual targeting determinations are made by the National Security Agency (NSA, the intelligence agency responsible for targeting under Section 702 FISA) in accordance with FISC-approved targeting procedures, which require the NSA to assess, based on the totality of the circumstances, that targeting a specific person is likely to acquire a category of foreign intelligence information identified in a certification²⁶⁸. This assessment must be particularized and fact-based, informed by analytical judgment, the specialized training and experience of the analyst, as well as the nature of the foreign intelligence information to be obtained²⁶⁹. The targeting is carried out by identifying so-called selectors that identify specific communications facilities, like the target's e-mail address or telephone number, but never key words or names of individuals²⁷⁰.

²⁶³ 50 U.S.C. § 1803 (i)(1),(3)(A).

²⁶⁴ 50 U.S.C. § 1803 (i)(2)(A).

²⁶⁵ 50 U.S.C. § 1803 (i)(2)(B).

²⁶⁶ See e.g. FISC Opinion of 18 October 2018, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, as confirmed by the Foreign Intelligence Court of Review in its Opinion of 12 July 2019, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

²⁶⁷ See e.g. FISC, Memorandum Opinion and Order at 35 (18 Nov. 2020) (Authorised for Public Release on 26 April 2021), (Annex D).

²⁶⁸ 50 U.S.C. § 1881a(a), Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, of March 2018 (NSA targeting procedures), available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, p. 1-4, further explained in PCLOB report, pp. 41-42.

²⁶⁹ NSA targeting procedures, p. 4.

²⁷⁰ See PCLOB, Section 702 Report, pp. 32-33, 45 with further references. See also Semiannual Assessment with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, p. 41 (October 2018), available at: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

- (146) NSA analysts will first identify non-U.S. persons located abroad whose surveillance will lead, based on the analysts' assessment, to the relevant foreign intelligence specified in the certification²⁷¹. As set out in the NSA's targeting procedures, the NSA can only direct surveillance at a target when it has already learned something about the target²⁷². This may follow from information from different sources, for instance human intelligence. Through these other sources, the analyst must also learn about a specific selector (i.e. communication account) used by the potential target. Once these individualised persons have been identified and their targeting has been approved by an extensive review mechanism within the NSA²⁷³, selectors identifying communication facilities (such as e-mail addresses) used by the targets will be 'tasked' (i.e. developed and applied)²⁷⁴.
- (147) The NSA must document the factual basis for the selection of the target²⁷⁵ and, at regular intervals after the initial targeting, affirm that the targeting standard continues to be met²⁷⁶. Once the targeting standard is no longer satisfied, collection must be ceased²⁷⁷. The selection by the NSA of each target and its record of each recorded targeting assessment and rationale is reviewed for compliance with the targeting procedures on a bi-monthly basis by officials in the intelligence oversight offices at the Department of Justice, who are under an obligation to report any violation to the FISC and to Congress²⁷⁸. The NSA's written documentation facilitates the FISC's oversight of whether specific individuals are properly targeted under Section 702 FISA, in accordance with its supervision powers described in recitals 173-174²⁷⁹. Finally, the Director of National Intelligence (DNI) is also required to report each year the total number of Section 702 FISA targets in public annual Statistical Transparency Reports. Companies that receive Section 702 FISA directives may publish aggregate data (via transparency reports) on the requests they receive²⁸⁰.

²⁷¹ PCLOB, Section 702 Report, pp. 42-43.

²⁷² NSA targeting procedures, p. 2.

²⁷³ PCLOB, Section 702 Report, p. 46. For example, the NSA must verify that there is a connection between the target and the selector, must document the foreign intelligence information expected to be acquired, this information must be reviewed and approved by two senior NSA analysts, and the overall process will be tracked for subsequent compliance reviews by the ODNI and Department of Justice. See NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16 April 2014.

²⁷⁴ 50 U.S.C. § 1881a (h).

²⁷⁵ NSA targeting procedures, p. 8. See also PCLOB, Section 702 Report, p 46. Failure to provide a written justification constitutes a documentation compliance incident that must be reported to the FISC and Congress. See Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, p. 41 (October 2018), DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017 at p. A-6, available at https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

²⁷⁶ See U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements, at 2-3 (July 15, 2015) and the information provided in Annex VII.

²⁷⁷ See U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements, at 2-3 (15 July 2015), which provides that the government "[i]f the Government later assesses that the continued tasking of a target's selector is not expected to result in the acquisition of foreign intelligence information, prompt detasking is required, and delay may result in a reportable compliance incident". See also the information provided in Annex VII.

²⁷⁸ PCLOB, Section 702 Report, pp. 70-72; Rule 13(b) of the Rules of Procedure of the United States Intelligence Surveillance Court, available at <https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

²⁷⁹ See also DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017 at p. A-6.

²⁸⁰ 50 U.S.C. § 1874.

- (148) As regards the other legal bases to collect personal data transferred to organisations in the U.S., different limitations and safeguards apply. In general, the collection of data in bulk is specifically prohibited under Section 402 FISA (pen register and trap and trace authority) and through the use of NSL, and the use of specific ‘selection terms’ is instead required²⁸¹.
- (149) To conduct traditional individualized electronic surveillance (pursuant to Section 105 FISA), intelligence agencies must submit an application to the FISC with a statement of the facts and circumstances relied upon to justify the belief that there is probable cause that the facility is used or about to be used by a foreign power or an agent of a foreign power²⁸². The FISC will assess, among others, whether on the basis of the submitted facts there is probable cause that this is indeed the case²⁸³.
- (150) To carry out a search of premises or property that is intended to result in an inspection, seizure, etc. of information, material, or property (e.g. a computer device) on the basis of Section 301 FISA, an application for an order by the FISC is required²⁸⁴. Such application must, inter alia, show that there is probable cause that the target of the search is a foreign power or an agent of a foreign power; that the premise or property to be searched contains foreign intelligence information and that the premise to be searched is owned, used, possessed by, or is in transit to or from an (agent of a) foreign power²⁸⁵.
- (151) Similarly, the installation of pen registers or trap and trace devices (pursuant to Section 402 FISA) requires an application for an order by the FISC (or a U.S. Magistrate Judge) and the use of a specific selection term, i.e. a term that specifically identifies a person, account, etc. and is used to limit, to the greatest extent reasonably possible, the scope of the information sought²⁸⁶. This authority does not concern the contents of communications, but rather aims at information about the customer or subscriber using a service (such as name, address, subscriber number, length/type of service received, source/mechanism of payment).
- (152) Section 501 FISA²⁸⁷, which allows the collection of business records of a common carrier (i.e. any person or entity transporting people or property by land, rail, water or air for compensation), public accommodation facility (e.g. a hotel, motel or inn), vehicle rental facility, or physical storage facility (i.e. which provides space for or services related to the storage of goods and materials)²⁸⁸, also requires an application to the FISC or a Magistrate Judge. This application must specify the records sought and the specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of foreign power²⁸⁹.

²⁸¹ 50 U.S. Code § 1842(c)(3) and, as regards NSL, 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); and 18 U.S.C. § 2709(a).

²⁸² ‘An agent of a foreign power’ may include non-U.S. persons that engage in international terrorism or the international proliferation of weapons of mass destruction (including preparatory acts) (50 U.S.C. § 1801 (b)(1)).

²⁸³ 50 U.S.C. § 1804. See also § 1841(4) with respect to the choice of selection terms.

²⁸⁴ 50 U.S.C. § 1821(5).

²⁸⁵ 50 U.S.C. § 1823(a).

²⁸⁶ 50 U.S.C. § 1842 with § 1841(2) and Section 3127 of Title 18.

²⁸⁷ 50 U.S.C. § 1862.

²⁸⁸ 50 U.S.C. §§ 1861-1862.

²⁸⁹ 50 U.S.C. § 1862(b).

- (153) Finally, NSL are authorised by different statutes and allow investigating agencies to obtain certain information (not including the content of communications) from certain entities (e.g. financial institutions, credit reporting agencies, electronic communication providers) contained in credit reports, financial records and electronic subscriber and transactional records²⁹⁰. The NSL statute that authorises access to electronic communications may be used only by the FBI and requires that requests use a term that specifically identifies a person, entity, telephone number, or account and certify that the information is relevant to an authorized national security investigation to protect against international terrorism or clandestine intelligence activities²⁹¹. Recipients of an NSL have the right to challenge it in court²⁹².

3.2.1.3 Further use of the information collected

- (154) The processing of personal data collected by U.S. intelligence agencies through signals intelligence is subject to a number of safeguards.
- (155) Firstly, each intelligence agency must ensure appropriate data security and prevent access by unauthorised persons to personal data collected through signals intelligence. In this respect, different instruments, including statute, guidelines and standards further specify the minimum information security requirements that have to be put in place (e.g. multifactor authentication, encryption, etc.)²⁹³. Access to collected data must be limited to authorised, trained personnel with a need to know the information to perform their mission²⁹⁴. More generally, intelligence agencies must provide appropriate training to their employees, including on procedures for reporting and addressing violations of the law (including EO 14086)²⁹⁵.
- (156) Secondly, intelligence agencies must comply with Intelligence Community standards for accuracy and objectivity, in particular with respect to ensuring data quality and reliability, the consideration of alternative sources of information and objectivity in performing analyses²⁹⁶.
- (157) Thirdly, as regards data retention, EO 14086 clarifies that personal data of non-U.S. persons is subject to the same retention periods as the ones that apply to the data of

²⁹⁰ 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; and 18 U.S.C. § 2709.

²⁹¹ 18 U.S.C. § 2709(b).

²⁹² E.g., 18 U.S.C. § 2709(d).

²⁹³ Section 2(c)(iii)(B)(1) EO 14086. See also Title VIII of the National Security Act (detailing the requirements for access to classified information), E.O. 12333 section 1.5 (requiring the Heads of Intelligence Community Agencies to follow information sharing and security guidelines, information privacy, and other legal requirements), National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems” (directing the Committee on National Security Systems to provide system security guidance for national security systems to executive departments and agencies), and National Security Memorandum 8, “Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems” (establishing timelines and guidance for how cybersecurity requirements will be implemented for national security systems, including multifactor authentication, encryption, cloud technologies, and endpoint detection services).

²⁹⁴ Section 2(c)(iii)(B)(2) EO 14086. In addition, personal data for which no final retention determination has been made may only be accessed in order to make or support such a determination or to conduct authorised administrative, testing, development, security or oversight functions (Section 2(c)(iii)(B)(3) EO 14086).

²⁹⁵ Section 2(d)(ii) EO 14086.

²⁹⁶ Section 2(c)(iii)(C) EO 14086.

U.S. persons²⁹⁷. Intelligence agencies are required to define specific retention periods and/or the factors that must be taken into account to determine the length of applicable retention periods (e.g. whether the information is evidence of a crime; whether the information constitutes foreign intelligence information; whether the information is needed to protect the safety of persons or organisations, including victims or targets of international terrorism), which are laid down in different legal instruments²⁹⁸.

- (158) Fourthly, specific rules apply as regards the dissemination of personal data collected through signals intelligence. As a general requirement, personal data on non-U.S. persons may only be disseminated if it involves the same type of information that can be disseminated about U.S. persons, e.g. information needed to protect the safety of a person or organisation (such as targets, victims or hostages of international terrorist organisations)²⁹⁹. Moreover, personal data may not be disseminated solely because of a person's nationality or country of residence or for the purpose of circumventing the requirements of EO 14086³⁰⁰. Dissemination within the U.S. government may only take place if an authorised and trained individual has a reasonable belief that the recipient has a need to know the information³⁰¹ and will protect it appropriately³⁰². To determine whether personal data can be disseminated to recipients outside the U.S. government (including a foreign government or international organisation), the purpose of the dissemination, the nature and extent of the data being disseminated, and the potential for harmful impact on the person(s) concerned must be taken into account³⁰³.
- (159) Finally, including in order to facilitate oversight of compliance with the applicable legal requirements as well as effective redress, each intelligence agency is required under EO 14086 to keep appropriate documentation about the collection of signals intelligence. The documentation requirements cover elements such as the factual basis for the assessment that a specific collection activity is necessary to advance a validated intelligence priority³⁰⁴.
- (160) In addition to the abovementioned safeguards of EO 14086 for the use of information collected through signals intelligence, all US intelligence agencies are subject to more general requirements on purpose limitation, data minimisation, accuracy, security, retention and dissemination, following in particular from OMB Circular No. A-130,

²⁹⁷ Section 2(c)(iii)(A)(2)(a)-(c) EO 14086. More generally, each agency must put in place policies and procedures designed to minimise the dissemination and retention of personal data collected through signals intelligence (Section 2(c)(iii)(A) EO 14086).

²⁹⁸ See e.g. Section 309 of the Intelligence Authorization Act for Fiscal Year 2015; minimisation procedures adopted by individual intelligence agencies under Section 702 FISA and authorised by the FISC; procedures approved by the Attorney General and the FRA (requiring U.S. federal agencies, including national security agencies, to establish retention periods for their records that must be approved by the National Archives and Record Administration).

²⁹⁹ Section 2(c)(iii)(A)(1)(a) and 5(d) EO 14086, in conjunction with Section 2.3 EO 12333.

³⁰⁰ Section 2(c)(iii)(A)(1)(b) and (e) EO 14086.

³⁰¹ See e.g., the AGG-DOM for instance provides that the FBI may only disseminate information if the recipient has a need to know to accomplish the recipient's mission or to protect the public.

³⁰² Section 2(c)(iii)(A)(1)(c) EO 14086. Intelligence agencies may for instance disseminate information in circumstances relevant to a criminal investigation or relating to a crime, including for example by disseminating warnings of threats of killing, serious bodily injury, or kidnapping; disseminating cyber threat, incident, or intrusion response information; and notifying victims or warning potential victims of crime.

³⁰³ Section 2(c)(iii)(A)(1)(d) EO 14086.

³⁰⁴ Section 2(c)(iii)(E) EO 14086.

the E-Government Act, the Federal Records Act (see recitals 101-106) and guidance from the Committee on National Security Systems (CNSS) ³⁰⁵.

3.2.2 Oversight

- (161) The activities of U.S. intelligence agencies are subject to supervision by different bodies.
- (162) Firstly, EO 14086 requires each intelligence agency to have senior-level legal, oversight and compliance officials to ensure compliance with applicable U.S. law³⁰⁶. In particular, they must conduct periodic oversight of signals intelligence activities and ensure that any non-compliance is remedied. Intelligence agencies must provide such officials with access to all relevant information to carry out their oversight functions and may not take any actions to impede or improperly influence their oversight activities³⁰⁷. Moreover, any significant non-compliance incident³⁰⁸ identified by an oversight official or any other employee must promptly be reported to the head of the intelligence agency and the Director of National Intelligence, who must ensure that any necessary actions are taken to remediate and prevent the recurrence of the significant incident of non-compliance³⁰⁹.
- (163) This oversight function is fulfilled by officers with a designated compliance role, as well as Privacy and Civil Liberties Officers and Inspectors General³¹⁰.
- (164) As is the case with respect to criminal law enforcement authorities, Privacy and Civil Liberties Officers exist at all intelligence agencies³¹¹. The powers of these officers typically encompass the supervision of procedures to ensure that the respective department/agency is adequately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints from individuals who consider that their privacy or civil liberties have been violated (and in some cases, like the Office of the Director of National Intelligence (ODNI), may themselves have the power to investigate complaints³¹²). The heads of intelligence agencies must ensure that Privacy and Civil Liberties Officers have the resources to fulfil their mandate, are given access to any material and personnel necessary to carry out their functions, and are informed about and are consulted on proposed policy changes³¹³. Privacy and Civil Liberties Officers periodically report to Congress and the PCLOB, including on the number and nature of the complaints received by the department/agency with a

³⁰⁵ See CNSS Policy No. 22, Cybersecurity Risk Management Policy and CNSS Instruction 1253, which provides detailed guidance on security measures to be put in place for national security systems.

³⁰⁶ Section 2(d)(i)(A)-(B) EO 14086.

³⁰⁷ Sections 2(d)(i)(B)-(C) EO 14086.

³⁰⁸ I.e. a systemic or intentional failure to comply with applicable U.S. law that could impugn the reputation or integrity of an element of the Intelligence Community or otherwise call into question the propriety of an Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned, see Section 5(l) EO 14086.

³⁰⁹ Section 2(d)(iii) EO 14086.

³¹⁰ Section 2(d)(i)(B) EO 14086.

³¹¹ See 42 U.S.C. § 2000ee-1. This includes for instance the Department of State, the Department of Justice, the Department of Homeland Security, the Department of Defense, the NSA, Central Intelligence Agency (CIA), FBI and the ODNI.

³¹² See Section 3(c) EO 14086.

³¹³ 42 U.S.C. § 2000ee-1(d).

summary of the disposition of such complaints, the reviews and inquiries conducted and the impact of the activities carried out by the Officer³¹⁴.

- (165) Secondly, each intelligence agency has an independent Inspector General with the responsibility, among others, to oversee foreign intelligence activities. This includes, within the ODNI, an Office of the Inspector General of the Intelligence Community with comprehensive jurisdiction over the entire Intelligence Community which is authorised to investigate complaints or information concerning allegations of unlawful conduct, or abuse of authority, in connection with ODNI and/or Intelligence Community programs and activities³¹⁵. As is the case for criminal law enforcement authorities (see recital 109), such Inspectors General are statutorily independent³¹⁶ and responsible for conducting audits and investigations relating to the programs and operations carried out by the respective agency for national intelligence purposes, including with respect to abuse or violation of the law³¹⁷. They have access to all

³¹⁴ See 42 U.S.C. § 2000ee-1 (f)(1),(2). For example the report of the NSA’s Civil Liberties, Privacy and Transparency Office covering January 2021 – June 2021 shows that it carried out 591 reviews for civil liberties and privacy impacts in various contexts, e.g. with respect to collection activities, information-sharing arrangements and decisions, data retention decisions, etc., taking into account different factors, such as the amount and type of information associated with the activity, the individuals involved, the purpose and anticipated use for the data, the safeguards in place to mitigate potential risks to privacy, etc.

(https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Similarly, the reports of the CIA’s Office of Privacy and Civil Liberties for January – June 2019 provide information on the Office’s oversight activities, e.g. a review of compliance with Attorney General Guidelines under EO 12333 with respect to the retention and dissemination of information, guidance provided on the implementation of PPD 28 and requirements to identify and address data breaches, and reviews of the use and handling of personal information (<https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf>).

³¹⁵ This Inspector General is appointed by the President, with Senate confirmation, and can be removed only by the President.

³¹⁶ Inspectors General have secure tenure and may only be removed by the President who must communicate to Congress in writing the reasons for any such removal. This does not necessarily mean that they are completely free from instructions. In some cases, the head of the department may prohibit the Inspector General from initiating, carrying out, or completing an audit or investigation where this is considered necessary to preserve important national (security) interests. However, Congress must be informed of the exercise of this authority and on this basis could hold the respective director responsible. See, e.g. Inspector General Act of 1978, § 8 (for the Department of Defense); § 8E (for the DOJ), § 8G (d)(2)(A),(B) (for the NSA); 50. U.S.C. § 403q (b) (for the CIA); Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f) (for the Intelligence Community).

³¹⁷ Inspector General Act of 1978, as amended, Pub. L. 117-108 of 8 April 2022. For example, as explained in its semi-annual reports to Congress covering the period 1 April 2021 to 31 March 2022, the NSA Inspector General carried out evaluations of the handling of U.S. person information collected under EO 12333, the process to purge signals intelligence data, an automated targeting tool used by the NSA, and compliance with documentation and querying rules with respect to Section 702 FISA collection, and issued several recommendations in this context (see <https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d>, pp. 5-8 and <https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d×tamp=1657810395907>, pp. 10-13). See also the recent audits and investigations carried out by the Inspector General of the Intelligence Community on information security and unauthorised disclosures of classified national security information (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, pp. 8, 11 and https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, pp. 19-20).

records, reports, audits, reviews, documents, papers, recommendations or other relevant material, if need be by subpoena, and may take testimony³¹⁸. Inspectors General refer cases of suspected criminal violations for prosecution and make recommendations for corrective action to agency heads³¹⁹. While their recommendations are non-binding, their reports, including on follow-up action (or the lack thereof)³²⁰ are generally made public and sent to Congress, which can on this basis exercise its own oversight function (see recitals 168-169)³²¹.

- (166) Thirdly, the Intelligence Oversight Board (IOB), which is established within the President's Intelligence Advisory Board (PIAB), oversees compliance by U.S. intelligence authorities with the Constitution and all applicable rules³²². The PIAB is an advisory body within the Executive Office of the President that consists of 16 members appointed by the President from outside the U.S. government. The IOB consists of a maximum of five members designated by the President from among PIAB members. According to EO 12333³²³, the heads of all intelligence agencies are required to report any intelligence activity for which there is reason to believe that it may be unlawful or contrary to an Executive Order or Presidential Directive to the IOB. To ensure that the IOB has access to the information necessary to perform its functions, Executive Order 13462 directs the Director of National Intelligence and heads of intelligence agencies to provide any information and assistance the IOB determines is needed to perform its functions, to the extent permitted by law³²⁴. The IOB is in turn required to inform the President about intelligence activities it believes may be in violation of U.S. law (including Executive Orders) and are not being adequately addressed by the Attorney General, Director of National Intelligence or the head of an intelligence agency³²⁵. In addition, the IOB is required to inform the Attorney General about possible violations of criminal law.
- (167) Fourthly, intelligence agencies are subject to oversight by the PCLOB. According to its founding statute, the PCLOB is entrusted with responsibilities in the field of counterterrorism policies and their implementation, with a view to protect privacy and civil liberties. In its review of intelligence agencies actions, it can access all relevant agency records, reports, audits, reviews, documents, papers and recommendations,

³¹⁸ See Inspector General Act of 1978, § 6.

³¹⁹ See *ibid.* §§ 4, 6-5.

³²⁰ As regards the follow-up that is provided to reports and recommendations of Inspectors General, see e.g. the response to a report of the DoJ Inspector General that found that the FBI was not sufficiently transparent with the FISC in applications from 2014 to 2019, which led to reforms to enhance compliance, oversight, and accountability at the FBI (e.g. the FBI Director [ordered](https://www.justice.gov/opa/pr/departments-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance) more than 40 corrective actions, including 12 specific to the FISA process relating to documentation, supervision, file maintenance, training and audits) (see <https://www.justice.gov/opa/pr/departments-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance> and <https://oig.justice.gov/reports/2019/o20012.pdf>). See for instance also the DoJ Inspector General's audit of the FBI Office of the General Counsel's roles and responsibilities in overseeing compliance with applicable laws, policies, and procedures relating to the FBI's national security activities and Appendix 2, which includes a letter from the FBI accepting all recommendations. In this respect, Appendix 3 provides an overview of the follow-up action and information the Inspector General required from the FBI in order to be able to close its recommendations (<https://oig.justice.gov/sites/default/files/reports/22-116.pdf>).

³²¹ See Inspector General Act of 1978, §§ 4(5), 5.

³²² See EO 13462.

³²³ Section 1.6(c) EO 12333.

³²⁴ Section 8(a) EO 13462.

³²⁵ Section 6(b) EO 13462.

including classified information, conduct interviews and hear testimony³²⁶. It receives reports from the civil liberties and privacy officers of several federal departments/agencies³²⁷, may issue recommendations to the government and intelligence agencies, and regularly reports to Congressional committees and the President³²⁸. Reports of the Board, including the ones to Congress, must be made publicly available to the greatest extent possible³²⁹. The PCLOB has issued several oversight and follow-up reports, including an analysis of the programs run on the basis of Section 702 FISA and the protection of privacy in this context, the implementation of PPD 28 and EO 12333³³⁰. The PCLOB is also charged with carrying out specific oversight functions as regards the implementation of EO 14086, in particular by reviewing whether agency procedures are consistent with the EO (see recital 126) and evaluating the correction functioning of the redress mechanism (see recital 194).

- (168) Fifthly, in addition to the oversight mechanisms within the executive branch, specific Committees in the U.S. Congress (the House and Senate Intelligence and Judiciary Committees) have oversight responsibilities regarding all U.S. foreign intelligence activities. Members of these Committees have access to classified information as well as intelligence methods and programs³³¹. The Committees exercise their oversight functions in different ways, in particular through hearings, investigations, reviews and reports³³².
- (169) The Congressional Committees receive regular reports on intelligence activities, including from the Attorney General, the Director of National Intelligence, intelligence agencies and other oversight bodies (e.g. Inspectors General), see recitals 164-165. In particular, according to the National Security Act, "[t]he President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant

³²⁶ 42 U.S.C. § 2000ee (g).

