

**TO THE PRESIDENT AND MEMBERS  
OF THE COURT OF JUSTICE  
OF THE EUROPEAN UNION**

IN CASE C-311/18

***DATA PROTECTION COMMISSIONER***

*Plaintiff*

**V.**

***FACEBOOK IRELAND LTD and  
MAXIMILIAN SCHREMS***

*Defendants*

**AND**

***the Government of the United States of America,  
Digital Europe, the Business Software Alliance and EPIC***

*Amicus curiae*

---

**WRITTEN OBSERVATIONS OF MAXIMILLIAN SCHREMS**

**Attachment 8**

**Expert Review by Prof. Franziska Boeham**

---

Prof. Dr. Franziska Boehm  
FIZ Karlsruhe – Leibniz-Institute for Information Infrastructure/Karlsruhe Institute of Technology  
Professor of law

# LEGAL EXPERTISE ON THE ADEQUACY OF THE PRIVACY SHIELD

---

Comparison between the GDPR and the Privacy  
Shield, Case C - 311/18

August 2018

## Content

I. SCOPE AND APPLICATION .....	4
1. Scope.....	4
2. Applicable Law .....	5
3. Exceptions.....	7
4. SUMMARY: APPLICATION AND SCOPE.....	9
II. MATERIAL PROTECTION .....	10
1. Data Quality .....	10
2. Legitimate Processing .....	12
3. Onward Transfer .....	15
4. SUMMARY: MATERIAL PROTECTION .....	19
III. RIGHT OF ACCESS.....	20
IV. ENFORCEMENT .....	24
1. Remedies .....	24
2. Sanctions.....	27
3. Supervisory Authority / Enforcement .....	29
4. SUMMARY: ENFORCEMENT .....	30
V. CONCLUSION .....	31

### Abbreviations used

**CFR** = Charter of Fundamental Rights of the European Union

**Directive 95/46** = Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281/31

**ECHR** = European Convention on Human Rights

**ECtHR** = European Court of Human Rights

**GDPR** = General Data Protection Regulation

**Privacy Shield** = 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 (notified under document C(2016) 4176), OJ L 207, 1.8.2016, p. 1–112

**US** = United States

Other abbreviations relating to specific measures are explained in the text.

The expertise includes a brief comparison between the basic data protection guarantees of the GDPR and the guarantees stipulated by the Privacy Shield. It focuses on the challenges in the commercial sector. It should give a quick overview of the most important data protection principles in both instruments and serve as background information for the written observations, in which the national security issues of the Privacy Shield are already addressed.

Starting point for the expertise are the provisions of the GDPR allowing the transfer of personal data of EU citizens to a third state. For this purpose, Article 45 GDPR requires an adequate level of protection in the third country. As the CJEU in the Schrems case (C-362/14) stipulated “the term ‘adequate level of protection’ must be understood as requiring the third country in fact to ensure, (...) a level of protection of fundamental rights and freedoms that is **essentially equivalent** to that guaranteed within the European Union”.<sup>1</sup> However, the level of protection does not have to be “identical to that guaranteed in the EU legal order”.<sup>2</sup> In consequence, minor differences of the level of protection can occur. The respect of basic and essentially equivalent data protection guarantees, however, has to be guaranteed by the third country to avoid that the level of protection of natural persons guaranteed by the GDPR is not undermined (compare Art. 44 GDPR). When assessing the adequacy, the following, exemplarily mentioned, criteria stipulated in Article 45 para 2 GDPR play a role.

- (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
- (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data

It results from Art. 45 para 1 GDPR that the Commission can adopt an adequacy decision for an entire third country, but also for “one or more specified sectors within that third country”. The same procedure was already possible under the former Directive 95/45. As the data protection framework in the US as an entire country could not be assessed as adequate, a specific regime, the Privacy Shield, was put in place to enable data transfer in specific situations (specific sectors). The Privacy Shield is the successor of the Safe Harbor Decision, which was declared invalid by the CJEU in 2015.

The following analysis is not intended to be exhaustive. It focuses on the commercial aspects of the Privacy Shield. It includes a comparison of the most important EU data protection principles with the Privacy Shield guarantees. Both instruments are illustrated by means of comparative tables.

---

<sup>1</sup> C-362/14 – Schrems, Judgment of the Court (Grand Chamber) of 6 October 2015 ECLI:EU:C:2015:650, para 73 and recital (104) GDPR.

<sup>2</sup> Ibid.