³²⁷ See 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). These include at least the Department of Justice, the Department of Defense, the Department of Homeland Security, the Director of National Intelligence and the Central Intelligence Agency, plus any other department, agency or element of the executive branch designated by the PCLOB to be appropriate for coverage.

³²⁸ 42 U.S.C. §2000ee (e).

³²⁹ 42 U.S.C. § 2000ee (f).

³³⁰ Available at <https://www.pclob.gov/Oversight>.

³³¹ 50 U.S.C. § 3091.

³³² For example, the Committees organise thematic hearings (see e.g. a recent hearing of the House Judiciary Committee on “digital dragnets”, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>, and a hearing of the House Intelligence Committee on the use of AI by the Intelligence Community, <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263>) regular oversight hearings, e.g. of the FBI and DoJ national security division, see <https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation>; <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966> and <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899>. As an example of an investigation, see the Senate Intelligence Committee investigation of Russian interference in the 2016 U.S. elections, see <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures>. In terms of reporting, see e.g. the overview of the Committee’s (oversight) activities in the report of the Senate Intelligence Committee covering the period 4 January 2019 – 3 January 2021 to the Senate, <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4>.

anticipated intelligence activity as required by this subchapter”³³³. In addition, “[t]he President shall ensure that any illegal intelligence activity is reported promptly to the congressional intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity”³³⁴.

- (170) Moreover, additional reporting requirements follow from specific statutes. In particular, FISA requires the Attorney General to “fully inform” the Senate and House Intelligence and Judiciary Committees regarding the government’s activities under certain sections of FISA³³⁵. It also requires the government to provide the Congressional committees with copies of all decisions, orders, or opinions of the FISC or FISCER that include “significant construction or interpretation” of FISA provisions. As regards surveillance under Section 702 FISA, parliamentary oversight is exercised through statutorily required reports to the Intelligence and Judiciary Committees, as well as frequent briefings and hearings. These include a semi-annual report by the Attorney General describing the use of Section 702 FISA, with supporting documents, including Department of Justice and ODNI compliance reports and a description of any incidents of non-compliance³³⁶, and a separate semi-annual assessment by the Attorney General and the DNI documenting compliance with the targeting and minimization procedures³³⁷.
- (171) In addition, FISA requires the U.S. government to disclose to Congress (and the public) each year the number of FISA orders sought and received, as well as estimates of the number of U.S. and non-U.S. persons targeted by surveillance, among others³³⁸. The Act also requires additional public reporting about the number of NSL issued, again both with regard to U.S. and non-U.S. persons (while at the same time allowing the recipients of FISA orders and certifications, as well as NSL requests, to issue transparency reports under certain conditions)³³⁹.
- (172) More generally, the U.S. Intelligence Community undertakes various efforts to provide transparency about its (foreign) intelligence activities. For example, in 2015, the ODNI adopted Principles of Intelligence Transparency and a Transparency Implementation Plan, and directed each intelligence agency to designate an Intelligence Transparency Officer to foster transparency and lead transparency initiatives³⁴⁰. As part of these efforts, the Intelligence Community has made and continues to make declassified parts of policies, procedures, oversight reports, reports on activities under Section 702 FISA and EO 12333, FISC decisions and other

³³³ See 50 U.S.C. § 3091(a)(1). This provision contains the general requirements as regards Congressional oversight in the area of national security.

³³⁴ See 50 U.S.C. §3091(b).

³³⁵ See 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

³³⁶ See 50 U.S.C. § 1881f.

³³⁷ See 50 U.S.C. § 1881a(l)(1).

³³⁸ 50 U.S.C. § 1873(b). In addition, according to Section 402, “the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term “specific selection term”, and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion”.

³³⁹ 50 U.S.C. §§ 1873(b)(7) and 1874.

³⁴⁰ <https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic>.

materials public, including on a dedicated webpage ‘IC on the Record’, managed by ODNI³⁴¹.

- (173) Finally, the collection of personal data pursuant to Section 702 FISA is, in addition to the supervision by oversight bodies mentioned in recitals 162-168, subject to oversight by the FISC³⁴². Pursuant to Rule 13 of the FISC Rules of Procedure, compliance officers in U.S. intelligence agencies are required to report any violations of FISA 702 targeting, minimization, and querying procedures to the DoJ and ODNI, who in turn report them to the FISC. Moreover, the DoJ and ODNI submit semi-annual joint oversight assessment reports to the FISC, which identify targeting compliance trends; provide statistical data; describe categories of compliance incidents; describe in detail the reasons certain targeting compliance incidents occurred, and outline the measures intelligence agencies have taken to avoid recurrence³⁴³.
- (174) Where necessary (e.g. if violations of targeting procedures are identified), the Court may order the relevant intelligence agency to take remedial action³⁴⁴. The remedies in question may range from individual to structural measures, e.g. from terminating data acquisition and deleting of unlawfully obtained data to a change in the collection practice, including in terms of guidance and training for staff³⁴⁵. Moreover, during its annual review of Section 702 certifications, the FISC considers non-compliance incidents to determine if the submitted certifications comply with FISA requirements. Similarly, if the FISC finds that the government’s certifications were not sufficient, including because of particular compliance incidents, it can issue a so-called ‘deficiency order’ requiring the government to remedy the violation within 30 days or requiring the government to cease or not begin implementing the Section 702 certification. Finally, the FISC assesses trends it observes in compliance issues and

³⁴¹ See ‘IC on the Record’, available at <https://icontherecord.tumblr.com/>.

³⁴² In the past, the FISC concluded that “[i]t is apparent to the Court that the implementing agencies, as well as [ODNI] and [DOJ’s National Security Division], devote substantial resources to their compliance and oversight responsibilities under Section 702. As a general rule, instances of non-compliance are identified promptly and appropriate remedial actions are taken, to include purging information that was improperly obtained or otherwise subject to destruction requirements under applicable procedures”. FISA Court, Memorandum Opinion and Order [caption redacted] (2014), available at <https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>.

³⁴³ See, e.g., DOJ/ODNI FISA 702 Compliance Report to FISC for June 2018 – Nov. 2018 at 21-65.

³⁴⁴ 50 U.S.C. § 1803(h). See also PCLOB, Section 702 Report, p. 76. In addition, see FISC Memorandum Opinion and Order of 3 October 2011 as an example of a deficiency order in which the government was ordered to correct the identified deficiencies within 30 days. Available at <https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>. See Walton Letter, Section 4, pp. 10 -11. See also FISC Opinion of 18 October 2018, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, as confirmed by the Foreign Intelligence Court of Review in its Opinion of 12 July 2019, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, in which the FISC inter alia ordered the government to comply with certain notification, documentation and reporting requirements towards the FISC.

³⁴⁵ See e.g. FISC, Memorandum Opinion and Order at 76 (6 Dec. 2019) (Authorised for Public Release on 4 September 2020), in which the FISC directed the government to submit a written report by 28 February 2020 on the steps the government was taking to improve processes for identifying and removing reports derived from FISA 702 information that were recalled for compliance reasons, as well as on other matters. See also Annex VII.

may require changes to procedures or additional oversight and reporting to address compliance trends³⁴⁶.

3.2.3 Redress

- (175) As explained in more detail in this section, a number of avenues in the United States provide Union data subjects with the possibility to bring legal action before an independent and impartial tribunal with binding powers. Together, they allow individuals to have access to their personal data, to have the lawfulness of government access to their data reviewed and, if a violation is found, to have such violation remedied, including through the rectification or erasure of their personal data.
- (176) First, a specific redress mechanism is established, under EO 14086, complemented by the AG Regulation establishing the Data Protection Review Court, to handle and resolve complaints from individuals concerning U.S. signals intelligence activities. Any individual in the EU is entitled to submit a complaint to the redress mechanism concerning an alleged violation of U.S. law governing signals intelligence activities (e.g. EO 14086, Section 702 FISA, EO 12333) that adversely affects their privacy and civil liberties interests³⁴⁷. This redress mechanism is available to individuals from countries or regional economic integration organisations that have been designated by the U.S. Attorney General as ‘qualifying states’³⁴⁸. On 30 June 2023, the European Union and the three European Free Trade Association countries that together constitute the European Economic Area have been designated by the Attorney General under Section 3(f) EO 14086 as a ‘qualifying state’³⁴⁹. This designation is without prejudice to Article 4(2) of the Treaty on the European Union.
- (177) A Union data subject who wishes to lodge such a complaint must submit it to a supervisory authority in an EU Member State competent for the oversight of the processing of personal data by public authorities (a DPA)³⁵⁰. This ensures easy access to the redress mechanism by allowing individuals to turn to an authority ‘close to home’ and with which they can communicate in their own language. After the requirements for filing a complaint referred to in recital 178 have been verified, the competent DPA will channel, via the secretariat of the European Data Protection Board, the complaint to the redress mechanism.
- (178) Bringing a complaint to the redress mechanism is subject to low admissibility requirements, as individuals do not need to demonstrate that their data has in fact been subject to U.S. signals intelligence activities³⁵¹. At the same time, to provide a starting point for the redress mechanism to carry out a review, certain basic information must be provided, e.g. regarding the personal data reasonably believed to have been

³⁴⁶ See Annex VII.

³⁴⁷ See Section 4(k)(iv) EO 14086, which provides that a complaint to the redress mechanism must be brought by a complainant acting on his/her own behalf (i.e. not as a representative of a government, nongovernmental or intergovernmental organisation). The notion of “adversely affected” does not require the complainant to meet a certain threshold in order to have access to the redress mechanism (see recital 178 in this regard). Rather, it clarifies that the ODNI CLPO and DPRC have the authority to remediate violations of U.S. law governing signals intelligence activities that adversely affect a complainant’s individual privacy and civil liberties interests. Conversely, violations of requirements under applicable US law that are not designed to protect individuals (e.g. budgetary requirements), would fall outside the jurisdiction of the ODNI CLPO and DPRC.

³⁴⁸ Section 3(f) EO 14086.

³⁴⁹ <https://www.justice.gov/opcl/executive-order-14086>.

³⁵⁰ Section 4(d)(v) EO 14086.

³⁵¹ See Section 4(k)(i)-(iv) EO 14086.

transferred to the U.S. and the means by which it was believed to have been transferred; the identities of the U.S. Government entities believed to be involved in the alleged violation (if known); the basis for alleging that a violation of U.S. law occurred (although this again does not require showing that personal data was in fact collected by U.S. intelligence agencies) and the nature of the relief sought.

- (179) The initial investigation of complaints to this redress mechanism is carried out by the ODNI CLPO, whose existing statutory role and powers have been expanded for those specific actions taken pursuant to EO 14086³⁵². Within the Intelligence Community, the CLPO is, *inter alia*, responsible for ensuring that the protection of civil liberties and privacy is appropriately incorporated in policies and procedures of the ODNI and intelligence agencies; overseeing compliance by the ODNI with applicable civil liberties and privacy requirements; and conducting privacy impact assessments³⁵³. The ODNI CLPO can only be dismissed by the Director of National Intelligence for cause, *i.e.* in case of misconduct, malfeasance, breach of security, neglect of duty, or incapacity³⁵⁴.
- (180) When conducting its review, the ODNI CLPO has access to the information for his/her assessment and can rely on the compelled assistance of Privacy and Civil Liberties Officers in the different intelligence agencies³⁵⁵. Intelligence agencies are prohibited from impeding or improperly influencing the ODNI CLPO's reviews. This includes the Director of National Intelligence who must not interfere with the review³⁵⁶. When reviewing a complaint, the ODNI CLPO must "apply the law impartially", having regard to both the national security interests in signal intelligence activities and privacy protections³⁵⁷.
- (181) As part of its review, the ODNI CLPO determines whether a violation of applicable U.S. law has occurred and, if that is the case, decides on an appropriate remediation³⁵⁸. The latter refers to measures that fully redress an identified violation, such as terminating unlawful acquisition of data, deleting unlawfully collected data, deleting the results of inappropriately conducted queries of otherwise lawfully collected data, restricting access to lawfully collected data to appropriately trained personnel, or recalling intelligence reports containing data acquired without lawful authorization or that were unlawfully disseminated³⁵⁹. Decisions of the ODNI CLPO on individual complaints (including on the remediation) are binding on intelligence agencies concerned³⁶⁰.
- (182) The ODNI CLPO must maintain documentation of its review and produce a classified decision explaining the basis for its factual findings, the determination with respect to whether a covered violation occurred and the determination of the appropriate remediation³⁶¹. If the ODNI CLPO's review reveals a violation of any authority subject to the oversight of the FISC, the CLPO must also provide a classified report to

³⁵² Section 3(c)(iv) EO 14086. See also National Security Act 1947, 50 U.S.C. §403-3d, Section 103D concerning the role of the CLPO within the ODNI.

³⁵³ 50 U.S.C § 3029 (b).

³⁵⁴ Section 3(c)(iv) EO 14086.

³⁵⁵ Section 3(c)(iii) EO 14086.

³⁵⁶ Section 3(c)(iv) EO 14086.

³⁵⁷ Section 3(c)(i)(B)(i) and (iii) EO 14086.

³⁵⁸ Section 3(c)(i) EO 14086.

³⁵⁹ Section 4(a) EO 14086.

³⁶⁰ Section 3(c)(d) EO 14086.

³⁶¹ Section 3(c)(i)(F)-(G) EO 14086.

the Assistant Attorney General for National Security, who in turn under an obligation to report the non-compliance to the FISC, which can take further enforcement action (in accordance with the procedure described in recitals 173-174)³⁶².

- (183) Once the review is completed, the ODNI CLPO informs the complainant, through the national authority, that “the review either did not identify any covered violations or the ODNI CLPO issued a determination requiring appropriate remediation”³⁶³. This allows protection of the confidentiality of activities conducted to protect national security, while providing the individuals with a decision confirming that their complaint has been duly investigated and adjudicated. This decision can moreover be challenged by the individual. To this end, (s)he will be informed of the possibility to appeal to the DPRC for a review of the CLPO’s determinations (see recitals 184 and further) and that, in case the Court would be seized, a special advocate will be selected to advocate regarding the complainant’s interest³⁶⁴.
- (184) Any complainant, as well as each element of the Intelligence Community, may seek review of the ODNI CLPO’s decision before the Data Protection Review Court (DPRC). Such applications for review must be submitted within 60 days after receiving the notification from the ODNI CLPO that its review is complete and include any information the individual wishes to provide to the DPRC (e.g. arguments on questions of law or the application of law to the facts of the case)³⁶⁵. Union data subjects may again submit their application to the competent DPA (see recital 177).
- (185) The DPRC is an independent tribunal established by the Attorney General on the basis of EO 14086³⁶⁶. It consists of at least six judges, appointed by the Attorney General in consultation with the PCLOB, the Secretary of Commerce and the Director of National Intelligence for renewable terms of four years³⁶⁷. The appointment of judges by the Attorney General is informed by the criteria used by the executive branch when assessing candidates for the federal judiciary, giving weight to any prior judicial experience³⁶⁸. In addition, the judges must be legal practitioners (i.e. active members in good standing of the bar and duly licensed to practice law) and have appropriate experience in privacy and national security law. The Attorney General must endeavour to ensure that at least half of the judges at any given time have prior judicial experience and all judges must hold security clearances to be able to access classified national security information³⁶⁹.
- (186) Only individuals who meet the qualifications mentioned in recital 185 and are not employees of the executive branch at the time of their appointment or in the preceding two years can be appointed to the DPRC. Similarly, during their term of office at the

³⁶² See also Section 3(c)(i)(D) EO 14086.

³⁶³ Section 3(c)(i)(E)(1) EO 14086.

³⁶⁴ Sections 3(c)(i)(E)(2)-(3) EO 14086.

³⁶⁵ Sections 201.6(a)-(b) AG Regulation.

³⁶⁶ Section 3(d)(i) and the AG Regulation. The Supreme Court of the United States has recognised the possibility for the Attorney General to establish independent bodies with decision-making power, including to adjudicate individual cases, see in particular *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954) and *United States v. Nixon*, 418 U.S. 683, 695 (1974). Compliance with the different requirements of EO 14086, e.g. the criteria and procedure for appointment and dismissal of DPRC judges, is notably subject to the supervision of the Inspector General of the Department of Justice (see also recital 109 on the statutory authority of Inspectors General).

³⁶⁷ Section 3(d)(i)(A) EO 14086 and Section 201.3(a) AG Regulation.

³⁶⁸ Section 201.3(b) AG Regulation.

³⁶⁹ Section 3(d)(i)(B) EO 14086.

DPRC, the judges may not have any official duties or employment within the U.S. Government (other than as judges at the DPRC)³⁷⁰.

- (187) The independence of the adjudication process is achieved through a number of guarantees. In particular, the executive branch (the Attorney General and intelligence agencies) are barred from interfering with or improperly influencing the DPRC's review³⁷¹. The DPRC itself is required to impartially adjudicate cases³⁷² and operates according to its own rules of procedure (adopted by majority vote). Moreover, DPRC judges may be dismissed only by the Attorney General and only for cause (i.e. misconduct, malfeasance, breach of security, neglect of duty or incapacity), after taking due account of the standards applicable to federal judges laid down in the Rules for Judicial-Conduct and Judicial-Disability Proceedings³⁷³.
- (188) Applications to the DPRC are reviewed by panels of three judges, including a presiding judge, who must act in accordance with the Code of Conduct for U.S. Judges³⁷⁴. Each panel is assisted by a Special Advocate³⁷⁵, who has access to all information pertaining to the case, including classified information³⁷⁶. The role of the Special Advocate is to ensure that the complainant's interests are represented and that the DPRC panel is well informed about all relevant issues of law and fact³⁷⁷. To further inform its position on an application for review to the DPRC by an individual, the Special Advocate can seek information from the complainant through written questions³⁷⁸.

³⁷⁰ Section 3(d)(i)(A) EO 14086 and Section 201.3(a) and (c) AG Regulation. Individuals appointed to the DPRC may participate in extrajudicial activities, including business, financial activities, non-profit fundraising and fiduciary activities, as well as the practice of law, as long as such activities do not interfere with the impartial performance of their duties or the effectiveness or independence of the DPRC (Section 201.7(c) AG Regulation).

³⁷¹ Sections 3(d)(iii)-(iv) EO 14086 and Section 201.7(d) AG Regulation.

³⁷² Section 3(d)(i)(D) EO 14086 and Section 201.9 AG Regulation.

³⁷³ Section 3(d)(iv) EO 14086 and Section 201.7(d) AG Regulation. See also *Bumap v. United States*, 252 U.S. 512, 515 (1920), which confirmed the long-standing principle in US law that the power of removal is incident to the power to appoint (as also recalled by the Office of Legal Counsel of the DoJ in *The Constitutional Separation of Powers Between the President and Congress*, 20 Op. O.L.C. 124, 166 (1996)).

³⁷⁴ Section 3(d)(i)(B) EO 14086 and Section 201.7(a)-(c) AG Regulation. The Office of Privacy and Civil Liberties of the Department of Justice (OPCL), which is responsible for providing administrative support to the DPRC and the Special Advocates (see Section 201.5 AG Regulation), selects a three-person panel on a rotating basis, seeking to ensure that each panel has at least one judge with prior judicial experience (if none of the judges on the panel has such experience, the presiding judge will be the judge first selected by the OPCL).

³⁷⁵ Section 201.4 AG Regulation. At least two Special Advocates are appointed by the Attorney General, in consultation with the Secretary of Commerce, the Director of National intelligence, and the PCLOB, for two-renewable terms. Special Advocates must have appropriate experience in the field of privacy and national security law, be experienced attorneys, active members in good standing of the bar and duly licensed to practice law. In addition, at the time of their initial appointment, they must not have been employees of the Executive Branch for the preceding two years. For each review of an application, the presiding judge selects a Special Advocate to assist the panel, see Section 201.8(a) AG Regulation.

³⁷⁶ Section 201.8(c) and 201.11 AG Regulation.

³⁷⁷ Section 3(d)(i)(C) EO 14086 and Section 201.8(e) AG Regulation. The Special Advocate does not act as an agent of or have an attorney-client relationship with the complainant.

³⁷⁸ See Section 201.8(d)(e) AG Regulation. Such questions are first reviewed by the OPCL, in consultation with the relevant Intelligence Community element, with a view to identify and exclude any classified or privileged or protected information before forwarding it to complainant. Additional information received by the Special Advocate in response to such questions is included in the submissions of the Special Advocate to the DPRC.

- (189) The DPRC reviews the determinations made by the ODNI CLPO (both whether a violation of applicable U.S. law occurred and as regards the appropriate remediation) based, at a minimum, on the record of the ODNI CLPO’s investigation, as well as any information and submissions provided by the complainant, the Special Advocate or an intelligence agency³⁷⁹. A DPRC panel has access to all information necessary to conduct a review, which it may obtain through the ODNI CLPO (the panel may e.g. request the CLPO to supplement its record with additional information or factual findings if necessary to carry out the review)³⁸⁰.
- (190) When concluding its review, the DPRC may (1) decide that there is no evidence indicating that signals intelligence activities occurred involving personal data of the complainant, (2) decide that the ODNI CLPO’s determinations were legally correct and supported by substantial evidence, or (3) if the DPRC disagrees with the determinations of the ODNI CLPO (whether a violation of applicable U.S. law occurred or the appropriate remediation), issue its own determinations³⁸¹.
- (191) In all cases, the DPRC adopts a written decision by majority vote. In case the review reveals a violation of the applicable rules, the decision will specify any appropriate remediation, which includes deleting unlawfully collected data, deleting the results of inappropriately conducted queries, restricting access to lawfully collected data to appropriately trained personnel, or recalling intelligence reports containing data acquired without lawful authorization or that were unlawfully disseminated³⁸². The decision of the DPRC is binding and final with respect to the complaint before it³⁸³. Moreover, if the review reveals a violation of any authority subject to the oversight of the FISC, the DPRC must also provide a classified report to the Assistant Attorney General for National Security, who in turn is under an obligation to report the non-compliance to the FISC, which can take further enforcement action (in accordance with the procedure described in recitals 173-174)³⁸⁴.
- (192) Each decision of a DPRC panel is transmitted to the ODNI CLPO³⁸⁵. In cases where the DPRC’s review was triggered by an application from the complainant, the complainant is notified through the national authority that the DPRC completed its review and that “the review either did not identify any covered violations or the DPRC issued a determination requiring appropriate remediation”³⁸⁶. The Office of Privacy

³⁷⁹ Section 3(d)(i)(D) EO 14086.

³⁸⁰ Section 3(d)(iii) EO 14086 and Section 201.9(b) AG Regulation.

³⁸¹ Section 3(d)(i)(E) EO 14086 and Section 201.9(c)-(e) AG Regulation. According to the definition of ‘appropriate remediation’, in Section 4(a) EO 14086, the DPRC must take into account “the ways that a violation of the kind identified have customarily been addressed” when deciding on a remedial measure to fully address a violation, i.e. the DPRC will consider, among other factors, how similar compliance issues were remedied in the past to ensure that the remedy is effective and appropriate.

³⁸² Section 4(a) EO 14086.

³⁸³ Section 3(d)(ii) EO 14086 and Section 201.9(g) AG Regulation. Given that the decision of the DPRC is final and binding, no other executive or administrative institution/body (including the President of the United States) can overrule the DPRC’s decision. This was also confirmed in case law of the Supreme Court, which clarified that, by delegating the Attorney General’s unique authority within the Executive Branch to issue binding decisions to an independent body, the Attorney General denies himself the ability to dictate the decision of that body in any way (see *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954)).

³⁸⁴ Section 3(d)(i)(F) EO 14086 and Section 201.9(i) AG Regulation.

³⁸⁵ Section 201.9(h) AG Regulation.

³⁸⁶ Section 3(d)(i)(H) EO 14086 and Section 201.9(h) AG Regulation. As regards the nature of the notification see Section 201.9 (h)(3) AG Regulation.

and Civil Liberties of the DoJ maintains a record of all information reviewed by the DPRC and all decisions issued, which is made available for consideration as non-binding precedent for future DPRC panels³⁸⁷.

- (193) The DoC is also required to maintain a record for each complainant who submitted a complaint³⁸⁸. To enhance transparency, the DoC must, at least every five years, contact relevant intelligence agencies to verify whether information pertaining to a review by the DPRC has been declassified³⁸⁹. If this is the case, the individual will be notified that such information may be available under applicable law (i.e. that (s)he may request access to under the Freedom of Information Act, see recital 199).
- (194) Finally, the correct functioning of this redress mechanism will be subject to regular and independent evaluation. More specifically, pursuant to EO 14086, the functioning of the redress mechanism is subject to annual review by the PCLOB, an independent body (see recital 110)³⁹⁰. As part of this review, the PCLOB will, inter alia, assess whether the ODNI CLPO and DPRC has processed complaints in a timely manner; whether they have obtained full access to necessary information; whether the substantive safeguards of EO 14086 have been properly considered in the review process; and whether the Intelligence Community has fully complied with determinations made by the ODNI CLPO and DPRC. The PCLOB will produce a report on the outcome of its review to the President, Attorney General, Director of National Intelligence, head of intelligence agencies, the ODNI CLPO and congressional intelligence committees, that will also be made public in an unclassified version – and will in turn feed into the periodic review of the functioning of the present Decision that will be conducted by the Commission. The Attorney General, Director of National Intelligence, ODNI CLPO and heads of intelligence agencies are required to implement or otherwise address all recommendations included in such reports. In addition, the PCLOB will make an annual public certification as to whether the redress mechanism is processing complaints consistent with the requirements of EO 14086.
- (195) In addition to the specific redress mechanism established under EO 14086, redress avenues are available to all individuals (irrespective of nationality or place of residence) before ordinary U.S. courts³⁹¹.
- (196) In particular, FISA and a related statute provides the possibility for individuals to bring a civil action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed³⁹²; to sue U.S.

³⁸⁷ Section 201.9(j) Ag Regulation.

³⁸⁸ Section 3(d)(v)(A) EO 14086.

³⁸⁹ Section 3(d)(v) EO 14086.

³⁹⁰ Section 3(e) EO 14086. See also

[https://documents.pcllob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20\(FINAL\).pdf](https://documents.pcllob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf).

³⁹¹ Access to these avenues is subject to the showing of ‘standing’. This standard, which applies to any individual regardless of nationality, stems from the ‘case or controversy’ requirement of the U.S. Const., Article III. According to the Supreme Court, this requires that (1) the individual has suffered an ‘injury in fact’ (i.e. an injury of a legally protected interested that is concrete and particularised and actual or imminent), (2) there is a causal connection between the injury and the conduct challenged before the court, and (3) it is likely, rather than speculative, that a favourable decision by the court will address the injury (see *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992)).

³⁹² 18 U.S.C. § 2712.

government officials acting in their personal capacity for money damages³⁹³; and to challenge the legality of surveillance (and seek to suppress the information) in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the U.S.³⁹⁴. More generally, if the government intends to use information obtained during intelligence operations against a suspect in a criminal case, constitutional and statutory requirements³⁹⁵ impose obligations to disclose certain information so the defendant can challenge the legality of the Government's collection and use of the evidence.

- (197) Moreover, there are several specific avenues to seek legal recourse against government officials for unlawful government access to, or use of personal data, including for purported national security purposes (i.e. the Computer Fraud and Abuse Act³⁹⁶; Electronic Communications Privacy Act³⁹⁷; and Right to Financial Privacy Act³⁹⁸). All of these legal actions concern specific data, targets and/or types of access (e.g. remote access of a computer via the internet) and are available under certain conditions (e.g. intentional/wilful conduct, conduct outside of official capacity, harm suffered).
- (198) A more general redress possibility is offered by the APA³⁹⁹, according to which “any person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action”, is entitled to seek judicial review⁴⁰⁰. This includes the possibility to ask the court to “hold unlawful and set aside agency action, findings, and conclusions found to be [...] arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law”⁴⁰¹. For example, a federal appellate court ruled on an APA claim in 2015 that the U.S. government's bulk collection of telephony metadata was not authorised by Section 501 FISA⁴⁰².
- (199) Finally, in addition to the redress avenues mentioned in recitals 176-198, any individual has the right to seek access to existing federal agency records under FOIA, including where these contain the individual's personal data⁴⁰³. Gaining such access can also facilitate bringing proceedings before ordinary courts, including in support of showing standing. Agencies may withhold information that falls within certain enumerated exceptions, including access to classified national security information and information concerning law enforcement investigations⁴⁰⁴, but complainants who

³⁹³ 50 U.S.C. § 1810.

³⁹⁴ 50 U.S.C. § 1806.

³⁹⁵ See, respectively, *Brady v. Maryland*, 373 U.S. 83 (1963) and the Jencks Act, 18 U.S.C. § 3500.

³⁹⁶ 18 U.S.C. § 1030.

³⁹⁷ 18 U.S.C. §§ 2701-2712.

³⁹⁸ 12 U.S.C. § 3417.

³⁹⁹ 5 U.S.C. § 702.

⁴⁰⁰ Generally, only “final” agency action — rather than “preliminary, procedural, or intermediate” agency action — is subject to judicial review. See 5 U.S.C. § 704.

⁴⁰¹ 5 U.S.C. § 706(2)(A).

⁴⁰² *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015), The bulk telephony collection program challenged in these cases was terminated by the USA FREEDOM Act in 2015.

⁴⁰³ 5 U.S.C. § 552. Similar laws exist at State level.

⁴⁰⁴ If this is the case, the individual will normally only receive a standard reply by which the agency declines either to confirm or deny the existence of any records. See *ACLU v CIA*, 710 F.3d 422 (D.C. Cir. 2014). The criteria for and duration of classification are laid down in Executive Order 13526, which provides, as a general rule, that a specific date or event for declassification must be established based on the duration of the national security sensitivity of the information, at which time the information must be automatically declassified (see Section 1.5 of EO 13526).

are dissatisfied with the response have the possibility to challenge it by seeking administrative and, subsequently, judicial review (before federal courts)⁴⁰⁵.

- (200) It follows from the above that when U.S. law enforcement and national security authorities access personal data falling within the scope of this Decision, such access is governed by a legal framework that lays down the conditions under which access can take place and ensures that access and further use of the data is limited to what is necessary and proportionate to the public interest objective pursued. These safeguards can be invoked by individuals who enjoy effective redress rights.

4. CONCLUSION

- (201) The Commission considers that the United States – through the Principles issued by the U.S. DoC – ensures a level of protection for personal data transferred from the Union to certified organisations in the United States under the EU-U.S. Data Privacy Framework that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679.
- (202) Moreover, the Commission considers that the effective application of the Principles is guaranteed by transparency obligations and the administration of the DPF by the DoC. In addition, taken as a whole, the oversight mechanisms and redress avenues in U.S. law enable infringements of the data protection rules to be identified and punished in practice and offer legal remedies to the data subject to obtain access to personal data relating to him/her and, eventually, the rectification or erasure of such data.
- (203) Finally, on the basis of the available information about the U.S. legal order, including the information contained in Annexes VI and VII, the Commission considers that any interference in the public interest, in particular for criminal law enforcement and national security purposes, by U.S. public authorities with the fundamental rights of the individuals whose personal data are transferred from the Union to the United States under the EU-U.S. Data Privacy Framework, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists. Therefore, in the light of the above findings, it should be decided that the United States ensures an adequate level of protection within the meaning of Article 45 of Regulation (EU) 2016/679, interpreted in light of the Charter of Fundamental Rights of the European Union, for personal data transferred from the European Union to organisations certified under the EU-U.S. Data Privacy Framework.
- (204) Given that the limitations, safeguards and redress mechanism established by EO 14086 are essential elements of the U.S. legal framework on which the Commission's assessment is based, the adoption of this Decision is notably based on the adoption of updated policies and procedures to implement EO 14086 by all U.S. intelligence agencies and the designation of the Union as a qualifying organisation for the purpose of the redress mechanism that have taken place respectively on 3 July 2023 (see recital 126) and 30 June 2023 (see recital 176).

5. EFFECTS OF THIS DECISION AND ACTION OF DATA PROTECTION AUTHORITIES

⁴⁰⁵ The court makes a de novo determination of whether records are lawfully withheld and can compel the government to provide access to records (5 U.S.C. § 552(a)(4)(B)).

- (205) Member States and their organs are required to take the measures necessary to comply with acts of the Union institutions, as the latter are presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality.
- (206) Consequently, a Commission adequacy decision adopted pursuant to Article 45(3) of Regulation (EU) 2016/679 is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities. In particular, transfers from a controller or processor in the Union to certified organisations in the United States may take place without the need to obtain any further authorisation.
- (207) It should be recalled that, pursuant to Article 58(5) of Regulation (EU) 2016/679 and as explained by the Court of Justice in the *Schrems* judgment⁴⁰⁶, where a national data protection authority questions, including upon a complaint, the compatibility of a Commission adequacy decision with the fundamental rights of the individual to privacy and data protection, national law must provide it with a legal remedy to put those objections before a national court which may be required to make a reference for a preliminary ruling to the Court of Justice⁴⁰⁷.

6. MONITORING AND REVIEW OF THIS DECISION

- (208) According to the case law of the Court of Justice⁴⁰⁸, and as recognised in Article 45(4) of Regulation (EU) 2016/679, the Commission should continuously monitor relevant developments in the third country after the adoption of an adequacy decision in order to assess whether the third country still ensures an essentially equivalent level of protection. Such a check is required, in any event, when the Commission receives information giving rise to a justified doubt in that respect.
- (209) Therefore, the Commission should on an on-going basis monitor the situation in the United States as regards the legal framework and actual practice for the processing of personal data as assessed in this Decision. To facilitate this process, the U.S. authorities should promptly inform the Commission of material developments in the U.S. legal order that have an impact on the legal framework that is the object of this Decision, as well as any evolution in practices related to the processing of the personal data assessed in this Decision, both as regards the processing of personal data by certified organisations in the United States and the limitations and safeguards applicable to access to personal data by public authorities.
- (210) Moreover, in order to allow the Commission to effectively carry out its monitoring function, the Member States should inform the Commission about any relevant action undertaken by the national data protection authorities, in particular regarding queries or complaints by Union data subjects concerning the transfer of personal data from the Union to certified organisations in the United States. The Commission should also be informed about any indications that the actions of U.S. public authorities responsible for the prevention, investigation, detection or prosecution of criminal offences, or for

⁴⁰⁶ *Schrems*, paragraph 65.

⁴⁰⁷ *Schrems*, paragraph 65: “It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision’s validity.”

⁴⁰⁸ *Schrems*, paragraph 76.

national security, including any oversight bodies, do not ensure the required level of protection.

- (211) In application of Article 45(3) of Regulation (EU) 2016/679⁴⁰⁹, the Commission, following the adoption of this Decision, should periodically review whether the findings relating to the adequacy of the level of protection ensured by the United States under the EU-U.S. DPF are still factually and legally justified. Since in particular EO 14086 and the AG Regulation require the creation of new mechanisms and the implementation of new safeguards, this Decision should be subject to a first review within one year after its entry into force, to verify whether all relevant elements have been fully implemented and are functioning effectively in practice. Following that first review, and depending on its outcome, the Commission will decide in close consultation with the Committee established under Article 93(1) of Regulation (EU) 2016/679 and the European Data Protection Board on the periodicity of future reviews⁴¹⁰.
- (212) To perform the reviews, the Commission should meet with the DoC, FTC and DoT accompanied, if appropriate, by other departments and agencies involved in the implementation of the EU-U.S. DPF, as well as, for matters pertaining to government access to data, representatives of the DoJ, ODNI (including the CLPO), other Intelligence Community elements, the DPRC as well as the Special Advocates. The participation in this meeting should be open to representatives of the members of the European Data Protection Board.
- (213) The reviews should cover all aspects of the functioning of this Decision with respect to the processing of personal data in the United States, and in particular the application and implementation of the Principles, with special attention paid to protections afforded in case of onward transfers; relevant case law developments; the effectiveness of the exercise of individual rights; the monitoring and enforcement of compliance with the Principles; as well as the limitations and safeguards with respect to government access, notably the implementation and application of the safeguards introduced by EO 14086, including through policies and procedures developed by intelligence agencies; the interplay between the EO 14086 and Section 702 FISA and EO 12333; and the effectiveness of the oversight mechanisms and redress avenues (including the functioning of the new redress mechanism established under EO 14086). In the context of such reviews, attention will also be paid to cooperation between the DPAs and competent authorities of the United States, including the development of guidance and other interpretative tools on the application of the Principles as well as on other aspects of the functioning of the Framework.
- (214) On the basis of the review, the Commission should prepare a public report to be submitted to the European Parliament and the Council.

7. SUSPENSION, REPEAL OR AMENDMENT OF THIS DECISION

- (215) Where available information, in particular information resulting from the monitoring of this Decision or provided by U.S. or Member States' authorities, reveals that the level of protection afforded to data transferred under this Decision may no longer be

⁴⁰⁹ According to Article 45(3) Regulation (EU) 2016/679, “[t]he implementing act shall provide for a mechanism for a periodic review, [...] which shall take into account all relevant developments in the third country or international organisation.”

⁴¹⁰ Article 45(3) Regulation (EU) 2016/679 provides that a periodic review must take place “at least every four years”. See also European Data Protection Board, Adequacy Referential, WP 254 rev. 01.

adequate, the Commission should promptly inform the competent U.S. authorities thereof and request that appropriate measures be taken within a specified, reasonable timeframe.

- (216) If, at the expiry of that specified timeframe, the competent U.S. authorities fail to take those measures or otherwise demonstrate satisfactorily that this Decision continues to be based on an adequate level of protection, the Commission will initiate the procedure referred to in Article 93(2) of Regulation (EU) 2016/679 with a view to partially or completely suspend or repeal this Decision.
- (217) Alternatively, the Commission will initiate that procedure with a view to amend the Decision, in particular by subjecting data transfers to additional conditions or by limiting the scope of the adequacy finding only to data transfers for which an adequate level of protection continues to be ensured.
- (218) In particular, the Commission should initiate the procedure for suspension or repeal in case of:
- (a) indications that organisations that have received personal data from the Union under this Decision do not comply with the Principles and that such non-compliance is not effectively addressed by the competent oversight and enforcement bodies;
 - (b) indications that the U.S. authorities do not comply with the applicable conditions and limitations for access by U.S. public authorities for law enforcement and national security purposes to personal data transferred under the EU-U.S. DPF ; or
 - (c) failure to effectively address complaints by Union data subjects, including by the ODNI CLPO and/or the DPRC.
- (219) The Commission should also consider initiating the procedure leading to the amendment, suspension or repeal of this Decision if the competent U.S. authorities fail to provide the information or clarifications necessary for the assessment of the level of protection afforded to personal data transferred from the Union to the United States, or as regards compliance with this Decision. In this respect, the Commission should take into account the extent to which the relevant information can be obtained from other sources.
- (220) On duly justified imperative grounds of urgency, for example if EO 14086 or the AG Regulation would be amended in a way that undermines the level of protection described in this Decision or if the Attorney General’s designation of the Union as a qualifying organisation for the purpose of the redress mechanism is withdrawn, the Commission will make use of the possibility to adopt, in accordance with the procedure referred to in Article 93(3) of Regulation (EU) 2016/679, immediately applicable implementing acts suspending, repealing or amending this Decision.

8. FINAL CONSIDERATIONS

- (221) The European Data Protection Board published its opinion⁴¹¹, which has been taken into consideration in the preparation of this Decision.

⁴¹¹ Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework of 28 February 2023.

- (222) The European Parliament adopted a resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework ⁴¹².
- (223) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93(1) Regulation (EU) 2016/679.

HAS ADOPTED THIS DECISION:

Article 1

For the purpose of Article 45 of Regulation (EU) 2016/679, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States that are included in the ‘Data Privacy Framework List’, maintained and made publicly available by the U.S. Department of Commerce, in accordance with Section I.3 of Annex I.

Article 2

Whenever the competent authorities in Member States, in order to protect individuals with regard to the processing of their personal data, exercise their powers pursuant to Article 58 of Regulation (EU) 2016/679 with respect to data transfers referred to in Article 1 of this Decision, the Member State concerned shall inform the Commission without delay.

Article 3

1. The Commission shall continuously monitor the application of the legal framework that is the object of this Decision, including the conditions under which onward transfers are carried out, individual rights are exercised and U.S. public authorities have access to data transferred on the basis of this Decision, with a view to assessing whether the United States continues to ensure an adequate level of protection as referred to in Article 1.
2. The Member States and the Commission shall inform each other of cases where it appears that the bodies in the United States with the statutory power to enforce compliance with the Principles set out in Annex I fail to provide effective detection and supervision mechanisms enabling infringements of the Principles set out in Annex I to be identified and punished in practice.
3. The Member States and the Commission shall inform each other of any indications that the interferences by U.S. public authorities responsible for the pursuit of national security, law enforcement or other public interests with the right of individuals to the protection of their personal data go beyond what is necessary and proportionate, and/or that there is no effective legal protection against such interferences.
4. After one year from the date of the notification of this Decision to the Member States and subsequently at a periodicity that will be decided in close consultation with the Committee established under Article 93(1) of Regulation (EU) 2016/679 and the European Data Protection Board, the Commission shall evaluate the finding referred to in Article 1(1) on the basis of all available information, including information

⁴¹² European Parliament Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)).

obtained through the review carried out together with the competent authorities of the United States.

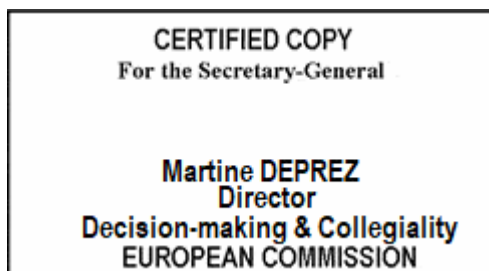
5. Where the Commission has indications that an adequate level of protection is no longer ensured, the Commission shall inform the competent U.S. authorities. If necessary, it will decide to suspend, amend or repeal this Decision, or limit its scope, in accordance with Article 45(5) of Regulation (EU) 2016/679. The Commission may also adopt such a decision if the lack of cooperation of the U.S. government prevents the Commission from determining whether the United States continues to ensure an adequate level of protection.

Article 4

This Decision is addressed to the Member States.

Done at Brussels, 10.7.2023

For the Commission
Didier REYNDEERS
Member of the Commission





Brussels, 10.7.2023
C(2023) 4745 final

ANNEXES 1 to 7

ANNEXES

to the

COMMISSION IMPLEMENTING DECISION

**pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
on the adequate level of protection of personal data under the EU-US Data Privacy
Framework**

ANNEX I

EU-U.S. DATA PRIVACY FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE

I. OVERVIEW

1. While the United States and the European Union (the “EU”) share a commitment to enhancing privacy protection, the rule of law, and a recognition of the importance of transatlantic data flows to our respective citizens, economies, and societies, the United States takes a different approach to privacy protection from that taken by the EU. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The U.S. Department of Commerce (“the Department”) is issuing the EU-U.S. Data Privacy Framework Principles, including the Supplemental Principles (collectively “the Principles”) and Annex I of the Principles (“Annex I”), under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). The Principles were developed in consultation with the European Commission (“the Commission”), industry, and other stakeholders to facilitate trade and commerce between the United States and EU. The Principles, a key component of the EU-U.S. Data Privacy Framework (“EU-U.S. DPF”), provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from the EU while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU countries. The Principles are intended for use solely by eligible organizations in the United States receiving personal data from the EU for the purpose of qualifying for the EU-U.S. DPF and thus benefitting from the Commission’s adequacy decision.¹ The Principles do not affect the application of the Regulation (EU) 2016/679 (“the General Data Protection Regulation” or “the GDPR”)² that applies to the processing of personal data in the EU Member States. Nor do the Principles limit privacy obligations that otherwise apply under U.S. law.
2. In order to rely on the EU-U.S. DPF to effectuate transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the Department (or its designee). While decisions by organizations to thus enter the EU-U.S. DPF are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply fully with the Principles. In order to enter the EU-U.S. DPF, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (the “FTC”), the U.S. Department of Transportation (the “DOT”) or another statutory body that will effectively ensure compliance with the Principles (*other U.S. statutory bodies recognized by the EU may be included as an annex in the future*); (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with these Principles; and (d) fully implement

¹ Provided that the Commission Decision on the adequacy of the protection provided by the EU-U.S. DPF applies to Iceland, Liechtenstein and Norway, the EU-U.S. DPF will cover both the EU, as well as these three countries. Consequently, references to the EU and its Member States will be read as including Iceland, Liechtenstein, and Norway.

² 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).

them³. An organization's failure to comply is enforceable by the FTC under Section 5 of the Federal Trade Commission (FTC) Act prohibiting unfair or deceptive acts in or affecting commerce (15 U.S.C. § 45); by the DOT under 49 U.S.C. § 41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice in air transportation or the sale of air transportation; or under other laws or regulations prohibiting such acts.

3. The Department will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles ("the Data Privacy Framework List"). EU-U.S. DPF benefits are assured from the date that the Department places the organization on the Data Privacy Framework List. The Department will remove from the Data Privacy Framework List those organizations that voluntarily withdraw from the EU-U.S. DPF or fail to complete their annual re-certification to the Department; these organizations must either continue to apply the Principles to the personal information they received under the EU-U.S. DPF and affirm to the Department on an annual basis their commitment to do so (*i.e.*, for as long as they retain such information), provide "adequate" protection for the information by another authorized means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the Commission), or return or delete the information. The Department will also remove from the Data Privacy Framework List those organizations that have persistently failed to comply with the Principles; these organizations must return or delete the personal information they received under the EU-U.S. DPF. An organization's removal from the Data Privacy Framework List means it is no longer entitled to benefit from the Commission's adequacy decision to receive personal information from the EU.
4. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Data Privacy Framework List. The Department will provide a clear warning that these organizations are not participants in the EU-U.S. DPF; that removal from the Data Privacy Framework List means that such organizations cannot claim to be EU-U.S. DPF compliant and must avoid any statements or misleading practices implying that they participate in the EU-U.S. DPF; and that such organizations are no longer entitled to benefit from the Commission's adequacy decision to receive personal information from the EU. An organization that continues to claim participation in the EU-U.S. DPF or makes other EU-U.S. DPF-related misrepresentations after it has been removed from the Data Privacy Framework List may be subject to enforcement action by the FTC, the DOT, or other enforcement authorities.
5. Adherence to these Principles may be limited: (a) to the extent necessary to comply with a court order or meet public interest, law enforcement, or national security requirements, including where statute or government regulation create conflicting obligations; (b) by statute, court order, or government regulation that creates explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the GDPR is to allow exceptions or derogations, under the conditions set out therein, provided such exceptions or derogations are applied in comparable contexts. In this context, safeguards in U.S. law to protect

³ The EU-U.S. Privacy Shield Framework Principles have been amended as the "EU-U.S. Data Privacy Framework Principles". (*See Supplemental Principle on Self-Certification*).

privacy and civil liberties include those required by Executive Order 14086⁴ under the conditions set out therein (including its requirements on necessity and proportionality). Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including by endeavouring to indicate in their privacy policies where exceptions to the Principles permitted by (b) above will apply. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

6. Organizations are obligated to apply the Principles to all personal data transferred in reliance on the EU-U.S. DPF after they enter the EU-U.S. DPF. An organization that chooses to extend EU-U.S. DPF benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department and conform to the requirements set forth in the Supplemental Principle on Self-Certification.
7. U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by organizations participating in the EU-U.S. DPF, except where such organizations have committed to cooperate with EU data protection authorities (“DPAs”). Unless otherwise stated, all provisions of the Principles apply where they are relevant.
8. Definitions:
 - a. “Personal data” and “personal information” are data about an identified or identifiable individual that are within the scope of the GDPR, received by an organization in the United States from the EU, and recorded in any form.
 - b. “Processing” of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
 - c. “Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.
9. The effective date of the Principles and Annex I of the Principles is the date of entry into force of the European Commission’s adequacy decision.

II. PRINCIPLES

1. NOTICE

- a. An organization must inform individuals about:
 - i. its participation in the EU-U.S. DPF and provide a link to, or the web address for, the Data Privacy Framework List,
 - ii. the types of personal data collected and, where applicable, the U.S. entities or U.S. subsidiaries of the organization also adhering to the Principles,

⁴ Executive Order of October 7, 2022, "Enhancing Safeguards for United States Signals Intelligence Activities."

- iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF,
 - iv. the purposes for which it collects and uses personal information about them,
 - v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,
 - vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,
 - vii. the right of individuals to access their personal data,
 - viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,
 - ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,
 - x. being subject to the investigatory and enforcement powers of the FTC, the DOT or any other U.S. authorized statutory body,
 - xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,⁵
 - xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and
 - xiii. its liability in cases of onward transfers to third parties.
- b. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

2. CHOICE

- a. An organization must offer individuals the opportunity to choose (*i.e.*, opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized

⁵ See, e.g., section (c) of the Recourse, Enforcement and Liability Principle.

by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.

- b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.
- c. For sensitive information (*i.e.*, personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (*i.e.*, opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. ACCOUNTABILITY FOR ONWARD TRANSFER

- a. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.
- b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

4. SECURITY

- a. Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. DATA INTEGRITY AND PURPOSE LIMITATION

- a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing.⁶ An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.
- b. Information may be retained in a form identifying or making identifiable⁷ the individual only for as long as it serves a purpose of processing within the meaning of 5(a). This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other principles and provisions of the EU-U.S. DPF. Organizations should take reasonable and appropriate measures in complying with this provision.