## I. SCOPE AND APPLICATION

### 1. Scope

The GDPR has a broad application to all private and public controllers and processors of personal data within the EU and beyond. The only activities that fall outside of the scope of European Law (e.g. states security, law enforcement and defence) are not governed by the GDPR under Article 2, but will usually be governed by the ECHR, CFR and/or national constitutional laws of the Member States.

Naturally the self-certification system of the Privacy Shield only applies to certified organizations established in the United States. This means that contrary to the GDPR, all government authorities and all non-certified organizations within the United States are not covered by the system. As soon as data is transferred to a non-certified entity, the guarantees of the Privacy Shield do not apply.

GDPR

**Article 2  
Material Scope**

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:  
 (a) in the course of an activity which falls outside the scope of Union law;  
 (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;  
 (c) by a natural person in the course of a purely personal or household activity;  
 (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences (...).

Privacy Shield

**Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce I. Overview (1)**

“(…) the Department of Commerce is issuing these Privacy Shield Principles (...) under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). (...) They are intended for use solely by organizations in the United States receiving personal data from the European Union for the purpose of qualifying for the Privacy Shield and thus benefitting from the European Commission’s adequacy decision. The Principles do not affect the application of national provisions implementing Directive 95/46/EC (“the Directive”) that apply to the processing of personal data in the Member States. Nor do the Principles limit privacy obligations that otherwise apply under U.S. law.”

**Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce I. Overview (2)**

In order to rely on the Privacy Shield to effectuate transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the Department of Commerce (...). While decisions by organizations to thus enter the Privacy Shield are entirely voluntary, effective compliance is compulsory (...)

	<p><b>Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce I. Overview (5)</b></p> <p>Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, (...); or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations (...)</p> <p><b>Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce I. Overview (6)</b></p> <p>Organizations are obligated to apply the Principles to all personal data transferred in reliance on the Privacy Shield after they enter the Privacy Shield.</p>
--	---

**COMPARISON:**

The GDPR applies to both the offering of goods or services within the EU and to the monitoring of data subjects' behaviors that take place within the EU regardless of where the controller or processor is located. In comparison, the Privacy Shield only applies to the US entities that have self-certified. Under the GDPR, the transfer of data to another entity falls under the general limitations of any "processing operation". Transfers outside of the area that is governed by the GDPR (countries that are not members of the EU/EEA) fall under additional limitations under Articles 44 and 49 of the GDPR. The Privacy Shield does not foresee any limitations on onward transfer other than "notice and choice", which effectively means that data subjects must have an option to "opt out" of an onward transfer (see further below). Furthermore, the material scope of the Privacy Shield still excludes some specific sectors (as financial services, transport, telecommunications), which are not authorized to join the process of self-certification, because the FTC lacks jurisdiction over them.

**2. Applicable Law**

The GDPR is to be interpreted within EU law and primary legislation, such as Articles 7 and 8 CFR and Article 8 ECHR. Following the system of a US self-certification system, the Privacy Shield is governed and interpreted under US law. In consequence, in cases of doubts relating to the interpretation and applicability of data protection principles in the framework of the Privacy Shield, only US law applies. Only if an US organization has submitted itself to the jurisdiction of a European Data Protection Authority, it is to be interpreted under EU law.

GDPR	Privacy Shield
<p style="text-align: center;"><b>Article 3: Territorial Scope</b></p> <p>1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.</p> <p>2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (1) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (2) the monitoring of their behaviour as far as their behaviour takes place within the Union.</p> <p>3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.</p>	<p style="text-align: center;"><b>Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce I. Overview (7)</b></p> <p>U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with European data protection authorities (“DPAs”). Unless otherwise stated, all provisions of the Principles apply where they are relevant.</p> <p>Compare also <b>Annex II</b> EU-US Privacy Shield Framework Principles issued by the Department of Commerce I. Overview 7.</p>

**COMPARISON:**

While the GDPR must be interpreted in line with higher ranking law (e.g. the CFR and the ECHR), the Privacy Shield is subject to a US interpretation, US laws and the US constitution, which are not granting protection for “non-US persons”<sup>3</sup> and base on concepts such as the “reasonable expectation of privacy”<sup>4</sup> and the so called “third party doctrine”<sup>5</sup>, which differ fundamentally from the EU understanding of privacy protection.

<sup>3</sup> Bowden, The US surveillance programmes and their impact on EU citizens’ fundamental rights, p. 19, study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs in September 2013, p. 20, para 2.2.3, available at: [http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE\\_NT%282013%29474405\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT%282013%29474405_EN.pdf) and Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a).