6. ACCESS

- a. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7. RECOURSE, ENFORCEMENT AND LIABILITY

- a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:
 - i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
 - ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true

⁶ Depending on the circumstances, examples of compatible processing purposes may include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection.

⁷ In this context, if, given the means of identification reasonably likely to be used (considering, among other things, the costs of and the amount of time required for identification and the available technology at the time of the processing) and the form in which the data is retained, an individual could reasonably be identified by the organization, or a third party if it would have access to the data, then the individual is "identifiable."

and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and

- iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.
- b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the EU-U.S. DPF. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.
- c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.
- d. In the context of an onward transfer, a participating organization has responsibility for the processing of personal information it receives under the EU-U.S. DPF and subsequently transfers to a third party acting as an agent on its behalf. The participating organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.
- e. When an organization becomes subject to a court order that is based on non-compliance or an order from a U.S. statutory body (*e.g.*, FTC or DOT) listed in the Principles or in a future annex to the Principles that is based on non-compliance, the organization shall make public any relevant EU-U.S. DPF-related sections of any compliance or assessment report submitted to the court or U.S. statutory body to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by participating organizations. The FTC and the DOT will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

III. SUPPLEMENTAL PRINCIPLES

1. Sensitive Data

- a. An organization is not required to obtain affirmative, express consent (*i.e.*, opt in) with respect to sensitive data where the processing is:
 - i. in the vital interests of the data subject or another person;
 - ii. necessary for the establishment of legal claims or defenses;
 - iii. required to provide medical care or diagnosis;
 - iv. carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
 - v. necessary to carry out the organization's obligations in the field of employment law; or
 - vi. related to data that are manifestly made public by the individual.

2. Journalistic Exceptions

- a. Given U.S. constitutional protections for freedom of the press, where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations.
- b. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Principles.

3. Secondary Liability

- a. Internet Service Providers ("ISPs"), telecommunications carriers, and other organizations are not liable under the Principles when on behalf of another organization they merely transmit, route, switch, or cache information. The EU-U.S. DPF does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

4. Performing Due Diligence and Conducting Audits

- a. The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. This is permitted by the Notice, Choice, and Access Principles under the circumstances described below.
- b. Public stock corporations and closely held companies, including participating organizations, are regularly subject to audits. Such audits,

particularly those looking into potential wrongdoing, may be jeopardized if disclosed prematurely. Similarly, a participating organization involved in a potential merger or takeover will need to perform, or be the subject of, a “due diligence” review. This will often entail the collection and processing of personal data, such as information on senior executives and other key personnel. Premature disclosure could impede the transaction or even violate applicable securities regulation. Investment bankers and attorneys engaged in due diligence, or auditors conducting an audit, may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations’ compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

5. The Role of the Data Protection Authorities

- a. Organizations will implement their commitment to cooperate with DPAs as described below. Under the EU-U.S. DPF, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Principles. More specifically as set out in the Recourse, Enforcement and Liability Principle, participating organizations must provide: (a)(i) recourse for individuals to whom the data relate; (a)(ii) follow-up procedures for verifying that the attestations and assertions they have made about their privacy practices are true; and (a)(iii) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle if it adheres to the requirements set forth here for cooperating with the DPAs.
- b. An organization commits to cooperate with the DPAs by declaring in its EU-U.S. DPF self-certification submission to the Department (*see* Supplemental Principle on Self-Certification) that the organization:
 - i. elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle by committing to cooperate with the DPAs;
 - ii. will cooperate with the DPAs in the investigation and resolution of complaints brought under the Principles; and
 - iii. will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.
- c. Operation of DPA Panels
 - i. The cooperation of the DPAs will be provided in the form of information and advice in the following way:

1. The advice of the DPAs will be delivered through an informal panel of DPAs established at the EU level, which will *inter alia* help ensure a harmonized and coherent approach.
 2. The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the EU-U.S. DPF. This advice will be designed to ensure that the Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.
 3. The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for EU-U.S. DPF purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.
 4. Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.
 5. The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.
 6. The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.
- ii. As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to refer the matter to the FTC, the DOT, or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department so that the Data Privacy Framework List can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act (15 U.S.C. § 45), 49 U.S.C. § 41712, or other similar statute.
- d. An organization that wishes its EU-U.S. DPF benefits to cover human resources data transferred from the EU in the context of the employment relationship must commit to cooperate with the DPAs with regard to such data (*see* Supplemental Principle on Human Resources Data).

- e. Organizations choosing this option will be required to pay an annual fee, which will be designed to cover the operating costs of the panel. They may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The amount of the fee will be determined by the Department after consultation with the Commission. The collection of the fee may be conducted by a third party selected by the Department to serve as the custodian of the funds collected for this purpose. The Department will closely cooperate with the Commission and the DPAs on the establishment of appropriate procedures for the distribution of funds collected through the fee, as well as other procedural and administrative aspects of the panel. The Department and the Commission may agree to alter how often the fee is collected.

6. Self-Certification

- a. EU-U.S. DPF benefits are assured from the date on which the Department places the organization on the Data Privacy Framework List. The Department will only place an organization on the Data Privacy Framework List after having determined that the organization's initial self-certification submission is complete, and will remove the organization from that list if it voluntarily withdraws, fails to complete its annual re-certification, or if it persistently fails to comply with the Principles (*see* Supplemental Principle on Dispute Resolution and Enforcement).
- b. To initially self-certify or subsequently re-certify for the EU-U.S. DPF, an organization must on each occasion provide to the Department a submission by a corporate officer on behalf of the organization that is self-certifying or re-certifying (as applicable) its adherence to the Principles⁸, that contains at least the following information:
 - i. the name of the self-certifying or re-certifying U.S. organization, as well as the name(s) of any of its U.S. entities or U.S. subsidiaries also adhering to the Principles that the organization wishes to cover;
 - ii. a description of the activities of the organization with respect to personal information that would be received from the EU under the EU-U.S. DPF;
 - iii. a description of the organization's relevant privacy policy/ies for such personal information, including:
 - 1. if the organization has a public website, the relevant web address where the privacy policy is available, or if the organization does not have a public website, where the privacy policy is available for viewing by the public; and
 - 2. its effective date of implementation;

⁸ The submission must be made via the Department's Data Privacy Framework website by an individual within the organization who is authorized to make representations on behalf of the organization and any of its covered entities regarding its adherence to the Principles.

- iv. a contact office within the organization for the handling of complaints, access requests, and any other issues arising under the Principles⁹, including:
 - 1. the name(s), job title(s) (as applicable), e-mail address(es), and telephone number(s) of the relevant individual(s) or relevant contact office(s) within the organization; and
 - 2. the relevant U.S. mailing address for the organization;
 - v. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
 - vi. the name of any privacy program in which the organization is a member;
 - vii. the method of verification (*i.e.*, self-assessment; or outside compliance reviews, including the third party that completes such reviews);¹⁰ and
 - viii. the relevant independent recourse mechanism(s) available to investigate unresolved Principles-related complaints.¹¹
- c. Where the organization wishes its EU-U.S. DPF benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where a statutory body listed in the Principles or a future annex to the Principles has jurisdiction to hear claims against the organization arising out of the processing of human resources information. In addition, the organization must indicate this in its initial self-certification submission, as well as in any re-certification submissions, and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with the Supplemental Principles on Human Resources Data and the Role of the Data Protection Authorities (as applicable) and that it will comply with the advice given by such authorities. The organization must also provide the Department with a copy of its human resources privacy policy and provide information where the privacy policy is available for viewing by its affected employees.
- d. The Department will maintain and make publicly available the Data Privacy Framework List of organizations that have filed completed, initial self-certification submissions and will update that list on the basis of completed, annual re-certification submissions, as well as notifications received pursuant to the Supplemental Principle on Dispute Resolution and Enforcement. Such re-certification submissions must be provided not less than annually; otherwise the organization will be removed from the Data Privacy Framework List and EU-U.S. DPF benefits will no longer be assured. All organizations that are placed on the Data Privacy Framework List by the Department must have relevant privacy policies that comply with the Notice Principle and state in those privacy policies that they

⁹ The primary “organization contact” or the “organization corporate officer” cannot be external to the organization (*e.g.*, outside counsel or an external consultant).

¹⁰ See Supplemental Principle on Verification.

¹¹ See Supplemental Principle on Dispute Resolution and Enforcement.

adhere to the Principles.¹² If available online, an organization’s privacy policy must include a hyperlink to the Department’s Data Privacy Framework website and a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved, Principles-related complaints free of charge to the individual.

- e. The Principles apply immediately upon self-certification. Participating organizations that previously self-certified to the EU-U.S. Privacy Shield Framework Principles will need to update their privacy policies to instead refer to the “EU-U.S. Data Privacy Framework Principles”. Such organizations shall include this reference as soon as possible, and in any event no later than three months from the effective date for the EU-U.S. Data Privacy Framework Principles.
- f. An organization must subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF. The undertaking to adhere to the Principles is not time-limited in respect of personal data received during the period in which the organization enjoys the benefits of the EU-U.S. DPF; its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the EU-U.S. DPF for any reason. An organization that wishes to withdraw from the EU-U.S. DPF must notify the Department of this in advance. This notification must also indicate what the organization will do with the personal data that it received in reliance on the EU-U.S. DPF (*i.e.*, retain, return, or delete the data, and if it will retain the data, the authorized means by which it will provide protection to the data). An organization that withdraws from the EU-U.S. DPF, but wants to retain such data must either affirm to the Department on an annual basis its commitment to continue to apply the Principles to the data or provide “adequate” protection for the data by another authorized means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the Commission); otherwise, the organization must return or delete the information.¹³ An organization that withdraws from the EU-U.S. DPF must remove from any relevant privacy policy any references to the EU-U.S. DPF that imply that the organization continues to participate in the EU-U.S. DPF and is entitled to its benefits.
- g. An organization that will cease to exist as a separate legal entity due to a change in corporate status, such as a result of a merger, takeover, bankruptcy, or dissolution must notify the Department of this in advance. The notification should also indicate whether the entity resulting from the

¹² An organization self-certifying for the first time may not claim EU-U.S. DPF participation in its final privacy policy until the Department notifies the organization that it may do so. The organization must provide the Department with a draft privacy policy, which is consistent with the Principles, when it submits its initial self-certification. Once the Department has determined that the organization’s initial self-certification submission is otherwise complete, the Department will notify the organization that it should finalize (*e.g.*, publish where applicable) its EU-U.S. DPF-consistent privacy policy. The organization must promptly notify the Department as soon as the relevant privacy policy is finalized, at which time the Department will place the organization on the Data Privacy Framework List.

¹³ If an organization elects at the time of its withdrawal to retain the personal data that it received in reliance on the EU-U.S. DPF and affirm to the Department on an annual basis that it continues to apply the Principles to such data, the organization must verify to the Department once a year following its withdrawal (*i.e.*, unless and until the organization provides “adequate” protection for such data by another authorized means, or returns or deletes all such data and notifies the Department of this action) what it has done with that personal data, what it will do with any of that personal data that it continues to retain, and who will serve as an ongoing point of contact for Principles-related questions.

change in corporate status will (i) continue to participate in the EU-U.S. DPF through an existing self-certification; (ii) self-certify as a new participant in the EU-U.S. DPF (*e.g.*, where the new entity or surviving entity does not already have an existing self-certification through which it could participate in the EU-U.S. DPF); or (iii) put in place other safeguards, such as a written agreement that will ensure continued application of the Principles to any personal data that the organization received under the EU-U.S. DPF and will be retained. Where neither (i), (ii), nor (iii) applies, any personal data that has been received under the EU-U.S. DPF must be promptly returned or deleted.

- h. When an organization leaves the EU-U.S. DPF for any reason, it must remove all statements implying that the organization continues to participate in the EU-U.S. DPF or is entitled to the benefits of the EU-U.S. DPF. The EU-U.S. DPF certification mark, if used, must also be removed. Any misrepresentation to the general public concerning an organization's adherence to the Principles may be actionable by the FTC, DOT, or other relevant government body. Misrepresentations to the Department may be actionable under the False Statements Act (18 U.S.C. § 1001).

7. Verification

- a. Organizations must provide follow-up procedures for verifying that the attestations and assertions they make about their EU-U.S. DPF privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Principles.
- b. To meet the verification requirements of the Recourse, Enforcement and Liability Principle, an organization must verify such attestations and assertions either through self-assessment or outside compliance reviews.
- c. Where the organization has chosen self-assessment, such verification must demonstrate that its privacy policy regarding personal information received from the EU is accurate, comprehensive, readily available, conforms to the Principles, and is completely implemented (*i.e.*, is being complied with). It must also indicate that individuals are informed of any in-house arrangements for handling complaints and of the independent recourse mechanism(s) through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying that the self-assessment has been completed must be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.
- d. Where the organization has chosen outside compliance review, such verification must demonstrate that its privacy policy regarding personal information received from the EU is accurate, comprehensive, readily available, conforms to the Principles, and is completely implemented (*i.e.*, is being complied with). It must also indicate that individuals are informed of mechanism(s) through which they may pursue complaints. The methods of review may include, without limitation, auditing, random reviews, use of "decoys", or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully

completed must be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.

- e. Organizations must retain their records on the implementation of their EU-U.S. DPF privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent dispute resolution body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also respond promptly to inquiries and other requests for information from the Department relating to the organization's adherence to the Principles.

8. Access

a. The Access Principle in Practice

- i. Under the Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. The Access Principle means that individuals have the right to:
 - 1. obtain from an organization confirmation of whether or not the organization is processing personal data relating to them;¹⁴
 - 2. have communicated to them such data so that they could verify its accuracy and the lawfulness of the processing; and
 - 3. have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.
- ii. Individuals do not have to justify requests for access to their personal data. In responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with or about the nature of the information or its use that is the subject of the access request.
- iii. Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other personal information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be restricted in any particular instance, it should provide the individual requesting

¹⁴ The organization should answer requests from an individual concerning the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data is disclosed.

access with an explanation of why it has made that determination and a contact point for any further inquiries.

b. Burden or Expense of Providing Access

- i. The right of access to personal data may be restricted in exceptional circumstances where the legitimate rights of persons other than the individual would be violated or where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question. Expense and burden are important factors and should be taken into account but they are not controlling factors in determining whether providing access is reasonable.
- ii. For example, if the personal information is used for decisions that will significantly affect the individual (*e.g.*, the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these Supplemental Principles, the organization would have to disclose that information even if it is relatively difficult or expensive to provide. If the personal information requested is not sensitive or not used for decisions that will significantly affect the individual, but is readily available and inexpensive to provide, an organization would have to provide access to such information.

c. Confidential Commercial Information

- i. Confidential commercial information is information that an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. Organizations may deny or limit access to the extent that granting full access would reveal its own confidential commercial information, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another that is subject to a contractual obligation of confidentiality.
- ii. Where confidential commercial information can be readily separated from other personal information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information.

d. Organization of Data Bases

- i. Access can be provided in the form of disclosure of the relevant personal information by an organization to the individual and does not require access by the individual to an organization's data base.
- ii. Access needs to be provided only to the extent that an organization stores the personal information. The Access Principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

e. When Access May be Restricted

- i. As organizations must always make good faith efforts to provide individuals with access to their personal data, the circumstances in which organizations may restrict such access are limited, and any reasons for restricting access must be specific. As under the GDPR,

an organization can restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:

1. interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;
 2. disclosure where the legitimate rights or important interests of others would be violated;
 3. breaching a legal or other professional privilege or obligation;
 4. prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or
 5. prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.
- ii. An organization which claims an exception has the burden of demonstrating its necessity, and the reasons for restricting access and a contact point for further inquiries should be given to individuals.
- f. Right to Obtain Confirmation and Charging a Fee to Cover the Costs for Providing Access
- i. An individual has the right to obtain confirmation of whether or not this organization has personal data relating to him or her. An individual also has the right to have communicated to him or her personal data relating to him or her. An organization may charge a fee that is not excessive.
 - ii. Charging a fee may be justified, for example, where requests for access are manifestly excessive, in particular because of their repetitive character.
 - iii. Access may not be refused on cost grounds if the individual offers to pay the costs.
- g. Repetitious or Vexatious Requests for Access
- i. An organization may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.
- h. Fraudulent Requests for Access

- i. An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

- i. Timeframe for Responses

- i. Organizations should respond to access requests within a reasonable time period, in a reasonable manner, and in a form that is readily intelligible to the individual. An organization that provides information to data subjects at regular intervals may satisfy an individual access request with its regular disclosure if it would not constitute an excessive delay.

9. Human Resources Data

- a. Coverage by the EU-U.S. DPF

- i. Where an organization in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the EU-U.S. DPF, the transfer enjoys the benefits of the EU-U.S. DPF. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU Member State where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.
- ii. The Principles are relevant only when individually identified or identifiable records are transferred or accessed. Statistical reporting relying on aggregate employment data and containing no personal data or the use of anonymized data does not raise privacy concerns.

- b. Application of the Notice and Choice Principles

- i. A U.S. organization that has received employee information from the EU under the EU-U.S. DPF may disclose it to third parties or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with the requisite choice before doing so, unless they have already authorized the use of the information for such purposes. Such use must not be incompatible with the purposes for which the personal information has been collected or subsequently authorized by the individual. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.
- ii. It should be noted that certain generally applicable conditions for transfer from some EU Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.
- iii. In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include,

for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.

- iv. To the extent and for the period necessary to avoid prejudicing the ability of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.
- c. Application of the Access Principle
 - i. The Supplemental Principle on Access provides guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the EU must comply with local regulations and ensure that EU employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The EU-U.S. DPF requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.
- d. Enforcement
 - i. In so far as personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the organization in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work. This includes cases where the alleged mishandling of their personal information is the responsibility of the U.S. organization that has received the information from the employer and thus involves an alleged breach of the Principles. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.
 - ii. A U.S. organization participating in the EU-U.S. DPF that uses EU human resources data transferred from the EU in the context of the employment relationship and that wishes such transfers to be covered by the EU-U.S. DPF must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases.
- e. Application of the Accountability for Onward Transfer Principle
 - i. For occasional employment-related operational needs of the participating organization with respect to personal data transferred under the EU-U.S. DPF, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, as otherwise required under the Accountability for Onward Transfer Principle, provided that the participating organization has complied with the Notice and Choice Principles.

10. **Obligatory Contracts for Onward Transfers**

a. Data Processing Contracts

- i. When personal data is transferred from the EU to the United States only for processing purposes, a contract will be required, regardless of participation by the processor in the EU-U.S. DPF.
- ii. Data controllers in the EU are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU, and whether or not the processor participates in the EU-U.S. DPF. The purpose of the contract is to make sure that the processor:
 1. acts only on instructions from the controller;
 2. provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and understands whether onward transfer is allowed; and
 3. taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.
- iii. Because adequate protection is provided by participating organizations, contracts with such organizations for mere processing do not require prior authorization.

b. Transfers within a Controlled Group of Corporations or Entities

- i. When personal information is transferred between two controllers within a controlled group of corporations or entities, a contract is not always required under the Accountability for Onward Transfer Principle. Data controllers within a controlled group of corporations or entities may base such transfers on other instruments, such as EU Binding Corporate Rules or other intra-group instruments (*e.g.*, compliance and control programs), ensuring the continuity of protection of personal information under the Principles. In case of such transfers, the participating organization remains responsible for compliance with the Principles.

c. Transfers between Controllers

- i. For transfers between controllers, the recipient controller need not be a participating organization or have an independent recourse mechanism. The participating organization must enter into a contract with the recipient third-party controller that provides for the same level of protection as is available under the EU-U.S. DPF, not including the requirement that the third party controller be a participating organization or have an independent recourse mechanism, provided it makes available an equivalent mechanism.

11. **Dispute Resolution and Enforcement**

- a. The Recourse, Enforcement and Liability Principle sets out the requirements for EU-U.S. DPF enforcement. How to meet the

requirements of point (a)(ii) of the Principle is set out in the Supplemental Principle on Verification. This Supplemental Principle addresses points (a)(i) and (a)(iii), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Recourse, Enforcement and Liability Principle's requirements. Organizations satisfy the requirements through the following: (i) compliance with private sector developed privacy programs that incorporate the Principles into their rules and that include effective enforcement mechanisms of the type described in the Recourse, Enforcement and Liability Principle; (ii) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (iii) commitment to cooperate with DPAs located in the EU or their authorized representatives.

- b. This list is intended to be illustrative and not limiting. The private sector may design additional mechanisms to provide enforcement, so long as they meet the requirements of the Recourse, Enforcement and Liability Principle and the Supplemental Principles. Please note that the Recourse, Enforcement and Liability Principle's requirements are additional to the requirement that self-regulatory efforts must be enforceable under Section 5 of the FTC Act (15 U.S.C. § 45) prohibiting unfair or deceptive acts, 49 U.S.C. § 41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice in air transportation or the sale of air transportation, or another law or regulation prohibiting such acts.
- c. In order to help ensure compliance with their EU-U.S. DPF commitments and to support the administration of the program, organizations, as well as their independent recourse mechanisms, must provide information relating to the EU-U.S. DPF when requested by the Department. In addition, organizations must respond expeditiously to complaints regarding their compliance with the Principles referred through the Department by DPAs. The response should address whether the complaint has merit and, if so, how the organization will rectify the problem. The Department will protect the confidentiality of information it receives in accordance with U.S. law.
- d. Recourse Mechanisms
 - i. Individuals should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Organizations must respond to an individual within 45 days of receiving a complaint. Whether a recourse mechanism is independent is a factual question that can be demonstrated notably by impartiality, transparent composition and financing, and a proven track record. As required by the Recourse, Enforcement and Liability Principle, the recourse available to individuals must be readily available and free of charge to individuals. Independent dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the independent dispute resolution body operating the recourse mechanism, but such requirements should be transparent and justified (for example, to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with

full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Principles. They should also cooperate in the development of tools, such as standard complaint forms to facilitate the complaint resolution process.

- ii. Independent recourse mechanisms must include on their public websites information regarding the Principles and the services that they provide under the EU-U.S. DPF. This information must include: (1) information on or a link to the Principles' requirements for independent recourse mechanisms; (2) a link to the Department's Data Privacy Framework website; (3) an explanation that their dispute resolution services under the EU-U.S. DPF are free of charge to individuals; (4) a description of how a Principles-related complaint can be filed; (5) the timeframe in which Principles-related complaints are processed; and (6) a description of the range of potential remedies.
- iii. Independent recourse mechanisms must publish an annual report providing aggregate statistics regarding their dispute resolution services. The annual report must include: (1) the total number of Principles-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed.
- iv. As set forth in Annex I, an arbitration option is available to an individual to determine, for residual claims, whether a participating organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles¹⁵ or with respect to an allegation about the adequacy of the EU-U.S. DPF. Under this arbitration option, the "EU-U.S. Data Privacy Framework Panel" (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. Individuals and participating organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.

e. Remedies and Sanctions

- i. The result of any remedies provided by the independent dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, insofar as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who brought the complaint will

¹⁵ The Principles, Overview, para. 5.

cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances.¹⁶ Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive awards. Private-sector independent dispute resolution bodies and self-regulatory bodies must notify failures of participating organizations to comply with their rulings to the governmental body with applicable jurisdiction or the courts, as appropriate, and the Department.

f. FTC Action

- i. The FTC has committed to reviewing on a priority basis referrals alleging non-compliance with the Principles received from: (i) privacy self-regulatory bodies and other independent dispute resolution bodies; (ii) EU Member States; and (iii) the Department, to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that it has reason to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. This includes false claims of adherence to the Principles or participation in the EU-U.S. DPF by organizations, which either are no longer on the Data Privacy Framework List or have never self-certified to the Department. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of any such actions it takes. The Department encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Principles.

g. Persistent Failure to Comply

- i. If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the EU-U.S. DPF. Organizations that have persistently failed to comply with the Principles will be removed from the Data Privacy Framework List by the Department and must return or delete the personal information they received under the EU-U.S. DPF.
- ii. Persistent failure to comply arises where an organization that has self-certified to the Department refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or government body, or where such a body, including the Department, determines that an organization frequently fails to

¹⁶ Independent dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used, or disclosed information in blatant contravention of the Principles.

comply with the Principles to the point where its claim to comply is no longer credible. In cases where such a determination is made by a body other than the Department the organization must promptly notify the Department of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001). An organization's withdrawal from a private-sector privacy self-regulatory program or independent dispute resolution mechanism does not relieve it of its obligation to comply with the Principles and would constitute a persistent failure to comply.

- iii. The Department will remove an organization from the Data Privacy Framework List for persistent failure to comply, including in response to any notification it receives of such non-compliance from the organization itself, a privacy self-regulatory body or another independent dispute resolution body, or a government body, but only after first providing the organization with 30 days' notice and an opportunity to respond¹⁷. Accordingly, the Data Privacy Framework List maintained by the Department will make clear which organizations are assured and which organizations are no longer assured of EU-U.S. DPF benefits.
- iv. An organization applying to participate in a self-regulatory body for the purposes of requalifying for the EU-U.S. DPF must provide that body with full information about its prior participation in the EU-U.S. DPF.

12. Choice – Timing of Opt Out

- a. Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.
- b. Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

13. Travel Information

- a. Airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, may be transferred to organizations located outside the EU in several different

¹⁷ The Department will indicate within the notice the amount of time, which will necessarily be less than 30 days, the organization has to respond to the notice.

circumstances. Under the GDPR, personal data may, in the absence of an adequacy decision, be transferred to a third country if appropriate data protection safeguards are provided pursuant to Article 46 GDPR or, in specific situations, if one of the conditions of Article 49 GDPR is fulfilled (e.g., where the data subject has explicitly consented to the transfer). U.S. organizations subscribing to the EU-U.S. DPF provide adequate protection for personal data and may therefore receive data transfers from the EU on the basis of Article 45 GDPR, without having to put in place a transfer instrument pursuant to Article 46 GDPR or meet the conditions of Article 49 GDPR. Since the EU-U.S. DPF includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to participating organizations. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may *inter alia* impose special conditions for the handling of sensitive data.

14. Pharmaceutical and Medical Products

a. Application of EU/Member State Laws or the Principles

- i. EU/Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.

b. Future Scientific Research

- i. Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the EU-U.S. DPF, the organization may use the data for a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow up, related studies, or marketing.
- ii. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the personal data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.

c. Withdrawal from a Clinical Trial

- i. Participants may decide or be asked to withdraw from a clinical trial at any time. Any personal data collected previous to withdrawal may still be processed along with other data collected

as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.

d. Transfers for Regulatory and Supervision Purposes

- i. Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Similar transfers are allowed to parties other than regulators, such as company locations and other researchers, consistent with the Principles of Notice and Choice.

e. “Blinded” Studies

- i. To ensure objectivity in many clinical trials, participants, and often investigators as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Participants in such clinical trials (referred to as “blinded” studies) do not have to be provided access to the data on their treatment during the trial if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort.
- ii. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring organization.

f. Product Safety and Efficacy Monitoring

- i. A pharmaceutical or medical device company does not have to apply the Principles with respect to the Notice, Choice, Accountability for Onward Transfer, and Access Principles in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.

g. Key-coded Data

- i. Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he or she can identify the research subject under special circumstances (*e.g.*, if follow-up medical attention is required). A transfer from the EU to the United States of data coded in this way that is EU personal data under EU law would be covered by the Principles.

15. Public Record and Publicly Available Information

- a. An organization must apply the Principles of Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability to personal data from publicly available sources. These Principles shall apply also to personal data collected from public records (*i.e.*, those records kept by government agencies or entities at any level that are open to consultation by the public in general).
- b. It is not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to public record information, as long as it is not combined with non-public record information, and any conditions for consultation established by the relevant jurisdiction are respected. Also, it is generally not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.
- c. Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the EU-U.S. DPF.
- d. It is not necessary to apply the Access Principle to public record information as long as it is not combined with other personal information (apart from small amounts used to index or organize the public record information); however, any conditions for consultation established by the relevant jurisdiction are to be respected. In contrast, where public record information is combined with other non-public record information (other than as specifically noted above), an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.
- e. As with public record information, it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information. Organizations that are in the business of selling publicly available information may charge the organization's customary fee in responding to requests for access. Alternatively, individuals may seek access to their information from the organization that originally compiled the data.

16. Access Requests by Public Authorities

- a. In order to provide transparency in respect of lawful requests by public authorities to access personal information, participating organizations may voluntarily issue periodic transparency reports on the number of requests for personal information they receive by public authorities for law enforcement or national security reasons, to the extent such disclosures are permissible under applicable law.
- b. The information provided by the participating organizations in these reports together with information that has been released by the intelligence community, along with other information, can be used to inform the

periodic joint review of the functioning of the EU-U.S. DPF in accordance with the Principles.

- c. Absence of notice in accordance with point (a)(xii) of the Notice Principle shall not prevent or impair an organization's ability to respond to any lawful request.

ANNEX I: ARBITRAL MODEL

This Annex I provides the terms under which organizations participating in the EU-U.S. DPF are obligated to arbitrate claims, pursuant to the Recourse, Enforcement and Liability Principle. The binding arbitration option described below applies to certain “residual” claims as to data covered by the EU-U.S. DPF. The purpose of this option is to provide a prompt, independent, and fair mechanism, at the option of individuals, for resolution of any claimed violations of the Principles not resolved by any of the other EU-U.S. DPF mechanisms.

A. Scope

This arbitration option is available to an individual to determine, for residual claims, whether a participating organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles¹⁸ or with respect to an allegation about the adequacy of the EU-U.S. DPF.

B. Available Remedies

Under this arbitration option, the “EU-U.S. Data Privacy Framework Panel” (the arbitration panel consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual’s data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the EU-U.S. Data Privacy Framework Panel with respect to remedies. In considering remedies, the EU-U.S. Data Privacy Framework Panel is required to consider other remedies that already have been imposed by other mechanisms under the EU-U.S. DPF. No damages, costs, fees, or other remedies are available. Each party bears its own attorney’s fees.

C. Pre-Arbitration Requirements

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with the organization and afford the organization an opportunity to resolve the issue within the timeframe set forth in section (d)(i) of the Supplemental Principle on Dispute Resolution and Enforcement; (2) make use of the independent recourse mechanism under the Principles, at no cost to the individual; and (3) raise the issue through the individual’s DPA to the Department and afford the Department an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the Department’s International Trade Administration, at no cost to the individual.

This arbitration option may not be invoked if the individual’s same claimed violation of the Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which the individual was a party; or (3) was previously settled by the parties. In addition, this option may not be invoked if a DPA (1) has authority under the Supplemental Principle on the Role of the Data Protection Authorities or the Supplemental Principle on Human Resources Data; or (2) has the authority to resolve the claimed violation directly with the organization. A DPA’s authority to resolve the same claim against an EU data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the DPA authority.

¹⁸ The Principles, Overview, para. 5.

D. Binding Nature of Decisions

An individual's decision to invoke this binding arbitration option is entirely voluntary. Arbitral decisions will be binding on all parties to the arbitration. Once invoked, the individual forgoes the option to seek relief for the same claimed violation in another forum, except that if non-monetary equitable relief does not fully remedy the claimed violation, the individual's invocation of arbitration will not preclude a claim for damages that is otherwise available in the courts.

E. Review and Enforcement

Individuals and participating organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.¹⁹ Any such cases must be brought in the federal district court whose territorial coverage includes the primary place of business of the participating organization.

This arbitration option is intended to resolve individual disputes, and arbitral decisions are not intended to function as persuasive or binding precedent in matters involving other parties, including in future arbitrations or in EU or U.S. courts, or FTC proceedings.

F. The Arbitration Panel

The parties will select arbitrators for the EU-U.S. Data Privacy Framework Panel from the list of arbitrators discussed below.

Consistent with applicable law, the Department and the Commission will develop a list of at least 10 arbitrators, chosen on the basis of independence, integrity, and expertise. The following shall apply in connection with this process:

Arbitrators:

¹⁹ Chapter 2 of the Federal Arbitration Act ("FAA") provides that "[a]n arbitration agreement or arbitral award arising out of a legal relationship, whether contractual or not, which is considered as commercial, including a transaction, contract, or agreement described in [section 2 of the FAA], falls under the Convention [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 ("New York Convention").]" 9 U.S.C. § 202. The FAA further provides that "[a]n agreement or award arising out of such a relationship which is entirely between citizens of the United States shall be deemed not to fall under the [New York] Convention unless that relationship involves property located abroad, envisages performance or enforcement abroad, or has some other reasonable relation with one or more foreign states." *Id.* Under Chapter 2, "any party to the arbitration may apply to any court having jurisdiction under this chapter for an order confirming the award as against any other party to the arbitration. The court shall confirm the award unless it finds one of the grounds for refusal or deferral of recognition or enforcement of the award specified in the said [New York] Convention." *Id.* § 207. Chapter 2 further provides that "[t]he district courts of the United States . . . shall have original jurisdiction over . . . an action or proceeding [under the New York Convention], regardless of the amount in controversy." *Id.* § 203.

Chapter 2 also provides that "Chapter 1 applies to actions and proceedings brought under this chapter to the extent that chapter is not in conflict with this chapter or the [New York] Convention as ratified by the United States." *Id.* § 208. Chapter 1, in turn, provides that "[a] written provision in . . . a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction, or the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." *Id.* § 2. Chapter 1 further provides that "any party to the arbitration may apply to the court so specified for an order confirming the award, and thereupon the court must grant such an order unless the award is vacated, modified, or corrected as prescribed in sections 10 and 11 of [the FAA]." *Id.* § 9.

- (1) will remain on the list for a period of 3 years, absent exceptional circumstances or removal for cause, renewable by the Department, with prior notification to the Commission, for additional 3-year terms;
- (2) shall not be subject to any instructions from, or be affiliated with, either party, or any participating organization, or the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority; and
- (3) must be admitted to practice law in the United States and be experts in U.S. privacy law, with expertise in EU data protection law.

G. Arbitration Procedures

The Department and the Commission have agreed, consistent with applicable law, to the adoption of arbitration rules that govern proceedings before the EU-U.S. Data Privacy Framework Panel.²⁰ In the event the rules governing the proceedings need to be changed, the Department and the Commission will agree to amend those rules or adopt a different set of existing, well-established U.S. arbitral procedures, as appropriate, subject to each of the following considerations:

1. An individual may initiate binding arbitration, subject to the pre-arbitration requirements provision above, by delivering a “Notice” to the organization. The Notice shall contain a summary of steps taken under Paragraph C to resolve the claim, a description of the alleged violation, and, at the choice of the individual, any supporting documents and materials and/or a discussion of law relating to the alleged claim.
2. Procedures will be developed to ensure that an individual’s same claimed violation does not receive duplicative remedies or procedures.
3. FTC action may proceed in parallel with arbitration.
4. No representative of the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority may participate in these arbitrations, provided, that at the request of an EU individual, DPAs may provide assistance in the preparation only of the Notice but DPAs may not have access to discovery or any other materials related to these arbitrations.
5. The location of the arbitration will be the United States, and the individual may choose video or telephone participation, which will be provided at no cost to the individual. In-person participation will not be required.

²⁰ The International Centre for Dispute Resolution (“ICDR”), the international division of the American Arbitration Association (“AAA”) (collectively “ICDR-AAA”), was selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles. On September 15, 2017, the Department and the Commission agreed to the adoption of a set of arbitration rules to govern binding arbitration proceedings described in Annex I of the Principles, as well as a code of conduct for arbitrators that is consistent with generally accepted ethical standards for commercial arbitrators and Annex I of the Principles. The Department and the Commission agreed to adapt the arbitration rules and code of conduct to reflect the updates under the EU-U.S. DPF, and the Department will work with the ICDR-AAA to make those updates.

6. The language of the arbitration will be English unless otherwise agreed by the parties. Upon a reasoned request, and taking into account whether the individual is represented by an attorney, interpretation at the arbitral hearing, as well as translation of arbitral materials will be provided at no cost to the individual, unless the EU-U.S. Data Privacy Framework Panel finds that, under the circumstances of the specific arbitration, this would lead to unjustified or disproportionate costs.
7. Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
8. Individual-specific discovery may be permitted if necessary, and such discovery will be treated confidentially by the parties and will only be used in connection with the arbitration.
9. Arbitrations should be completed within 90 days of the delivery of the Notice to the organization at issue, unless otherwise agreed to by the parties.

H. Costs

Arbitrators should take reasonable steps to minimize the costs or fees of the arbitrations.

The Department will, consistent with applicable law, facilitate the maintenance of a fund, to which participating organizations will be required to contribute, based in part on the size of the organization, which will cover the arbitral cost, including arbitrator fees, up to maximum amounts (“caps”). The fund will be managed by a third party, which will report regularly to the Department on the operations of the fund. The Department will work with the third party to periodically review the operation of the fund, including the need to adjust the amount of the contributions or of the caps on the arbitral cost, and consider, among other things, the number of arbitrations and the costs and timing of the arbitrations, with the understanding that there will be no excessive financial burden imposed on participating organizations. The Department will notify the Commission of the outcome of such reviews with the third party and will provide the Commission with prior notification of any adjustments of the amount of the contributions. Attorney’s fees are not covered by this provision or any fund under this provision.

ANNEX II



UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

July 6, 2023

The Honorable Didier Reynders
Commissioner for Justice
European Commission
Rue de la Loi/ Weststraat 200
1049 Brussels
Belgium

Dear Commissioner Reynders:

On behalf of the United States, I am pleased to transmit herewith a package of EU-U.S. Data Privacy Framework materials that, combined with Executive Order 14086, “Enhancing Safeguards for United States Signals Intelligence Activities” and 28 CFR part 201 amending Department of Justice regulations to establish the “Data Protection Review Court”, reflects important and detailed negotiations to strengthen privacy and civil liberties protections. These negotiations have resulted in new safeguards to ensure that U.S. signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives and a new mechanism for European Union (“EU”) individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities, which together will ensure the privacy of EU personal data. The EU-U.S. Data Privacy Framework will underpin an inclusive and competitive digital economy. We should both be proud of the improvements reflected in that Framework, which will enhance the protection of privacy around the world. This package, along with the Executive Order, Regulations, and other materials available from public sources, provides a very strong basis for a new adequacy finding by the European Commission.¹

The following materials are attached:

- The EU-U.S. Data Privacy Framework Principles, including the Supplemental Principles (collectively “the Principles”) and Annex I of the Principles (*i.e.*, an annex providing the terms under which Data Privacy Framework organizations are obligated to arbitrate certain residual claims as to personal data covered by the Principles);

¹ Provided that the Commission Decision on the adequacy of the protection provided by the EU-U.S. Data Privacy Framework applies to Iceland, Liechtenstein and Norway, the EU-U.S. Data Privacy Framework Package will cover both the European Union, as well as these three countries.

- A letter from the Department's International Trade Administration, which administers the Data Privacy Framework program, describing the commitments that our Department has made to ensure that the EU-U.S. Data Privacy Framework operates effectively;
- A letter from the Federal Trade Commission describing its enforcement of the Principles;
- A letter from the Department of Transportation describing its enforcement of the Principles;
- A letter prepared by the Office of the Director of National Intelligence regarding safeguards and limitations applicable to U.S. national security authorities; and
- A letter prepared by the Department of Justice regarding safeguards and limitations on U.S. Government access for law enforcement and public interest purposes.

The full EU-U.S. Data Privacy Framework Package will be published on the Department's Data Privacy Framework website and the Principles and Annex I of the Principles will be effective on the date of entry into force of the European Commission's adequacy decision.

You can be assured that the United States takes these commitments seriously. We look forward to working with you as the EU-U.S. Data Privacy Framework is implemented and as we embark on the next phase of this process together.

Sincerely,



Gina M. Raimondo

ANNEX III



UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

December 12, 2022

The Honorable Didier Reynders
Commissioner for Justice
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgium

Dear Commissioner Reynders:

On behalf of the International Trade Administration (“ITA”), I am pleased to describe the commitments the Department of Commerce (“the Department”) has made to ensure the protection of personal data through its administration and supervision of the Data Privacy Framework program. Finalizing the EU-U.S. Data Privacy Framework (“EU-U.S. DPF”) is a major achievement for privacy and for businesses on both sides of the Atlantic, as it will offer confidence to EU individuals that their data will be protected and that they will have legal remedies to address concerns related to their data, and will enable thousands of businesses to continue to invest and otherwise engage in trade and commerce across the Atlantic to the benefit of our respective economies and citizens. The EU-U.S. DPF reflects years of hard work and collaboration with you and your colleagues in the European Commission (“the Commission”). We look forward to continuing to work with the Commission to ensure that this collaborative effort functions effectively.

The EU-U.S. DPF will yield significant benefits for both individuals and businesses. First, it provides an important set of privacy protections for the data of EU individuals transferred to the United States. It requires participating U.S. organizations to develop a conforming privacy policy; publicly commit to comply with the “EU-U.S. Data Privacy Framework Principles”, including the Supplemental Principles (collectively “the Principles”), and Annex I of the Principles (*i.e.*, an annex providing the terms under which EU-U.S. DPF organizations are obligated to arbitrate certain residual claims as to personal data covered by the Principles), so that the commitment becomes enforceable under U.S. law¹; annually re-certify their compliance to the Department; provide free, independent dispute

¹ Organizations that self-certified their commitment to comply with the EU-U.S. Privacy Shield Framework Principles and wish to enjoy the benefits of participating in the EU-U.S. DPF must comply with the “EU-U.S. Data Privacy Framework Principles”. This commitment to comply with the “EU-U.S. Data Privacy Framework Principles” shall be reflected in the privacy policies of such participating organizations as soon as possible, and in any event no later than three months from the effective date for the “EU-U.S. Data Privacy Framework Principles”. (*See* section (e) of the Supplemental Principle on Self-Certification).

resolution to EU individuals; and be subject to the investigatory and enforcement authority of a U.S. statutory body listed in the Principles (*e.g.*, the Federal Trade Commission (the “FTC”) and Department of Transportation (the “DOT”)), or a U.S. statutory body listed in a future annex to the Principles. While an organization’s decision to self-certify is voluntary, once an organization publicly commits to the EU-U.S. DPF, its commitment is enforceable under U.S. law by the FTC, DOT, or another U.S. statutory body depending on which body has jurisdiction over the participating organization. Second, the EU-U.S. DPF will enable businesses in the United States, including subsidiaries of European businesses located in the United States, to receive personal data from the European Union to facilitate data flows that support transatlantic trade. Data flows between the United States and the European Union are the largest in the world and underpin the \$7.1 trillion U.S.-EU economic relationship, which supports millions of jobs on both sides of the Atlantic. Businesses that rely on transatlantic data flows come from all industry sectors and include major Fortune 500 firms, as well as many small and medium-sized enterprises. Transatlantic data flows allow U.S. organizations to process data required to offer goods, services, and employment opportunities to European individuals.

The Department is committed to working closely and productively with our EU counterparts to effectively administer and supervise the Data Privacy Framework program. This commitment is reflected in the Department’s development and continued refinement of a variety of resources to assist organizations with the self-certification process, creation of a website to provide targeted information to stakeholders, collaboration with the Commission and European data protection authorities (“DPAs”) to develop guidance that clarifies important elements of the EU-U.S. DPF, outreach to facilitate increased understanding of organizations’ data protection obligations, and oversight and monitoring of organizations’ compliance with the program’s requirements.

Our ongoing cooperation with valued EU counterparts will enable the Department to ensure that the EU-U.S. DPF functions effectively. The United States Government has a long history of working with the Commission to promote shared data protection principles, bridging the differences in our respective legal approaches while furthering trade and economic growth in the European Union and the United States. We believe that the EU-U.S. DPF, which is an example of this cooperation, will allow the Commission to issue a new adequacy decision that will permit organizations to use the EU-U.S. DPF to transfer personal data from the European Union to the United States consistent with EU law.

Administration and Supervision of the Data Privacy Framework Program by the Department of Commerce

The Department is firmly committed to the effective administration and supervision of the Data Privacy Framework program and will undertake appropriate efforts and dedicate appropriate resources to ensure that outcome. The Department will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles (“the Data Privacy Framework List”), which it will update on the basis of annual re-certification submissions made by participating organizations and by removing organizations when they voluntarily withdraw, fail to complete the annual re-certification in accordance with the Department’s procedures, or are found to persistently fail to comply. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that have been removed from the Data Privacy Framework List and will identify the reason each organization was removed. The aforementioned authoritative list and record will remain available to the public on the

Department's Data Privacy Framework website. The Data Privacy Framework website will include a prominently placed explanation indicating that any organization removed from the Data Privacy Framework List must cease making claims that it participates in or complies with the EU-U.S. DPF and that it may receive personal information pursuant to the EU-U.S. DPF. Such an organization must nevertheless continue to apply the Principles to the personal information that it received while it participated in the EU-U.S. DPF for as long as it retains such information. The Department, in furtherance of its overarching, ongoing commitment to the effective administration and supervision of the Data Privacy Framework program, specifically undertakes to do the following:

Verify Self-Certification Requirements

- The Department will, prior to finalizing an organization's initial self-certification or annual re-certification (collectively "self-certification") and placing or maintaining an organization on the Data Privacy Framework List, verify that the organization has, at a minimum, met the relevant requirements set forth in the Supplemental Principle on Self-Certification concerning what information an organization must provide in its self-certification submission to the Department and provided at an appropriate time a relevant privacy policy that informs individuals about all 13 of the enumerated elements set forth in the Notice Principle. The Department will verify that the organization has:
 - identified the organization that is submitting its self-certification, as well as any U.S. entities or U.S. subsidiaries of the self-certifying organization that are also adhering to the Principles that the organization wishes to be covered by its self-certification;
 - provided required organization contact information (*e.g.*, contact information for specific individual(s) and/or office(s) within the self-certifying organization responsible for handling complaints, access requests, and any other issues arising under the EU-U.S. DPF);
 - described the purpose(s) for which the organization would collect and use personal information received from the European Union;
 - indicated what personal information would be received from the European Union in reliance on the EU-U.S. DPF and therefore be covered by its self-certification;
 - if the organization has a public website, provided the web address where the relevant privacy policy is readily available on that website, or if the organization does not have a public website, provided the Department with a copy of the relevant privacy policy and where that privacy policy is available for viewing by affected individuals (*i.e.*, affected employees if the relevant privacy policy is a human resources privacy policy or the public if the relevant privacy policy is not a human resources privacy policy);
 - included in its relevant privacy policy at the appropriate time (*i.e.*, initially only in a draft privacy policy provided along with the submission if that submission is an initial self-certification; otherwise, in a final and where applicable published privacy policy) a statement that it adheres to the Principles and a hyperlink to or the web address for the Department's Data Privacy Framework website (*e.g.*, the homepage or the Data Privacy Framework List web page);
 - included in its relevant privacy policy at the appropriate time all of the 12 other enumerated elements set forth in the Notice Principle (*e.g.*, the possibility, under certain conditions, for the affected EU individual to invoke binding arbitration; the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements; and its liability in cases of onward transfers to third parties);
 - identified the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of

- laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
- identified any privacy program in which the organization is a member;
 - identified whether the relevant method (*i.e.*, follow-up procedures that it must provide) for verifying its compliance with the Principles is “self-assessment” (*i.e.*, in-house verification) or “outside compliance review” (*i.e.*, third-party verification) and if it identified the relevant method as outside compliance review, also identified the third party that has completed that review;
 - identified the appropriate independent recourse mechanism that is available to address complaints brought under the Principles and provide appropriate recourse free of charge to the affected individual.
 - If the organization has selected an independent recourse mechanism provided by a private-sector alternative dispute resolution body, it included in its relevant privacy policy a hyperlink to or the web address for the relevant website or complaint submission form of the mechanism that is available to investigate unresolved complaints brought under the Principles.
 - If the organization either is required to (*i.e.*, with respect to human resources data transferred from the European Union in the context of the employment relationship) or has elected to cooperate with the appropriate DPAs in the investigation and resolution of complaints brought under the Principles, it declared its commitment to such cooperation with the DPAs and compliance with their related advice to take specific action to comply with the Principles.
- The Department will also verify that the organization’s self-certification submission is consistent with its relevant privacy policy/ies. Where a self-certifying organization wishes to cover any of its U.S. entities or U.S. subsidiaries that have separate, relevant privacy policies, the Department will also review the relevant privacy policies of such covered entities or subsidiaries to ensure that they include all of the required elements set forth in the Notice Principle.
 - The Department will work with statutory bodies (*e.g.*, FTC and DOT) to verify that the organizations are subject to the jurisdiction of the relevant statutory body identified in their self-certification submissions, where the Department has reason to doubt that they are subject to that jurisdiction.
 - The Department will work with private-sector alternative dispute resolution bodies to verify that the organizations are actively registered for the independent recourse mechanism identified in their self-certification submissions; and work with those bodies to verify that the organizations are actively registered for the outside compliance review identified in their self-certification submissions, where those bodies may offer both types of services.
 - The Department will work with the third party selected by the Department to serve as the custodian of the funds collected through the DPA panel fee (*i.e.*, the annual fee designed to cover the operating costs of the DPA panel) to verify that the organizations have paid that fee for the relevant year, where the organizations have identified the DPAs as the relevant independent recourse mechanism.
 - The Department will work with the third party selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles to verify that the organizations have contributed to that arbitral fund.
 - Where the Department identifies any issues during its review of organizations’ self-certification submissions, it will inform them that they must address all such issues within the appropriate timeframe designated by the Department.² The Department will also inform them that failure to respond within timeframes designated by the Department or other failure to complete their self-certification in accordance with the Department’s procedures will lead to those self-certification submissions being considered abandoned, and that any

² *E.g.*, As regards re-certification, the expectation would be that organizations address all such issues within 45 days; subject to the designation by the Department of a different, appropriate timeframe.

misrepresentation about an organization's participation in or compliance with the EU-U.S. DPF may be subject to enforcement action by the FTC, the DOT, or other relevant government body. The Department will inform the organizations through the means of contact that the organizations provided to the Department.