<sup>4</sup> Compare for instance: Reidenberg, Joel R., Privacy in Public (September 8, 2014), 69 University of Miami Law Review 141 (2014); Fordham Law Legal Studies Research Paper No. 2493449, available at SSRN: <https://ssrn.com/abstract=2493449>; Edwards, Lilian and Urquhart, Lachlan, Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence? (December 11, 2015), International Journal of Law and Information Technology (Autumn 2016) 24 (3), 279-310, available at SSRN: <https://ssrn.com/abstract=2702426>; Tokson, Matthew, Knowledge and Fourth Amendment Privacy (March 14, 2016), Northwestern University Law Review, Vol. 111, p. 139, 2017, available at SSRN: <https://ssrn.com/abstract=2746534>.



### 3. Exceptions

The GDPR allows for a number of limitations in the application of data protection principles (Art. 23 GDPR). Such limitations are usually to be interpreted narrowly and are limited by national constitutional laws, the European Convention of Human Rights and the Charta of Fundamental Rights.<sup>6</sup> EU law requires that restrictions are provided for by a law that fulfills certain minimum requirements, such as accessibility, foreseeability and clear and precise rules with regard to the circumstances justifying a limitation.<sup>7</sup> Article 52 (1) of the CFR further requires that limitations and restrictions to the fundamental rights of the CFR respect the essence of the rights and are subject to the principle of proportionality. Further, “limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.”<sup>8</sup>

The Privacy Shield incorporates all these limitations by referring to Directive 95/46 in Subparagraph (c) of the fifth Paragraph of the Privacy Shield. In addition to the limitations in Directive 95/46, the Privacy Shield adds further exceptions in its subparagraphs (a) and (b) of principle five (I. Overview, principle 5). The limitations included in this principle make clear that any law, government regulation, and case law override the self-certification. In addition, all national security, public interest and law enforcement requirements make the Privacy Shield non-applicable, even if they are not specified in a law, government regulation or case law.

This means in practice that any form of US statute/executive regulation can add further limitations to the ones provided for in Directive 95/46/the GDPR. In consequence, the Privacy Shield principles only apply when there is no other specific regulation within the US legal system.

GDPR

Privacy Shield

<b>Article 23: Restrictions</b>	<b>Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce I. Overview (5)</b>
-------------------------------------	--

<sup>5</sup> Compare for instance: Richards, Neil M., The Third-Party Doctrine and the Future of the Cloud (May 1, 2017), Washington University Law Review, Vol. 94, No. 1441, 2017, Washington University in St. Louis Legal Studies Research Paper, Available at SSRN: <https://ssrn.com/abstract=3123199>; Stern, Simon, The Third-Party Doctrine and the Third Person (May 22, 2013), New Criminal Law Review, Vol. 16, 2013, 364-412, available at SSRN: <https://ssrn.com/abstract=2268288>; Friedman, Perry, Revisiting the Third-Party Doctrine (October 30, 2016), Criminal Law Bulletin, Vol. 53 No. 2, available at SSRN: <https://ssrn.com/abstract=2871831>.

<sup>6</sup> Compare: ECtHR, Rotaru v. Romania, no. 28341/95, para. 47; CJEU, C-293/12 Digital Rights Ireland and 594/12 Seitlinger and Others paras 38 et seq.

<sup>7</sup> CJEU, OPINION 1/15 OF THE COURT (Grand Chamber) on the EU-Canada PNR exchange of 26 July 2017, para 141; ECtHR, S. and Marper v. UK, no. 30562/04 and 30566/04, para. 95; Copland v. UK, no. 62617/00, para. 46; Amann v. Switzerland, no. 27798/95, para. 55.

<sup>8</sup> CJEU, C-293/12 Digital Rights Ireland and 594/12 Seitlinger and Others, para. 38; Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 34.

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article (...) when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- a) national security;
- b) defence;
- c) public security;
- d) the prevention, investigation, detection or prosecution of criminal offences (...);
- e) other important objectives of general public interest of the Union or of a Member State(...);
- f) the protection of judicial independence and judicial proceedings;
- g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
  1. the protection of the data subject or the rights and freedoms of others;
  2. the enforcement of civil law claims.
- i) In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:
  1. the purposes of the processing or categories of processing;
  2. the categories of personal data;
  3. the scope of the restrictions introduced;
  4. the safeguards to prevent abuse or unlawful access or transfer;
  5. the specification of the controller or categories of controllers;
  6. the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
  7. the risks to the rights and freedoms of data subjects; and
  8. the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Adherence to these Principles may be limited:

- (a) to the extent necessary to meet national security, public interest, or law enforcement requirements;
- (b) by statute, government regulation, or case law that create conflicting obligations or 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 Directive of Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts.

Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. 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.

## COMPARISON

The US constitution as well as most US laws and regulations do not grant a right to privacy to “non-US persons”. In contrast, it is clear from the wording of Annex II EU-US Privacy Shield Framework Principles (I. Overview, principle (5)) that every “statute, government regulation, or case law that create conflicting obligations or explicit authorizations” in the US can override the guarantees of the Privacy Shield. Further, it not particularly specified what has to be understood by “explicit authorizations”. And, although it is governmental law, which creates such obligations, the certifying organization has “to demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization”. The burden to interpret such laws is therefore on the organization. There is no provision requiring the restricting laws to take the balancing of interest or proportionality aspects into account. As there is no comparable proportionality requirement in US law, this provision can have a wide-ranging effect on the enforcement of fundamental rights (Article 7, 8 and 52 (1) CFR).

As a result, in particular the provisions of Annex II EU-US Privacy Shield Framework Principles (I. Overview, principle (5)) are capable of broadly restricting the rights of the persons whose data have been transferred. Further, there are the limitations regarding national security, signal intelligence and the Presidential Policy Directive 28. Those limitations are however addressed already in the written observations and are not repeated here.

## 4. SUMMARY: APPLICATION AND SCOPE

With regard to the scope of protection, it can be concluded that the scope of the Privacy Shield is relatively narrow and includes only the about 3.400 organizations that have self-certified. If Privacy Shield data is transferred to organizations which are not subject to the Privacy Shield rules, constitutional protection or protection following from other legal sources for data of EU citizens is almost non-existent. The Privacy Shield does not foresee any limitations on onward transfer other than “notice and choice”, which effectively means that data subjects must have an option to “opt out” of an onward transfer (see further below). In addition, the Privacy Shield is governed and interpreted under US law and Privacy and data protection rules in the US differ significantly from the protection guaranteed in the EU. There are no general privacy or data protection laws in the US and constitutional protection of privacy for “non-US persons” is not provided for. Sectoral regulations govern certain aspects of privacy and data protection in a particular context (for instance Health Data, Online Data of Children, Credit Information).

In addition to the week protection outside of the Privacy Shield framework, the Privacy Shield rules do not apply, if a “statute, government regulation, or case law that create conflicting obligations or explicit authorizations” in the US exist. All instruments can then override the guarantees of the Privacy Shield. Other explicit “authorizations” may even limit the scope further. In consequence, in particular the provisions of Annex II EU-US Privacy Shield Framework Principles (I. Overview, principle (5)) are capable of broadly restricting the rights of the persons whose data have been transferred

## II. MATERIAL PROTECTION

### 1. Data Quality

Data quality requirements constitute a central limitation for every kind of data usage in EU law.<sup>9</sup> Art. 5 GDPR requires therefore certain basic data protection principles, such as lawfulness; fairness; transparency; limitation to a specific, explicit and legitimate purpose; data minimization; accuracy and storage limitation. . Each of the principles is not only important as a single principle; they also have a considerable meaning in their entirety. This idea as well as the specific principles that limit data processing can be found in primary EU law. Article 8 (2) CFR mentions most of the rules laid down in Article 5 GDPR. Article 8 ECHR and the case law of the ECtHR equally and regularly refer to the above-mentioned quality requirements.<sup>10</sup> The same principles can be found in the “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”<sup>11</sup> and the “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”<sup>12</sup> of the Council of Europe. The mentioning of these principles in several sources of law and the reference in case law show their high acceptance even beyond mere EU law.

Data quality principles, respectively “data integrity and purpose limitation” principles, are laid down in the Privacy Shield as well. However, they are important legal differences, which leave important doubts on the adequacy of the guarantees of the Privacy Shield.

#### GDPR

<b>Article 5</b>	
<b>Principles relating to processing of personal data</b>	
1.	Personal data shall be:
(a)	processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
(b)	collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (...);
(c)	adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
(d)	accurate and, where necessary, kept up to date (...) ('accuracy');
(e)	kept in a form which permits identification of data subjects for no

#### Privacy Shield

<b>Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce II. Principles (5) Data integrity and purpose limitation</b>	
a.	Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. 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

<sup>9</sup> Compare Handbook on European data protection law, chapter 3 ([http://www.echr.coe.int/Documents/Handbook\\_data\\_protection\\_ENG.pdf](http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf)); Brühann, in: Grabitz/Hilf, Art. 6 para 6.