Facilitate Cooperation with Alternative Dispute Resolution Bodies That Provide Principles-Related Services

- The Department will work with private-sector alternative dispute resolution bodies providing independent recourse mechanisms, which are available to investigate unresolved complaints brought under the Principles, to verify that they meet, at a minimum, the requirements set forth in the Supplemental Principle on Dispute Resolution and Enforcement. The Department will verify that they:
 - include information on their public websites regarding the Principles and the services that they provide under the EU-U.S. DPF, which must include: (1) information on or a hyperlink to the Principles' requirements for independent recourse mechanisms; (2) a hyperlink to the Department's Data Privacy Framework website; (3) an explanation that their dispute resolution services under the EU-U.S. DPF are free of charge to individuals; (4) a description of how a Principles-related complaint can be filed; (5) the timeframe in which Principles-related complaints are processed; and (6) a description of the range of potential remedies. The Department will provide the bodies with timely notice of material changes to the Department's supervision and administration of the Data Privacy Framework program, where such changes are imminent or have already been made and such changes are relevant to the role that the bodies play under the EU-U.S. DPF;
 - publish an annual report providing aggregate statistics regarding their dispute resolution services, which must include: (1) the total number of Principles-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed. The Department will provide the bodies with specific, complementary guidance on what information they should provide in those annual reports elaborating upon those requirements (*e.g.*, listing the specific criteria that a complaint must meet to be considered a Principles-related complaint for purposes of the annual report), as well as identifying other types of information they should provide (*e.g.*, if the body also provides a Principles-related verification service, a description of how the body avoids any actual or potential conflicts of interest in situations when it provides an organization with both verification services and dispute resolution services). The additional guidance provided by the Department will also specify the date by which the bodies' annual reports should be published for the relevant reporting period.

Follow Up with Organizations That Wish to Be or Have Been Removed from the Data Privacy Framework List

- If an organization wishes to withdraw from the EU-U.S. DPF, the Department will require that the organization remove from any relevant privacy policy any references to EU-U.S. DPF that imply that it continues to participate in the EU-U.S. DPF and that it may receive personal data pursuant to the EU-U.S. DPF (*see* description of the Department's commitment to search for false claims of participation). The Department will also require that the organization complete and submit to the Department an appropriate questionnaire to verify:

- its wish to withdraw;
 - which of the following it will do with the personal data that it received in reliance on the EU-U.S. DPF while it participated in the EU-U.S. DPF: (a) retain such data, continue to apply the Principles to such data, and affirm to the Department on an annual basis its commitment to apply the Principles to such data; (b) retain such data and provide “adequate” protection for such data by another authorized means; or (c) return or delete all such data by a specified date; and
 - who within the organization will serve as an ongoing point of contact for Principles-related questions.
- If an organization elected (a) as described immediately above, the Department will also require that it complete and submit to the Department each year after its withdrawal (*i.e.*, by the first anniversary of its withdrawal, as well as by every subsequent anniversary unless and until the organization either provides “adequate” protection for such data by another authorized means or returns or deletes all such data and notifies the Department of this action) an appropriate questionnaire to verify what it has done with that personal data, what it will do with any of that personal data that it continues to retain, and who within the organization will serve as an ongoing point of contact for Principles-related questions.
 - If an organization has allowed its self-certification to lapse (*i.e.*, neither completed its annual re-certification of its adherence to the Principles nor was removed from the Data Privacy Framework List for some other reason, such as withdrawal), the Department will direct it to complete and submit to the Department an appropriate questionnaire to verify whether it wishes to withdraw or re-certify:
 - and if it wishes to withdraw, further verify what it will do with the personal data that it received in reliance on the EU-U.S. DPF while it participated in the EU-U.S. DPF (*see* previous description of what an organization must verify if it wishes to withdraw);
 - and if it intends to re-certify, further verify that during the lapse of its certification status it applied the Principles to personal data received under the EU-U.S. DPF and clarify what steps it will take to address the outstanding issues that have delayed its re-certification.
 - If an organization is removed from the Data Privacy Framework List for any of the following reasons: (a) withdrawal from the EU-U.S. DPF, (b) failure to complete the annual re-certification of its adherence to the Principles (*i.e.*, either started, but failed to complete the annual re-certification process in a timely manner or did not even start the annual re-certification process), or (c) “persistent failure to comply”, the Department will send a notification to the contact(s) identified in the organization’s self-certification submission specifying the reason for the removal and explaining that it must cease making any explicit or implicit claims that it participates in or complies with the EU-U.S. DPF and that it may receive personal data pursuant to the EU-U.S. DPF. The notification, which may also include other content tailored to fit the reason for the removal, will indicate that organizations misrepresenting their participation in or compliance with the EU-U.S. DPF, including where they represent that they are participating in the EU-U.S. DPF after having been removed from the Data Privacy Framework List, may be subject to enforcement action by the FTC, the DOT, or other relevant government body.

Search for and Address False Claims of Participation

- On an ongoing basis, when an organization: (a) withdraws from participation in the EU-U.S. DPF, (b) fails to complete the annual re-certification of its adherence to the Principles (*i.e.*, either started, but failed to complete the annual re-certification process in a timely manner or did not even start the annual re-certification process), (c) is removed as a participant in the EU-U.S. DPF notably for “persistent failure to comply,” or (d) fails to complete an initial self-certification of its adherence to the Principles (*i.e.*, started, but failed to complete the

initial self-certification process in a timely manner), the Department will undertake, on an *ex officio* basis action to verify that any relevant published privacy policy of the organization does not contain references to the EU-U.S. DPF that imply that the organization participates in the EU-U.S. DPF and that it may receive personal data pursuant to the EU-U.S. DPF.

Where the Department finds such references, the Department will inform the organization that the Department will, as appropriate, refer the matter to the relevant agency for potential enforcement action if the organization continues to misrepresent its participation in the EU-U.S. DPF. The Department will inform the organization through the means of contact the organization provided to the Department or where necessary other appropriate means. If the organization neither removes the references nor self-certifies its compliance under the EU-U.S. DPF in accordance with the Department's procedures, the Department will *ex officio*, refer the matter to the FTC, DOT, or other appropriate enforcement agency, or take other appropriate action to ensure proper use of the EU-U.S. DPF certification mark;

- The Department will undertake other efforts to identify false claims of EU-U.S. DPF participation and improper use of the EU-U.S. DPF certification mark, including by organizations that unlike the organizations described immediately above have never even started the self-certification process (*e.g.*, conducting appropriate Internet searches to identify references to EU-U.S. DPF in organizations' privacy policies). Where through such efforts the Department identifies false claims of EU-U.S. DPF participation and improper use of the EU-U.S. DPF certification mark, the Department will inform the organization that the Department will, as appropriate, refer the matter to the relevant agency for potential enforcement action if the organization continues to misrepresent its participation in the EU-U.S. DPF. The Department will inform the organization through the means of contact, if any, the organization provided to the Department or where necessary other appropriate means. If the organization neither removes the references nor self-certifies its compliance under the EU-U.S. DPF in accordance with the Department's procedures, the Department will *ex officio*, refer the matter to the FTC, DOT, or other appropriate enforcement agency, or take other appropriate action to ensure proper use of the EU-U.S. DPF certification mark;
- The Department will promptly review and address specific, non-frivolous complaints about false claims of EU-U.S. DPF participation that the Department receives (*e.g.*, complaints received from the DPAs, independent recourse mechanisms provided by private-sector alternative dispute resolution bodies, data subjects, EU and U.S. businesses, and other types of third parties); and
- The Department may take other appropriate corrective action. Misrepresentations to the Department may be actionable under the False Statements Act (18 U.S.C. § 1001).

Conduct Periodic *ex officio* Compliance Reviews and Assessments of the Data Privacy Framework Program

- On an ongoing basis, the Department will undertake efforts to monitor effective compliance by EU-U.S. DPF organizations to identify issues that may warrant follow-up action. In particular, the Department will conduct, on an *ex officio* basis routine spot checks of randomly selected EU-U.S. DPF organizations, as well as *ad hoc* spot checks of specific EU-U.S. DPF organizations when potential compliance deficiencies are identified (*e.g.*, potential compliance deficiencies brought to the attention of the Department by third parties) to verify: (a) that the point(s) of contact responsible for the handling of complaints, access requests, and other issues arising under the EU-U.S. DPF are available; (b) where applicable, that the organization's public-facing privacy policy is readily available for viewing by the public both on the organization's public website and via a hyperlink on the Data Privacy Framework List; (c) that the organization's privacy policy continues to comply with the self-certification requirements described in the Principles; and (d) that the independent recourse mechanism identified by the organization is available to address complaints brought under

the EU-U.S. DPF. The Department will also actively monitor the news for reports that provide credible evidence of non-compliance by EU-U.S. DPF organizations;

- As part of the compliance review, the Department will require that a EU-U.S. DPF organization complete and submit to the Department a detailed questionnaire when: (a) the Department has received any specific, non-frivolous complaints about the organization's compliance with the Principles, (b) the organization does not respond satisfactorily to inquiries by the Department for information relating to the EU-U.S. DPF, or (c) there is credible evidence that the organization does not comply with its commitments under the EU-U.S. DPF. Where the Department has sent such a detailed questionnaire to an organization and the organization fails to satisfactorily reply to the questionnaire, the Department will inform the organization that the Department will, as appropriate, refer the matter to the relevant agency for potential enforcement action if the Department does not receive a timely and satisfactory response from the organization. The Department will inform the organization through the means of contact the organization provided to the Department or where necessary other appropriate means. If the organization does not provide a timely and satisfactory response, the Department will *ex officio* refer the matter to the FTC, DOT, or other appropriate enforcement agency, or take other appropriate action towards ensuring compliance. The Department shall, when appropriate, consult with the competent data protection authorities about such compliance reviews; and
- The Department will assess periodically the administration and supervision of the Data Privacy Framework program to ensure that its monitoring efforts, including any such efforts undertaken through the use of search tools (*e.g.*, to check for broken links to EU-U.S. DPF organizations' privacy policies), are appropriate to address existing issues and any new issues as they arise.

Tailor the Data Privacy Framework Website to Targeted Audiences

The Department will tailor the Data Privacy Framework website to focus on the following target audiences: EU individuals, EU businesses, U.S. businesses, and DPAs. The inclusion of material targeted directly to EU individuals and EU businesses will facilitate transparency in a number of ways. With regard to EU individuals, the website will clearly explain: (1) the rights the EU-U.S. DPF provides to EU individuals; (2) the recourse mechanisms available to EU individuals when they believe an organization has breached its commitment to comply with the Principles; and (3) how to find information pertaining to an organization's EU-U.S. DPF self-certification. With regard to EU businesses, it will facilitate verification of: (1) whether an organization is a participant in the EU-U.S. DPF; (2) the type of information covered by an organization's EU-U.S. DPF self-certification; (3) the privacy policy that applies to the covered information; and (4) the method the organization uses to verify its adherence to the Principles. With regard to U.S. businesses, it will clearly explain: (1) the benefits of EU-U.S. DPF participation; (2) how to join the EU-U.S. DPF, as well as how to re-certify to and withdraw from the EU-U.S. DPF; and (3) how the United States administers and enforces the EU-U.S. DPF. The inclusion of material targeted directly to DPAs (*e.g.*, information about the Department's dedicated point of contact for DPAs and a hyperlink to Principles-related content on the FTC website) will facilitate both cooperation and transparency. The Department will also work on an *ad hoc* basis with the Commission and the European Data Protection Board ("EDPB") to develop additional, topical material (*e.g.*, answers to frequently asked questions) for use on the Data Privacy Framework website, where such information would facilitate the efficient administration and supervision of the Data Privacy Framework program.

Facilitate Cooperation with DPAs

To increase opportunities for cooperation with DPAs, the Department will maintain a dedicated point of contact at the Department to act as a liaison with DPAs. In instances where a DPA believes that a EU-U.S. DPF organization is not complying with the Principles, including following a complaint from an EU individual, the DPA will be able to reach out to the dedicated point of contact at the Department to refer the organization for further review. The Department will make its best effort to facilitate resolution of the complaint with the EU-U.S. DPF organization. Within 90 days after receipt of the complaint, the Department will provide an update to the DPA. The dedicated point of contact will also receive referrals regarding organizations that falsely claim to participate in the EU-U.S. DPF. The dedicated point of contact will track all referrals from DPAs received by the Department, and the Department will provide in the joint review described below a report analyzing in aggregate the complaints it receives each year. The dedicated point of contact will assist DPAs seeking information related to a specific organization's self-certification or previous participation in the EU-U.S. DPF, and the dedicated point of contact will respond to DPA inquiries regarding the implementation of specific EU-U.S. DPF requirements. The Department will also cooperate with the Commission and the EDPB on procedural and administrative aspects of the DPA panel, including the establishment of appropriate procedures for the distribution of funds collected through the DPA panel fee. We understand that the Commission will work with the Department to facilitate resolution of any issues that may arise regarding those procedures. In addition, the Department will provide DPAs with material regarding the EU-U.S. DPF for inclusion on their own websites to increase transparency for EU individuals and EU businesses. Increased awareness regarding the EU-U.S. DPF and the rights and responsibilities it creates should facilitate the identification of issues as they arise, so that these can be appropriately addressed.

Fulfill Its Commitments under Annex I of the Principles

The Department will fulfill its commitments under Annex I of the Principles, including maintaining a list of arbitrators chosen with the Commission on the basis of independence, integrity, and expertise; and supporting, as appropriate, the third party selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles.³ The Department will work with the third party to, among other things, verify that the third party maintains a website with guidance on the arbitration process, including: (1) how to initiate proceedings and submit documents; (2) the list of arbitrators maintained by the Department and how to select arbitrators from that list; (3) the governing arbitral procedures and arbitrator code of conduct adopted by the Department and the Commission;⁴ and (4) the collection and payment of arbitrator fees. In addition, the Department will work with the third party to periodically review the operation of the arbitral fund, including the need to adjust the amount of the contributions or the caps (*i.e.*, maximum amounts) on the arbitral cost, and consider, among other things, the number of arbitrations and the costs and timing of the arbitrations, with the understanding that there will be no excessive financial burden

³ The International Centre for Dispute Resolution ("ICDR"), the international division of the American Arbitration Association ("AAA") (collectively "ICDR-AAA"), was selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles.

⁴ On September 15, 2017, the Department and the Commission agreed to the adoption of a set of arbitral rules to govern binding arbitration proceedings described in Annex I of the Principles, as well as a code of conduct for arbitrators that is consistent with generally accepted ethical standards for commercial arbitrators and Annex I of the Principles. The Department and the Commission agreed to adapt the arbitration rules and code of conduct to reflect the updates under the EU-U.S. DPF, and the Department will work with the ICDR-AAA to make those updates.

imposed on EU-U.S. DPF organizations. The Department will notify the Commission of the outcome of such reviews with the third party and will provide the Commission with prior notification of any adjustments of the amount of the contributions.

Conduct Joint Reviews of the Functioning of the EU-U.S. DPF

The Department and other agencies, as appropriate, will hold meetings on a periodic basis with the Commission, interested DPAs, and appropriate representatives from the EDPB, where the Department will provide updates on the EU-U.S. DPF. The meetings will include discussion of current issues related to the functioning, implementation, supervision, and enforcement of the Data Privacy Framework program. The meetings may, as appropriate, include discussion of related topics, such as other data transfer mechanisms that benefit from the safeguards under the EU-U.S. DPF.

Update of Laws

The Department will make reasonable efforts to inform the Commission of material developments in the law in the United States so far as they are relevant to the EU-U.S. DPF in the field of data privacy protection and the limitations and safeguards applicable to access to personal data by U.S. authorities and its subsequent use.

U.S. Government Access to Personal Data

The United States has issued Executive Order 14086, “Enhancing Safeguards for United States Signals Intelligence Activities” and 28 CFR part 201 amending Department of Justice regulations to establish the Data Protection Review Court (the “DPRC”), which provide strong protection for personal data with respect to government access to data for national security purposes. The protection provided includes: strengthening privacy and civil liberties safeguards to ensure that U.S. signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives; establishing a new redress mechanism with independent and binding authority; and enhancing the existing rigorous and layered oversight of U.S. signals intelligence activities. Through these protections, EU individuals may seek redress from a new multi-layer redress mechanism that includes an independent DPRC that would consist of individuals chosen from outside the U.S. Government who would have full authority to adjudicate claims and direct remedial measures as needed. The Department will maintain a record of EU individuals who submit a qualifying complaint pursuant to Executive Order 14086 and 28 CFR part 201. Five years after the date of this letter, and on a five-year basis thereafter, the Department will contact relevant agencies regarding whether information pertaining to the review of qualifying complaints or review of any applications for review submitted to the DPRC has been declassified. If such information has been declassified, the Department will work with the relevant DPA to inform the EU individual. These enhancements confirm that EU personal data transferred to the United States will be treated in a manner consistent with EU legal requirements with respect to government access to data.

On the basis of the Principles, Executive Order 14086, 28 CFR part 201, and the accompanying letters and materials, including the Department’s commitments regarding the administration and supervision of the Data Privacy Framework program, our expectation is that the Commission will determine that the EU-U.S. DPF provides adequate protection for the

purposes of EU law and data transfers from the European Union will continue to organizations that participate in the EU-U.S. DPF. We also expect that transfers to U.S. organizations made in reliance on EU Standard Contractual Clauses or EU Binding Corporate Rules will be further facilitated by the terms of those arrangements.

Sincerely,

A handwritten signature in black ink that reads "Marisa Lago". The signature is written in a cursive, slightly slanted style.

Marisa Lago



Office of the Chair

ANNEX IV

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

June 9, 2023

Didier Reynders
Commissioner for Justice
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Dear Commissioner Reynders:

The United States Federal Trade Commission (“FTC”) appreciates the opportunity to address its enforcement role in connection with the EU-U.S. Data Privacy Framework (“EU-U.S. DPF”) Principles. The FTC has long committed to protecting consumers and privacy across borders, and we are committed to enforcement of the commercial sector aspects of this framework. The FTC has performed such a role since the year 2000, in connection with the U.S.-EU Safe Harbor Framework, and most recently since 2016, in connection with the EU-U.S. Privacy Shield Framework.¹ On July 16, 2020, the Court of Justice of the European Union (“CJEU”) invalidated the European Commission’s adequacy decision underlying the EU-U.S. Privacy Shield Framework, on the basis of issues other than the commercial principles that the FTC enforced. The U.S. and the European Commission have since negotiated the EU-U.S. Data Privacy Framework to address that CJEU ruling.

I write to confirm the FTC’s commitment to vigorous enforcement of the EU-U.S. DPF Principles. Notably, we affirm our commitment in three key areas: (1) referral prioritization and investigations; (2) seeking and monitoring orders; and (3) enforcement cooperation with EU data protection authorities (“DPAs”).

I. Introduction

a. FTC Privacy Enforcement and Policy Work

The FTC has broad civil enforcement authority to promote consumer protection and competition in the commercial sphere. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumers and their data.

¹ Letter from Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework (February 29, 2016), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european>. The FTC also previously committed to enforce the U.S.-EU Safe Harbor Program. Letter from Robert Pitofsky, FTC Chairman, to John Mogg, Director DG Internal Market, European Commission (July 14, 2000), available at <https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission>. This letter replaces those earlier commitments.

The primary law enforced by the FTC, the FTC Act, prohibits “unfair” or “deceptive” acts or practices in or affecting commerce.² The FTC also enforces targeted statutes that protect information relating to health, credit, and other financial matters, as well as children’s online information, and has issued regulations implementing each of these statutes.³

The FTC has also recently pursued numerous initiatives to strengthen our privacy work. In August of 2022 the FTC announced it is considering rules to crack down on harmful commercial surveillance and lax data security.⁴ The goal of the project is to build a robust public record to inform whether the FTC should issue rules to address commercial surveillance and data security practices, and what those rules should potentially look like. We have welcomed comments from EU stakeholders on this and other initiatives.

Our “PrivacyCon” conferences continue to gather leading researchers to discuss the latest research and trends related to consumer privacy and data security. We also have increased our agency’s ability to keep pace with the technology developments at the center of much of our privacy work, building a growing team of technologists and interdisciplinary researchers. We also, as you know, announced a joint dialogue with you and your colleagues at the European Commission, which includes addressing such privacy-related topics as dark patterns and business models characterized by pervasive data collection.⁵ We also recently issued a report to Congress warning about harms associated with using artificial intelligence (“AI”) to address online harms identified by Congress. This report raised concerns regarding inaccuracy, bias, discrimination, and commercial surveillance creep.⁶

b. U.S. Legal Protections Benefitting EU Consumers

The EU-U.S. DPF operates in the context of the larger U.S. privacy landscape, which also protects EU consumers in a number of ways. The FTC Act’s prohibition on unfair or deceptive acts or practices is not limited to protecting U.S. consumers from U.S. companies, as it includes those practices that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct in the United States. Further, the FTC can use all remedies that are available to protect domestic consumers when protecting foreign consumers.⁷

² 15 U.S.C. § 45(a). The FTC does not have jurisdiction over criminal law enforcement or national security matters. Nor can the FTC reach most other governmental actions. In addition, there are exceptions to the FTC’s jurisdiction over commercial activities, including with respect to banks, airlines, the business of insurance, and the common carrier activities of telecommunications service providers. The FTC also does not have jurisdiction over most non-profit organizations, though it does have jurisdiction over sham charities or other non-profits that in fact operate for profit. The FTC also has jurisdiction over non-profit organizations that operate for the profit of their for-profit members, including by providing substantial economic benefits to those members. In some instances, the FTC’s jurisdiction is concurrent with that of other law enforcement agencies. We have developed strong working relationships with federal and state authorities, and work closely with them to coordinate investigations or make referrals where appropriate.

³ See FTC, Privacy and Security, <https://www.ftc.gov/business-guidance/privacy-security>.

⁴ See Press Release, Fed. Trade Comm’n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices>.

⁵ See Joint Press Statement by Didier Reynders, Commissioner for Justice of the European Commission and Lina Khan, Chair of the United States Federal Trade Commission (March 30, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

⁶ See Press Release, Fed. Trade Comm’n, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (June 16, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems>.

⁷ 15 U.S.C. § 45(a)(4)(B). Further, “unfair or deceptive acts or practices” includes such acts or practices involving foreign commerce that (i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States. 15 U.S.C. § 45(a)(4)(A).

The FTC also enforces other targeted laws whose protections extend to non-U.S. consumers, such as the Children’s Online Privacy Protection Act (“COPPA”). Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under the age of 13, provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. Moreover, in addition to the U.S. federal laws enforced by the FTC, other federal and state consumer protection, data breach, and privacy laws may provide additional benefits to EU consumers.

c. FTC Enforcement Activity

The FTC brought cases under both the U.S.-EU Safe Harbor and EU-U.S. Privacy Shield frameworks and continued to enforce the EU-U.S. Privacy Shield even after the CJEU invalidation of the adequacy decision underlying the EU-U.S. Privacy Shield Framework.⁸ Several of the FTC’s recent complaints have included counts alleging that firms violated EU-U.S. Privacy Shield provisions, including in proceedings against Twitter,⁹ CafePress,¹⁰ and Flo.¹¹ In the enforcement action against Twitter, the FTC secured \$150 million from Twitter for its violation of an earlier FTC order with practices affecting more than 140 million customers, including violating EU-U.S. Privacy Shield Principle 5 (Data Integrity and Purpose Limitation). Further, the agency’s order requires that Twitter allow users to employ secure multi-factor authentication methods that do not require users to provide their telephone numbers.

In *CafePress*, the FTC alleged that the company failed to secure consumers’ sensitive information, covered up a major data breach, and violated EU-U.S. Privacy Shield Principles 2 (Choice), 4 (Security), and 6 (Access). The FTC’s order requires the company to replace inadequate authentication measures with multifactor authentication, substantively limit the amount of data it collects and retains, encrypt Social Security numbers, and have a third party assess its information security programs and provide the FTC with a copy that can be publicized.

In *Flo*, the FTC alleged that the fertility-tracking app disclosed user health information to third-party data analytics providers after commitments to keep such information private. The FTC complaint specifically notes the company’s interactions with EU consumers and that Flo violated EU-U.S. Privacy Shield Principles 1 (Notice), 2 (Choice), 3 (Accountability for Onward Transfer), and 5 (Data Integrity and Purpose Limitation). Among other things, the agency’s order requires Flo to notify affected users about the disclosure of their personal information and to instruct any third party that received users’ health information to destroy that data. Importantly, FTC orders protect all consumers worldwide who interact with a U.S. business, not just those consumers who have lodged complaints.

Many past U.S.-EU Safe Harbor and EU-U.S. Privacy Shield enforcement cases involved organizations that completed an initial self-certification through the Department of

⁸ See Appendix A for a list of FTC Safe Harbor and Privacy Shield matters.

⁹ See Press Release, Fed. Trade Comm’n, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (May 25, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads>.

¹⁰ See Press Release, Fed. Trade Comm’n, FTC Takes Action Against CafePress for Data Breach Cover Up (March 15, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover>.

¹¹ See Press Release, Fed. Trade Comm’n, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (June 22, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>.

Commerce, but failed to maintain their annual self-certification while they continued to represent themselves as current participants. Other cases involved false claims of participation by organizations that never completed an initial self-certification through the Department of Commerce. Going forward, we expect to focus our proactive enforcement efforts on the types of substantive violations of the EU-U.S. DPF Principles alleged in cases such as Twitter, CafePress, and Flo. Meanwhile, the Department of Commerce will administer and supervise the self-certification process, maintain the authoritative list of EU-U.S. DPF participants, and address other program participation claim issues.¹² Importantly, organizations claiming EU-U.S. DPF participation may be subject to substantive enforcement of the EU-U.S. DPF Principles even if they fail to make or maintain their self-certification through the Department of Commerce.

II. Referral Prioritization and Investigations

As we did under the U.S.-EU Safe Harbor Framework and the EU-U.S. Privacy Shield Framework, the FTC commits to give priority consideration to EU-U.S. DPF Principles referrals from the Department of Commerce and EU Member States. We will also prioritize consideration of referrals for non-compliance with the EU-U.S. DPF Principles from privacy self-regulatory organizations and other independent dispute resolution bodies.

To facilitate referrals under the EU-U.S. DPF from EU Member States, the FTC has created a standardized referral process and has provided guidance to EU Member States on the type of information that would best assist the FTC in its inquiry into a referral. As part of this effort, the FTC has designated an agency point of contact for EU Member State referrals. It is most useful when the referring authority has conducted a preliminary inquiry into the alleged violation and can cooperate with the FTC in an investigation.

Upon receipt of such a referral from the Department of Commerce, an EU Member State, or self-regulatory organization or other independent dispute resolution bodies the FTC can take a range of actions to address the issues raised. For example, we may review the organization's privacy policies, obtain further information directly from the organization or from third parties, follow up with the referring entity, assess whether there is a pattern of violations or significant number of consumers affected, determine whether the referral implicates issues within the purview of the Department of Commerce, assess whether additional efforts to put market participants on notice would be helpful, and, as appropriate, initiate an enforcement proceeding.

In addition to prioritizing EU-U.S. DPF Principles referrals from the Department of Commerce, EU Member States, and privacy self-regulatory organizations or other independent dispute resolution bodies,¹³ the FTC will continue to investigate significant EU-U.S. DPF Principles violations on its own initiative where appropriate, using a range of tools. As part of the FTC's program of investigating privacy and security issues involving commercial organizations, the agency has routinely examined whether the entity at issue was making EU-U.S. Privacy Shield representations. If the entity made such representations and the investigation revealed apparent violations of the EU-U.S. Privacy Shield Principles, the FTC included allegations of EU-U.S. Privacy Shield violations in its enforcement actions. We will continue this proactive approach, now with respect to the EU-U.S. DPF Principles.

¹² Letter from Marisa Lago, Under Secretary of Commerce for International Trade, to the Honorable Didier Reynders, Commissioner for Justice, European Commission (December 12, 2022).

¹³ Although the FTC does not resolve or mediate individual consumer complaints, the FTC affirms that it will prioritize EU-U.S. DPF Principles referrals from EU DPAs. In addition, the FTC uses complaints in its Consumer Sentinel database, which is accessible by many other law enforcement agencies, to identify trends, determine enforcement priorities, and identify potential investigative targets. EU individuals can use the same complaint system available to U.S. consumers to submit a complaint to the FTC at <https://reportfraud.ftc.gov/>. For individual EU-U.S. DPF Principles complaints, however, it may be most useful for EU individuals to submit complaints to their Member State DPA or independent dispute resolution body.

III. Seeking and Monitoring Orders

The FTC also affirms its commitment to seek and monitor enforcement orders to ensure compliance with the EU-U.S. DPF Principles. We will require compliance with the EU-U.S. DPF Principles through a variety of appropriate injunctive provisions in future FTC EU-U.S. DPF Principles orders. Violations of the FTC's administrative orders can lead to civil penalties of up to \$50,120 per violation, or \$50,120 per day for a continuing violation,¹⁴ which, in the case of practices affecting many consumers, can amount to millions of dollars. Each consent order also has reporting and compliance provisions. The entities under order must retain documents demonstrating their compliance for a specified number of years. The orders must also be disseminated to employees responsible for ensuring order compliance.

The FTC systematically monitors compliance with existing EU-U.S. Privacy Shield Principles orders, as it does with all of its orders, and brings actions to enforce them when necessary.¹⁵ Importantly, FTC orders will continue to protect all consumers worldwide who interact with a business, not just those consumers who have lodged complaints. Finally, the FTC will maintain an online list of companies subject to orders obtained in connection with enforcement of the EU-U.S. DPF Principles.¹⁶

IV. Enforcement Cooperation with EU DPAs

The FTC recognizes the important role that EU DPAs can play with respect to EU-U.S. DPF Principles compliance and encourages increased consultation and enforcement cooperation. Indeed, a coordinated approach to the challenges posed by current digital market developments, and data-intensive business models, is increasingly critical. The FTC will exchange information on referrals with referring enforcement authorities, including the status of referrals, subject to confidentiality laws and restrictions. To the extent feasible given the number and type of referrals received, the information provided will include an evaluation of the referred matters, including a description of significant issues raised and any action taken to address law violations within the jurisdiction of the FTC. The FTC will also provide feedback to the referring authority on the types of referrals received in order to increase the effectiveness of efforts to address unlawful conduct. If a referring enforcement authority seeks information about the status of a particular referral for purposes of pursuing its own enforcement proceeding, the FTC will respond, taking into account the number of referrals under consideration and subject to confidentiality and other legal requirements.

The FTC will also work closely with EU DPAs to provide enforcement assistance. In appropriate cases, this could include information sharing and investigative assistance pursuant to the U.S. SAFE WEB Act, which authorizes FTC assistance to foreign law enforcement agencies when the foreign agency is enforcing laws prohibiting practices that are substantially similar to those prohibited by laws the FTC enforces.¹⁷ As part of this assistance, the FTC can share information obtained in connection with an FTC investigation, issue compulsory process on

¹⁴ 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. This amount is periodically adjusted for inflation.

¹⁵ Last year the FTC voted to streamline the process for investigating repeat offenders. *See* Press Release, Fed. Trade Comm'n, FTC Authorizes Investigations into Key Enforcement Priorities (Jul. 1, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities>.

¹⁶ *Cf.* FTC, Privacy Shield, <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>.

¹⁷ In determining whether to exercise its U.S. SAFE WEB Act authority, the FTC considers, *inter alia*: "(A) whether the requesting agency has agreed to provide or will provide reciprocal assistance to the Commission; (B) whether compliance with the request would prejudice the public interest of the United States; and (C) whether the requesting agency's investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons." 15 U.S.C. § 46(j)(3). This authority does not apply to enforcement of competition laws.

behalf of the EU DPA conducting its own investigation, and seek oral testimony from witnesses or defendants in connection with the DPA's enforcement proceeding, subject to the requirements of the U.S. SAFE WEB Act. The FTC regularly uses this authority to assist other authorities around the world in privacy and consumer protection cases.

In addition to any consultation with referring EU DPAs on case-specific matters, the FTC will participate in periodic meetings with designated representatives of the European Data Protection Board ("EDPB") to discuss in general terms how to improve enforcement cooperation. The FTC will also participate, along with the Department of Commerce, the European Commission, and EDPB representatives, in the periodic review of EU-U.S. DPF to discuss its implementation. The FTC also encourages the development of tools that will enhance enforcement cooperation with EU DPAs, as well as other privacy enforcement authorities around the world. The FTC is pleased to affirm its commitment to enforcing the commercial sector aspects of the EU-U.S. DPF. We see our partnership with EU colleagues as a critical part of providing privacy protection for both our citizens and yours.

Sincerely,

A handwritten signature in cursive script that reads "Lina Khan".

Lina M. Khan
Chair, Federal Trade Commission

Appendix A

Privacy Shield and Safe Harbor Enforcement

| | Docket/FTC File No. | Case | Link |
|----|---|---|-------------------------------------|
| 1 | FTC File No. 2023062 Case No. 3:22-cv-03070 (N.D. Cal.) | US v. Twitter, Inc. | Twitter |
| 2 | FTC File No. 192 3209 | In the Matter of Residual Pumpkin Entity, LLC, formerly d/b/a CafePress , and PlanetArt, LLC, d/b/a CafePress | CafePress |
| 3 | FTC File No. 192 3133 Docket No. C-4747 | In the Matter of Flo Health, Inc. | Flo Health |
| 4 | FTC File No. 192 3050 Docket No. C-4723 | In the Matter of Ortho-Clinical Diagnostics, Inc. | Ortho-Clinical |
| 5 | FTC File No. 192 3092 Docket No. C-4709 | In the Matter of T&M Protection, LLC | T&M Protection |
| 6 | FTC File No. 192 3084 Docket No. C-4704 | In the Matter of TDARX, Inc. | TDARX |
| 7 | FTC File No. 192 3093 Docket No. C-4706 | In the Matter of Global Data Vault, LLC | Global Data |
| 8 | FTC File No. 192 3078 Docket No. C-4703 | In the Matter of Incentive Services, Inc. | Incentive Services |
| 9 | FTC File No. 192 3090 Docket No. C-4705 | In the Matter of Click Labs, Inc. | Click Labs |
| 10 | FTC File No. 182 3192 Docket No. C-4697 | In the Matter of Medable, Inc. | Medable |
| 11 | FTC File No. 182 3189 Docket No. 9386 | In the Matter of NTT Global Data Centers Americas, Inc., as successor in interest to RagingWire Data Centers, Inc. | RagingWire |
| 12 | FTC File No. 182 3196 Docket No. C-4702 | In the Matter of Thru, Inc. | Thru |
| 13 | FTC File No. 182 3188 Docket No. C-4698 | In the Matter of DCR Workforce, Inc. | DCR Workforce |
| 14 | FTC File No. 182 3194 Docket No. C-4700 | In the Matter of LotaData, Inc. | LotaData |
| 15 | FTC File No. 182 3195 Docket No. C-4701 | In the Matter of EmpiriStat, Inc. | EmpiriStat |
| 16 | FTC File No. 182 3193 Docket No. C-4699 | In the Matter of 214 Technologies, Inc., also d/b/a Trueface.ai | Trueface.ai |
| 17 | FTC File No. 182 3107 Docket No. 9383 | In the Matter of Cambridge Analytica, LLC | Cambridge Analytica |
| 18 | FTC File No. 182 3152 Docket No. C-4685 | In the Matter of SecureTest, Inc. | SecurTest |
| 19 | FTC File No. 182 3144 Docket No. C-4664 | In the Matter of VenPath, Inc. | VenPath |

| | | | |
|----|--|--|--------------------------------------|
| 20 | FTC File No. 182 3154 Docket No. C-4666 | In the Matter of SmartStart Employment Screening, Inc. | SmartStart |
| 21 | FTC File No. 182 3143 Docket No. C-4663 | In the Matter of mResourceLLC , d/b/a Loop Works LLC | mResource |
| 22 | FTC File No. 182 3150 Docket No. C-4665 | In the Matter of Idmission LLC | IDmission |
| 23 | FTC File No. 182 3100 Docket No. C-4659 | In the Matter of ReadyTech Corporation | ReadyTech |
| 24 | FTC File No. 172 3173 Docket No. C-4630 | In the Matter of Decusoft, LLC | Decusoft |
| 25 | FTC File No. 172 3171 Docket No. C-4628 | In the Matter of Tru Communication, Inc. | Tru |
| 26 | FTC File No. 172 3172 Docket No. C-4629 | In the Matter of Md7, LLC | Md7 |
| 30 | FTC File No. 152 3198 Docket No. C-4543 | In the Matter of Jhayrmaine Daniels (d/b/a California Skate-Line) | Jhayrmaine Daniels |
| 31 | FTC File No. 152 3190 Docket No. C-4545 | In the Matter of Dale Jarrett Racing Adventure, Inc. | Dale Jarrett |
| 32 | FTC File No. 152 3141 Docket No. C-4540 | In the Matter of Golf Connect, LLC | Golf Connect |
| 33 | FTC File No. 152 3202 Docket No. C-4546 | In the Matter of Inbox Group, LLC | Inbox Group |
| 34 | File No. 152 3187 Docket No. C-4542 | In the Matter of IOActive, Inc. | IOActive |
| 35 | FTC File No. 152 3140 Docket No. C-4549 | In the Matter of Jubilant Clinsys, Inc. | Jubilant |
| 36 | FTC File No. 152 3199 Docket No. C-4547 | In the Matter of Just Bagels Manufacturing, Inc. | Just Bagels |
| 37 | FTC File No. 152 3138 Docket No. C-4548 | In the Matter of NAICS Association, LLC | NAICS |
| 38 | FTC File No. 152 3201 Docket No. C-4544 | In the Matter of One Industries Corp. | One Industries |
| 39 | FTC File No. 152 3137 Docket No. C-4550 | In the Matter of Pinger, Inc. | Pinger |
| 40 | FTC File No. 152 3193 Docket No. C-4552 | In the Matter of SteriMed Medical Waste Solutions | SteriMed |
| 41 | FTC File No. 152 3184 Docket No. C-4541 | In the Matter of Contract Logix, LLC | Contract Logix |
| 42 | FTC File No. 152 3185 Docket No. C-4551 | In the Matter of Forensics Consulting Solutions, LLC | Forensics Consulting |
| 43 | FTC File No. 152 3051 Docket No. C-4526 | In the Matter of American Int'l Mailing, Inc. | AIM |
| 44 | FTC File No. 152 3015 Docket No. C-4525 | In the Matter of TES Franchising, LLC | TES |
| 45 | FTC File No. 142 3036 Docket No. C-4459 | In the Matter of American Apparel, Inc. | American Apparel |

| | | | |
|----|--|--|--------------------------------------|
| 46 | FTC File No. 142 3026 Docket No. C-4469 | In the Matter of Fantage.com, Inc. | Fantage |
| 47 | FTC File No. 142 3017 Docket No. C-4461 | In the Matter of Apperian, Inc. | Apperian |
| 48 | FTC File No. 142 3018 Docket No. C-4462 | In the Matter of Atlanta Falcons Football Club, LLC | Atlanta Falcons |
| 49 | FTC File No. 142 3019 Docket No. C-4463 | In the Matter of Baker Tilly Virchow Krause, LLP | Baker Tilly |
| 50 | FTC File No. 142 3020 Docket No. C-4464 | In the Matter of BitTorrent, Inc. | BitTorrent |
| 51 | FTC File No. 142 3022 Docket No. C-4465 | In the Matter of Charles River Laboratories, Int'l | Charles River |
| 52 | FTC File No. 142 3023 Docket No. C-4466 | In the Matter of DataMotion, Inc. | DataMotion |
| 53 | FTC File No. 142 3024 Docket No. C-4467 | In the Matter of DDC Laboratories, Inc. , d/b/a DNA Diagnostics Center | DDC |
| 54 | FTC File No. 142 3028 Docket No. C-4470 | In the Matter of Level 3 Communications, LLC | Level 3 |
| 55 | FTC File No. 142 3025 Docket No. C-4468 | In the Matter of PDB Sports, Ltd. , d/b/a the Denver Broncos Football Club, LLP | Broncos |
| 56 | FTC File No. 142 3030 Docket No. C-4471 | In the Matter of Reynolds Consumer Products, Inc. | Reynolds |
| 57 | FTC File No. 142 3031 Docket No. C-4472 | In the Matter of Receivable Management Services Corporation | Receivable Mgmt |
| 58 | FTC File No. 142 3032 Docket No. C-4473 | In the Matter of Tennessee Football, Inc. | Tennessee Football |
| 59 | FTC File No. 102 3058 Docket No. C-4369 | In the Matter of Myspace LLC | Myspace |
| 60 | FTC File No. 092 3184 Docket No. C-4365 | In the Matter of Facebook, Inc. | Facebook |
| 61 | FTC File No. 092 3081 Civil Action No. 09-CV- 5276 (C.D. Cal.) | FTC v. Javian Karnani, and Balls of Kryptonite, LLC , d/b/a Bite Size Deals, LLC, and Best Priced Brands, LLC | Balls of Kryptonite |
| 62 | FTC File No. 102 3136 Docket No. C-4336 | In the Matter of Google, Inc. | Google |
| 63 | FTC File No. 092 3137 Docket No. C-4282 | In the Matter of World Innovators, Inc. | World Innovators |
| 64 | FTC File No. 092 3141 Docket No. C-4271 | In the Matter of Progressive Gaitways LLC | Progressive Gaitways |
| 65 | FTC File No. 092 3139 Docket No. C-4270 | In the Matter of Onyx Graphics, Inc. | Onyx Graphics |
| 66 | FTC File No. 092 3138 Docket No. C-4269 | In the Matter of ExpatEdge Partners, LLC | ExpatEdge |
| 67 | FTC File No. 092 3140 Docket No. C-4281 | In the Matter of Directors Desk LLC | Directors Desk |
| 68 | FTC File No. 092 3142 Docket No. C-4272 | In the Matter of Collectify LLC | Collectify |

ANNEX V



THE SECRETARY OF TRANSPORTATION WASHINGTON, DC 20590

July 6, 2023

Commissioner Didier Reynders
European Commission
Rue de la Loi / Wetstraat 200
1049 1049 Brussels
Belgium

Dear Commissioner Reynders:

The United States Department of Transportation (“Department” or “DOT”) appreciates the opportunity to describe its role in enforcing the EU-U.S. Data Privacy Framework (“EU-U.S. DPF”) Principles. The EU-U.S. DPF will play a critical role in protecting personal data provided during commercial transactions in an increasingly interconnected world. It will enable businesses to conduct important operations in the global economy, while at the same time ensuring that EU consumers retain important privacy protections.

The DOT first publicly expressed its commitment to enforcement of the U.S.-EU Safe Harbor Framework in a letter sent to the European Commission over 22 years ago, commitments that were repeated and expanded upon in a 2016 letter regarding the EU-U.S. Privacy Shield Framework. The DOT pledged to vigorously enforce the U.S.-EU Safe Harbor Privacy Principles, and then the EU-U.S. Privacy Shield Principles, in those letters. The DOT extends this commitment to the EU-U.S. DPF Principles and this letter memorializes that commitment.

Notably, the DOT confirms its commitment in the following key areas: (1) prioritizing investigation of alleged EU-U.S. DPF Principles violations; (2) appropriate enforcement action against entities making false or deceptive claims of EU-U.S. DPF participation; and (3) monitoring and making public enforcement orders concerning EU-U.S. DPF Principles violations. We provide information about each of these commitments and, for necessary context, pertinent background about the DOT’s role in protecting consumer privacy and enforcing the EU-U.S. DPF Principles.

1. Background

A. DOT’s Privacy Authority

The Department is strongly committed to ensuring the privacy of information provided by consumers to airlines and ticket agents. The DOT’s authority to take action in this area is found in 49 U.S.C. 41712, which prohibits a carrier or ticket agent from engaging in “an unfair or deceptive practice” in air transportation or the sale of air transportation. Section 41712 is patterned after Section 5 of the Federal Trade Commission (FTC) Act (15 U.S.C. 45). Recently, DOT issued regulations defining unfair and deceptive practices, consistent with both DOT and FTC precedent (14 CFR § 399.79). Specifically, a practice is “unfair” if it causes or is likely to cause substantial injury, which is not reasonably avoidable, and the harm is not outweighed by benefits to consumers or competition. A practice is “deceptive” to consumers if it is likely to

mislead a consumer, acting reasonably under the circumstances, with respect to a material matter. A matter is material if it is likely to have affected the consumer's conduct or decision with respect to a product or service. Aside from these general principles, DOT specifically interprets section 41712 as prohibiting carriers and ticket agents from: (1) violating the terms of its privacy policy; (2) violating any rule issued by the Department that identifies specific privacy practices as unfair or deceptive; or (3) violating the Children's Online Privacy Protection Act (COPPA) or FTC rules implementing COPPA; or (4) failing, as a participant in the EU-U.S. DPF, to comply with the EU-U.S. DPF Principles.¹

As noted above, under federal law, the DOT has exclusive authority to regulate the privacy practices of airlines, and it shares jurisdiction with the FTC with respect to the privacy practices of ticket agents in the sale of air transportation.

As such, once a carrier or seller of air transportation publicly commits to the EU-U.S. DPF Principles, the Department is able to use the statutory powers of section 41712 to ensure compliance with those principles. Therefore, once a passenger provides information to a carrier or ticket agent that has committed to honoring the EU-U.S. DPF Principles, any failure to do so by the carrier or ticket agent would be a violation of section 41712.

B. Enforcement Practices

The Department's Office of Aviation Consumer Protection ("OACP")² investigates and prosecutes cases under 49 U.S.C. 41712. It enforces the statutory prohibition in section 41712 against unfair and deceptive practices primarily through negotiation, preparing cease and desist orders, and drafting orders assessing civil penalties. The office learns of potential violations largely from complaints it receives from individuals, travel agents, airlines, and U.S. and foreign government agencies. Consumers may use the DOT's website to file privacy complaints against airlines and ticket agents.³

If a reasonable and appropriate settlement in a case is not reached, OACP has the authority to institute an enforcement proceeding involving an evidentiary hearing before a DOT administrative law judge ("ALJ"). The ALJ has the authority to issue cease-and-desist orders and civil penalties. Violations of section 41712 can result in the issuance of cease and desist orders and the imposition of civil penalties of up to \$37,377 for each violation of section 41712.

The Department does not have the authority to award damages or provide pecuniary relief to individual complainants. However, the Department does have the authority to approve settlements resulting from investigations brought by its OACP that directly benefit consumers (e.g., cash, vouchers) as an offset to monetary penalties otherwise payable to the U.S. Government. This has occurred in the past, and may also occur in the context of the EU-U.S. DPF Principles when circumstances warrant. Repeated violations of section 41712 by an airline would also raise questions regarding the airline's compliance disposition which could, in egregious situations, result in an airline being found to be no longer fit to operate and, therefore, losing its economic operating authority.

To date, the DOT has received relatively few complaints involving alleged privacy violations by ticket agents or airlines. When they arise, they are investigated according to the principles set forth above.

¹ <https://www.transportation.gov/individuals/aviation-consumer-protection/privacy>.

² Formerly known as the Office of Aviation Enforcement and Proceedings.

³ <http://www.transportation.gov/airconsumer/privacy-complaints>.

C. DOT Legal Protections Benefiting EU Consumers

Under section 41712, the prohibition on unfair or deceptive practices in air transportation or the sale of air transportation applies to U.S. and foreign air carriers as well as ticket agents. The DOT frequently takes action against U.S. and foreign airlines for practices that affect both foreign and U.S. consumers on the basis that the airline's practices took place in the course of providing transportation to or from the United States. The DOT does and will continue to use all remedies that are available to protect both foreign and U.S. consumers from unfair or deceptive practices in air transportation by regulated entities.

The DOT also enforces, with respect to airlines, other targeted laws whose protections extend to non-U.S. consumers such as the Children's Online Privacy Act ("COPPA"). Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under 13 provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. To the extent that U.S. or foreign airlines doing business in the United States violate COPPA, the DOT would have jurisdiction to take enforcement action.

II. **EU-U.S. DPF Principles Enforcement**

If an airline or ticket agent chooses to participate in the EU-U.S. DPF and the Department receives a complaint that such an airline or ticket agent had allegedly violated the EU-U.S. DPF Principles, the Department would take the following steps to vigorously enforce the EU-U.S. DPF Principles.

A. Prioritizing Investigation of Alleged Violations

The Department's OACP will investigate each complaint alleging EU-U.S. DPF Principles violations, including complaints received from EU data protection authorities ("DPAs") and take enforcement action where there is evidence of a violation. Further, OACP will cooperate with the FTC and Department of Commerce and place a priority on allegations that the regulated entities are not complying with privacy commitments made as part of the EU-U.S. DPF.

Upon receipt of an allegation of a violation of the EU-U.S. DPF Principles, OACP may take a range of actions as part of its investigation. For example, it may review the ticket agent or airline's privacy policies, obtain further information from the ticket agent or airline or from third parties, follow up with the referring entity, and assess whether there is a pattern of violations or significant number of consumers affected. In addition, it would determine whether the issue implicates matters within the purview of the Department of Commerce or FTC, assess whether consumer education and business education would be helpful, and as appropriate, initiate an enforcement proceeding.

If the Department becomes aware of potential EU-U.S. DPF Principles violations by ticket agents, it will coordinate with the FTC on the matter. We will also advise the FTC and the Department of Commerce of the outcome of any EU-U.S. DPF Principles enforcement action.

B. Addressing False or Deceptive Participation Claims

The Department remains committed to investigating EU-U.S. DPF Principles violations, including false or deceptive claims of participation in the EU-U.S. DPF. We will give priority consideration to referrals from the Department of Commerce regarding organizations that it identifies as improperly holding themselves out to be EU-U.S. DPF participants or using the EU-U.S. DPF certification mark without authorization.

In addition, we note that if an organization's privacy policy promises that it complies with the EU-U.S. DPF Principles, its failure to make or maintain a self-certification through the Department of Commerce likely will not, by itself, excuse the organization from DOT enforcement of those commitments.

C. Monitoring and Making Public Enforcement Orders Concerning EU-U.S. DPF Violations

The Department's OACP also remains committed to monitoring enforcement orders as needed to ensure compliance with the EU-U.S. DPF Principles. Specifically, if the office issues an order directing an airline or ticket agent to cease and desist from future violations of the EU-U.S. DPF Principles and section 41712, it will monitor the entity's compliance with the cease-and-desist provision in the order. In addition, the office will ensure that orders resulting from EU-U.S. DPF Principles cases are available on its website.

We look forward to our continued work with our federal partners and EU stakeholders on EU-U.S. DPF matters.

I hope that this information proves helpful. If you have any questions or need further information, please feel free to contact me.

Sincerely,



Pete Buttigieg

ANNEX VI



U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General

Washington, D.C. 20530

June 23, 2023

Ms. Ana Gallego Torres
Director-General for Justice and Consumers
European Commission
Rue Montoyer/Montoyerstraat 59
1049 Brussels
Belgium

Dear Ms. Director-General Gallego Torres:

This letter provides a brief overview of the primary investigative tools used to obtain commercial data and other record information from corporations in the United States for criminal law enforcement or public interest (civil and regulatory) purposes, including the access limitations set forth in those authorities.¹ All the legal processes described in this letter are nondiscriminatory in that they are used to obtain information from corporations in the United States, including from companies that will self-certify through the EU-U.S. Data Privacy Framework, without regard to the nationality or place of residence of the data subject. Further, corporations that receive legal process in the United States may challenge it in court as discussed below.²

Of particular note with respect to the seizure of data by public authorities is the Fourth Amendment to the United States Constitution, which provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. As the United States Supreme Court

¹ This overview does not describe the national security investigative tools used by law enforcement in terrorism and other national security investigations, including National Security Letters (NSLs) for certain record information in credit reports, financial records, and electronic subscriber and transaction records, 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, and for electronic surveillance, search warrants, business records, and other collection of information pursuant to the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq.

² This letter discusses federal law enforcement and regulatory authorities. Violations of state law are investigated by state law enforcement authorities and are tried in state courts. State law enforcement authorities use warrants and subpoenas issued under state law in essentially the same manner as described herein, but with the possibility that state legal process may be subject to additional protections provided by state constitutions or statutes that exceed those of the U.S. Constitution. State law protections must be at least equal to those of the U.S. Constitution, including but not limited to the Fourth Amendment.

stated in *Berger v. State of New York*, "[t]he basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." 388 U.S. 41, 53 (1967) (citing *Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). In domestic criminal investigations, the Fourth Amendment generally requires law enforcement officers to obtain a court-issued warrant before conducting a search. See *Katz v. United States*, 389 U.S. 347, 357 (1967). Standards for the issuance of a warrant, such as the probable cause and particularity requirements, apply to warrants for physical searches and seizures as well as to warrants for the stored content of electronic communications issued under the Stored Communications Act as discussed below. When the warrant requirement does not apply, government activity is still subject to a "reasonableness" test under the Fourth Amendment. The Constitution itself, therefore, ensures that the U.S. government does not have limitless, or arbitrary, power to seize private information.³

Criminal Law Enforcement Authorities:

Federal prosecutors, who are officials of the Department of Justice (DOJ), and federal investigative agents including agents of the Federal Bureau of Investigation (FBI), a law enforcement agency within DOJ, are able to compel production of documents and other record information from corporations in the United States for criminal investigative purposes through several types of compulsory legal processes, including grand jury subpoenas, administrative subpoenas, and search warrants, and may acquire other communications pursuant to federal criminal wiretap and pen register authorities.

Grand Jury or Trial Subpoenas: Criminal subpoenas are used to support targeted law enforcement investigations. A grand jury subpoena is an official request issued from a grand jury (usually at the request of a federal prosecutor) to support a grand jury investigation into a particular suspected violation of criminal law. Grand juries are an investigative arm of the court and are empaneled by a judge or magistrate. A subpoena may require someone to testify at a proceeding, or to produce or make available business records, electronically stored information, or other tangible items. The information must be relevant to the investigation and the subpoena cannot be unreasonable because it is overbroad, or because it is oppressive or burdensome. A recipient can file a motion to challenge a subpoena based on those grounds. See Fed. R. Crim. P. 17. In limited circumstances, trial subpoenas for documents may be used after the case has been indicted by the grand jury.

Administrative Subpoena Authority: Administrative subpoena authorities may be exercised in criminal or civil investigations. In the criminal law enforcement context, several federal statutes authorize the use of administrative subpoenas to produce or make available business records, electronically stored information, or other tangible items relevant to investigations involving health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations implicating government agencies. If the government seeks to enforce an administrative subpoena in court, the recipient of the administrative subpoena, like the recipient of a grand jury subpoena, can argue that the subpoena is unreasonable because it is overbroad, or because it is oppressive or burdensome.

³ With respect to the Fourth Amendment principles on safeguarding privacy and security interests that are discussed above, U.S. courts regularly apply those principles to new types of law enforcement investigative tools that are enabled by developments in technology. For example, in 2018 the Supreme Court ruled that the government's acquisition in a law enforcement investigation of historical cell-site location information from a cell phone company for an extended period of time is a "search" subject to the Fourth Amendment warrant requirement. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

Court Orders For Pen Register and Trap and Traces: Under criminal pen register and trap-and-trace provisions, law enforcement may obtain a court order to acquire real-time, non-content dialing, routing, addressing, and signaling information about a phone number or email upon certification that the information provided is relevant to a pending criminal investigation. See 18 U.S.C. §§ 3121-3127. The use or installation of such a device outside the law is a federal crime.

Electronic Communications Privacy Act (ECPA): Additional rules govern the government's access to subscriber information, traffic data, and stored content of communications held by internet service providers (also known as "ISPs"), telephone companies, and other third-party service providers, pursuant to Title II of ECPA, also called the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712. The SCA sets forth a system of statutory privacy rights that limit law enforcement access to data beyond what is required under Constitutional law from customers and subscribers of ISPs. The SCA provides for increasing levels of privacy protections depending on the intrusiveness of the collection. For subscriber registration information, Internet Protocol (IP) addresses and associated time stamps, filed billing information, criminal law enforcement authorities must obtain a subpoena. For most other stored, non-content information, such as email headers without the subject line, law enforcement must present specific facts to a judge demonstrating that the requested information is relevant and material to an ongoing criminal investigation. To obtain the stored content of electronic communications, generally, criminal law enforcement authorities must obtain a warrant from a judge based on probable cause to believe the account in question contains evidence of a crime. The SCA also provides for civil liability and criminal penalties.⁴

Court Orders for Surveillance Pursuant to Federal Wiretap Law: Additionally, law enforcement may intercept in real time wire, oral, or electronic communications for criminal investigative purposes pursuant to the federal wiretap law. See 18 U.S.C. §§ 2510-2523. This authority is available only pursuant to a court order in which a judge finds, inter alia, that there is probable cause to believe that the wiretap or electronic interception will produce evidence of a federal crime, or the whereabouts of a fugitive fleeing from prosecution. The statute provides for civil liability and criminal penalties for violations of the wiretapping provisions.

Search Warrant-Fed. R. Crim. P. Rule 41: Law enforcement can physically search premises in the United States when authorized to do so by a judge. Law enforcement must demonstrate to the judge based on a showing of probable cause that a crime was committed or is about to be committed and that items connected to the crime are likely to be found in the place specified by the warrant. This authority is often used when a physical search by police of a premise is needed due to the danger that evidence may be destroyed if a subpoena or other production order is served on the corporation. A person subject to a search or whose property is subject to a search may move to suppress evidence obtained or derived from an unlawful search if that evidence is introduced against that person during a criminal trial. See *Mapp v. Ohio*, 367 U.S. 643 (1961). When a data holder is required to disclose data pursuant to a

⁴ In addition, section 2705(b) of the SCA authorizes the government to obtain a court order, based on a demonstrated need for protection from disclosure, prohibiting a communications services provider from voluntarily notifying its users of the receipt of SCA legal process. In October 2017, Deputy Attorney General Rod Rosenstein issued a memorandum to DOJ attorneys and agents setting out guidance to ensure that applications for such protective orders are tailored to the specific facts and concerns of an investigation and establishing a general one-year ceiling on how long an application may seek to delay notice. In May 2022, Deputy Attorney General Lisa Monaco issued supplementary guidance on the topic, which among other matters established internal DOJ approval requirements for applications to extend a protective order beyond the initial one-year period and required the termination of protective orders at the close of an investigation.

warrant, the compelled party may challenge the requirement to disclose as unduly burdensome. See *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (holding that "due process requires a hearing on the issue of burdensomeness before compelling a telephone company to provide" assistance with a search warrant); *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980) (reaching same conclusion based on court's supervisory authority).

DOJ Guidelines and Policies: In addition to these Constitutional, statutory, and rule-based limitations on government access to data, the Attorney General has issued guidelines that place further limits on law enforcement access to data, and that also contain privacy and civil liberties protections. For instance, the Attorney General's Guidelines for Domestic FBI Operations (September 2008) (hereinafter AG FBI Guidelines), available at <http://www.justice.gov/archive/opa/docs/guidelines.pdf>, set limits on use of investigative means to seek information related to investigations that involve federal crimes. These guidelines require that the FBI use the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties and the potential damage to reputation. Further, they note that "it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into . the lives of law-abiding people." AG FBI Guidelines at 5. The FBI has implemented these guidelines through the FBI Domestic Investigations and Operations Guide (DIOG), available at <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29>, a comprehensive manual that includes detailed limits on use of investigative tools and guidance to assure that civil liberties and privacy are protected in every investigation. Additional rules and policies that prescribe limitations on the investigative activities of federal prosecutors are set out in the Justice Manual, also available online at <https://www.justice.gov/jm/justicemanual>.

Civil and Regulatory Authorities (Public Interest):

There are also significant limits on civil or regulatory (i.e., "public interest") access to data held by corporations in the United States. Agencies with civil and regulatory responsibilities may issue subpoenas to corporations for business records, electronically stored information, or other tangible items. These agencies are limited in their exercise of administrative or civil subpoena authority not only by their organic statutes, but also by independent judicial review of subpoenas prior to potential judicial enforcement. See, e.g., Fed. R. Civ. P. 45. Agencies may seek access only to data that is relevant to matters within their scope of authority to regulate. Further, a recipient of an administrative subpoena may challenge the enforcement of that subpoena in court by presenting evidence that the agency has not acted in accordance with basic standards of reasonableness, as discussed earlier.

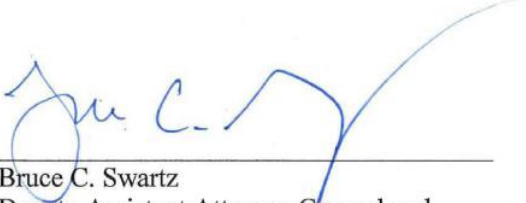
There are other legal bases for companies to challenge data requests from administrative agencies based on their specific industries and the types of data they possess. For example, financial institutions can challenge administrative subpoenas seeking certain types of information as violations of the Bank Secrecy Act and its implementing regulations. 31 U.S.C. § 5318; 31 C.F.R. Chapter X. Other businesses can rely on the Fair Credit Reporting Act, 15 U.S.C. § 1681b, or a host of other sector specific laws. Misuse of an agency's subpoena authority can result in agency liability, or personal liability for agency officers. See, e.g., Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3423. Courts in the United States thus stand as the guardians against improper regulatory requests and provide independent oversight of federal agency actions.

Finally, any statutory power that administrative authorities have to physically seize

records from a company in the United States pursuant to an administrative search must meet requirements based on the Fourth Amendment. See *See v. City of Seattle*, 387 U.S. 541 (1967).

Conclusion:

All law enforcement and regulatory activities in the United States must conform to applicable law, including the U.S. Constitution, statutes, rules, and regulations. Such activities must also comply with applicable policies, including any Attorney General Guidelines governing federal law enforcement activities. The legal framework described above limits the ability of U.S. law enforcement and regulatory agencies to acquire information from corporations in the United States-whether the information concerns U.S. persons or citizens of foreign countries-and in addition permits judicial review of any government requests for data pursuant to these authorities.



Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

ANNEX VII

OFFICE OF THE DIRECTOR OF NATIONAL
INTELLIGENCE OFFICE OF GENERAL
COUNSEL

WASHINGTON, DC 20511

December 9, 2022

Leslie B. Kiernan
General Counsel
U.S. Department of
Commerce 1401 Constitution
Ave., NW Washington, DC
20230

Dear Ms. Kiernan,

On October 7, 2022, President Biden signed Executive Order 14086, *Enhancing Safeguards for United States Signals Intelligence Activities*, which bolsters the rigorous array of privacy and civil liberties safeguards that apply to U.S. signals intelligence activities. These safeguards include: requiring signals intelligence activities to meet enumerated legitimate objectives; explicitly barring such activities for the purpose of specific prohibited objectives; putting in place novel procedures for ensuring that signals intelligence activities further these legitimate objectives and do not further prohibited objectives; requiring that signals intelligence activities be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority and only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized; and directing Intelligence Community (IC) elements to update their policies and procedures to reflect the Executive Order's required signals intelligence safeguards. Most significantly, the Executive Order also introduces an independent and binding mechanism enabling individuals from "qualifying states," as designated pursuant to the Executive Order, to seek redress if they believe they were subjected to unlawful U.S. signals intelligence activities, including activities violating the protections found in the Executive Order.

President Biden's issuance of Executive Order 14086 marked the culmination of well over a year of detailed negotiations between representatives from the European Commission (EC) and the United States and directs the steps the United States will take to implement its commitments under the EU-U.S. Data Privacy Framework. Consistent with the cooperative spirit that produced the Framework, it is my understanding that you have received two sets of questions from the EC about

how the IC will implement the Executive Order. I am happy to address these questions with this letter.

Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA Section 702)

The first set of questions concerns FISA Section 702, which allows the collection of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States with the compelled assistance of electronic communication service providers. Specifically, the questions concern the interplay between that provision and Executive Order 14086, as well as the other safeguards that apply to activities conducted pursuant to FISA Section 702.

To begin, we can confirm that the IC will apply the safeguards set forth in Executive Order 14086 to activities conducted pursuant to FISA Section 702.

In addition, numerous other safeguards apply to the Government's use of FISA Section 702. For example, all FISA Section 702 certifications must be signed by both the Attorney General and Director of National Intelligence (DNI), and the Government must submit all such certifications for approval by the Foreign Intelligence Surveillance Court (FISC), which is comprised of independent, life-tenured judges who serve non-renewable seven-year terms. The certifications identify categories of foreign intelligence information to be collected, which must meet the statutory definition of foreign intelligence information, through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The certifications have included information concerning international terrorism and other topics, such as the acquisition of information concerning weapons of mass destruction. Each annual certification must be submitted to the FISC for approval in a certification application package that includes the Attorney General's and DNI's certifications, affidavits by certain heads of intelligence agencies, and targeting procedures, minimization procedures, and querying procedures that are binding on the Government. The targeting procedures require, among other things, that the IC reasonably assess, based on the totality of the circumstances, that the targeting will likely lead to the collection of foreign intelligence information identified in a FISA Section 702 certification.

Moreover, when collecting information pursuant to FISA Section 702, the IC must: provide a written explanation of the basis for their assessment, at the time of targeting, that the target is expected to possess, is expected to receive, or is likely to communicate foreign intelligence information identified in a FISA Section 702 certification; confirm that the targeting standard as set forth in FISA Section 702 targeting procedures remains satisfied; and cease collection if the standard is no longer satisfied. *See U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements*, at 2-3 (July 15, 2015).

Requiring the IC to record in writing, and regularly affirm the validity of, its assessment that FISA Section 702 targets meet the applicable targeting standards facilitates the FISC's supervision of the IC's targeting activities. Each recorded targeting assessment and rationale is reviewed on a bimonthly basis by intelligence oversight attorneys in the Department of Justice (DOJ), who conduct this oversight function independently from foreign intelligence operations. The DOJ section performing this

function is then responsible under a long-established FISC rule to report to the FISC any violations of the applicable procedures. This reporting, along with regular meetings between the FISC and this DOJ section regarding oversight of FISA Section 702 targeting, enables the FISC to enforce compliance with the FISA Section 702 targeting and other procedures and otherwise ensure that the Government's activities are lawful. In particular, the FISC can do this in a number of ways, including by issuing binding remedial decisions to terminate the Government's authority to collect against a particular target, or to modify or delay FISA Section 702 data collection. The FISC also can require the Government to provide further reporting or briefing on its compliance with targeting and other procedures or require changes to those procedures.

The "Bulk" Collection of Signals Intelligence

The second set of questions concerns the "bulk" collection of signals intelligence, which is defined by Executive Order 14086 as "the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms)."

With respect to these questions, we first note that neither FISA nor National Security Letters authorize bulk collection. With respect to FISA:

- Titles I and III of FISA, which respectively authorize electronic surveillance and physical searches, require a court order (with limited exceptions, such as emergency circumstances) and always require probable cause to believe that the target is a foreign power or an agent of a foreign power. *See* 50 U.S.C. §§ 1805, 1824.
- The USA FREEDOM Act of 2015 amended Title IV of FISA, which authorizes the use of pen registers and trap and trace devices, pursuant to court order (except in emergency circumstances), to require the Government to base requests on a "specific selection term." *See* 50 U.S.C. § 1842(c)(3).
- Title V of FISA, which permits the Federal Bureau of Investigation (FBI) to obtain certain types of business records, requires a court order based on an application that specifies that "there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." *See* 50 U.S.C. § 1862(b)(2)(B).¹
- Finally, FISA Section 702 authorizes the "targeting of persons reasonably

¹ From 2001 until 2020, Title V of FISA permitted the FBI to seek authorization from the FISC to obtain "tangible things" that are relevant to certain authorized investigations. *See* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001). This language, which has sunset and is thus no longer the law, provided the authority pursuant to which the Government at one time collected telephony metadata in bulk. Even before the provision sunset, however, the USA FREEDOM Act had amended it to require the Government to base an application to the FISC on a "specific selection term." *See* USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, § 103 (2015).

believed to be located outside the United States to acquire foreign intelligence information." *See* 50 U.S.C. § 1881a(a). Thus, as the Privacy and Civil Liberties Oversight Board has noted, the Government's collection of data under FISA Section 702 "consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence," such that the "program does not operate by collecting communications in bulk." Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, at 103 (July 2, 2014).²

With respect to National Security Letters, the USA FREEDOM Act of 2015 imposes a "specific selection term" requirement on the use of such letters. *See* 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b).

Further, Executive Order 14086 provides that "[t]argeted collection shall be prioritized" and that, when the IC does conduct bulk collection, the "bulk collection of signals intelligence shall be authorized only based on a determination ... that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection." *See* Executive Order 14086, § 2(c)(ii)(A).

Moreover, when the IC determines that bulk collection satisfies these standards, Executive Order 14086 provides additional safeguards. Specifically, the Executive Order requires the IC, when conducting bulk collection, to "apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information." *See id.* The Order also states that "signals intelligence activities," which include the querying of signals intelligence obtained by bulk collection, "shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority." *See id.* § 2(a)(ii)(A). The Order further implements this principle by stating that the IC may only query unminimized signals intelligence obtained in bulk in pursuit of six permissible objectives, and that such queries must be conducted according to policies and procedures that "appropriately take into account the impact [of the queries] on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside." *See id.* § 2(c)(iii)(D). Lastly, the Order provides for handling, security, and access controls for data collected. *See id.* § 2(c)(iii)(A) and § 2(c)(iii)(B).

* * * * *

We hope these clarifications are of assistance. Please do not hesitate to contact us if you have further questions about how the U.S. IC plans to implement Executive Order 14086.

² Sections 703 and 704, which authorize the IC to target U.S. persons located overseas, require a court order (except in emergency circumstances) and always require probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power. *See* 50 U.S.C. §§ 1881b, 1881c.

Sincerely,

A handwritten signature in black ink, appearing to read 'C. Fonzone', followed by a vertical line on the right side.

Christopher C. Fonzone
General Counsel



Brussels, 10.7.2023
C(2023) 4745 final

ANNEX 8

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

**pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
on the adequate level of protection of personal data under the EU-US Data Privacy
Framework**

ANNEX VIII

List of abbreviations

The following abbreviations appear in this Decision:

| | |
|--------------------|---|
| AAA | American Arbitration Association |
| AG Regulation | Attorney General Regulation on the Data Protection Review Court |
| AGG-DOM | Attorney General Guidelines for Domestic FBI Operations |
| APA | Administrative Procedure Act |
| CIA | Central Intelligence Agency |
| CNSS | Committee on National Security Systems |
| Court of Justice | Court of Justice of the European Union |
| Decision | Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework |
| DHS | Department of Homeland Security |
| DNI | Director of National Intelligence |
| DoC | U.S. Department of Commerce |
| DoJ | U.S. Department of Justice |
| DoT | U.S. Department of Transportation |
| DPA | Data Protection Authority |
| DPF List | Data Privacy Framework List |
| DPRC | Data Protection Review Court |
| ECOA | Equal Credit Opportunity Act |
| ECPA | Electronic Communications Privacy Act |
| EEA | European Economic Area |
| EO 12333 | Executive Order 12333 ‘United States Intelligence Activities’ |
| EO 14086, the EO | Executive Order 14086 ‘Enhancing Safeguards for US Signals Intelligence Activities’ |
| EU-U.S. DPF or DPF | EU-U.S. Data Privacy Framework |
| EU-U.S. DPF Panel | EU-U.S. Data Privacy Framework Panel |
| FBI | Federal Bureau of Investigation |
| FCRA | Fair Credit Reporting Act |

| | |
|--------------------------|---|
| FISA | Foreign Intelligence Surveillance Act |
| FISC | Foreign Intelligence Surveillance Court |
| FISCR | Foreign Intelligence Surveillance Court of Review |
| FOIA | Freedom of Information Act |
| FRA | Federal Records Act |
| FTC | U.S. Federal Trade Commission |
| HIPAA | Health Insurance Portability and Accountability Act |
| ICDR | International Centre for Dispute Resolution |
| IOB | Intelligence Oversight Board |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NSL | National Security Letter(s) |
| ODNI | Office of the Director of National Intelligence |
| ODNI CLPO, CLPO | Civil Liberties Protection Officer of the Director of National Intelligence |
| OMB | Office of Management and Budget |
| OPCL | Office of Privacy and Civil Liberties of the Department of Justice |
| PCLOB | Privacy and Civil Liberties Oversight Board |
| PIAB | President's Intelligence Advisory Board |
| PPD 28 | Presidential Policy Directive 28 |
| Regulation (EU) 2016/679 | 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 |
| SAOP | Senior Agency Official for Privacy |
| The Principles | EU-U.S. Data Privacy Framework Principles |
| U.S. | United States |
| Union | European Union |