<sup>10</sup> Compare ECtHR, S. and Marper v. UK, no. 30562/04 and 30566/04, para. 103; Gardel v. France, no. 16428/05, para. 62.

<sup>11</sup> Available at: <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm#part2>.

<sup>12</sup> Available at: <http://conventions.coe.int/Treaty/en/Treaties/html/108.htm>.

longer than is necessary for the purposes for which the personal data are processed (...) ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data (...) ('integrity and confidentiality'). 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	information. b. Information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of 5a. 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 Framework. Organizations should take reasonable and appropriate measures in complying with this provision.
---	---

### COMPARISON

Although at first view, the data quality principles of the GDPR and the Privacy Shield principles seems to read similarly, there are important differences when looking at them in detail:

First, the “data integrity and purpose limitation” principle makes reference to storage limitation of personal data that is “relevant” for the processing. This wording however, is very broad and lacks proportionality and reasonableness standards, which have not been incorporated in Privacy Shield. Specifically, the Privacy Shield requires information to be “retained in a form identifying or making identifiable the individual only for as long as” it is “relevant for the purposes of processing” (compare 5 b). “Relevance”, however, does not guarantee that the processing is limited only to the data necessary for the processing at stake.<sup>13</sup>

Second, according to the Privacy Shield, “[t]o 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” (5 a). The wording adopted in Privacy Shield is identical to the one contained in predecessor agreement, the Safe Harbour. Such wording makes the accuracy of data dependent on the purpose of processing, which is not compliant with EU law. During the negotiations to the Privacy Shield, the Art. 29 Working Party therefore proposed to remove this wording from the text.<sup>14</sup> Still, this proposal did not make it in the final decision.

Third, the scope of the purpose limitation principle contained in “data integrity and purpose limitation” principle is different compared to the Notice and the Choice principles contained also in Privacy Shield. It even contradicts the latter principle.

---

<sup>13</sup> Compare to this point: Opinion 01/2016 of the Art. 29 Working Party, WP 328 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, p. 23 et seq., point 2.2.4 (a).

<sup>14</sup> Opinion 01/2016 of the Art. 29 Working Party, WP 328 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, p. 24, point 2.2.4 (b).

According to the data integrity and purpose limitation principle, organisations “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”. However, the opt-in mechanism under the Choice principle allows for the use of data for purposes, which are “materially different from the purposes for which the data have originally been collected”. This inconsistency stems from the fact that both the terms “incompatible purpose” and “materially different purpose” are used in the same text, with both concepts lacking a clear definition.<sup>15</sup> The Art. 29 Working Party “has serious concerns about the fact that such inconsistency might lead to great difficulties to reconcile the data integrity and Purpose Limitation principle (Annex II, II.5) with the Choice principle (Annex II, II.2), since the “data integrity and purpose limitation” principle states that the data cannot be processed in a way that is incompatible with the purposes for which they were collected, while the other provides for an opt-out mechanism in case the data are processed for a purpose that is materially different from the original purpose”.<sup>16</sup>

More general remarks relate to the fact that crucial elements like “fairness” and “lawfulness” are missing in data quality description of the Privacy Shield. Equally, the “adequacy” element is not mentioned in the data quality principles. In consequence, there is no starting-point for conducting the proportionality test, which is crucial in European data protection legislation.<sup>17</sup> The Privacy Shield also does not require the purpose to be “explicit”, “specified” or “legitimate”. As the further elements (accuracy; completeness; currentness) refer to the defined purpose, the formulation of a broad purpose paves the way for various forms of processing. With regard to such broad definition of the purpose it is not unlikely that the data are regarded as relevant, necessary, compatible and current for various different purposes.

In summary, it can be observed that the “data integrity and purpose limitation” principle fundamentally from the requirements of Art. 5 GDPR and in this way from European data protection standards. Important minimum standards (fairness, lawfulness, adequacy, explicit purpose limitation) resulting from the GDPR, Article 7, 8 CFR and Article 8 ECHR are not applied at all or applied in a much less stringent way.

## 2. Legitimate Processing

EU law prohibits data processing, unless there is an explicit allowance. The GDPR is following the doctrine established under the ECHR and enshrined in Article 8 CFR as well, regarding the authorization of processing operations. The most relevant condition that makes data processing legitimate is the consent of the data subject. Additionally, Art. 6 (1) GDPR contains five more reasons that can be applied for arguing that the processing

---

<sup>15</sup> Compare Opinion 01/2016 of the Art. 29 Working Party, WP 328 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, p. 24 et seq., point 2.2.4 (c).

<sup>16</sup> Opinion 01/2016 of the Art. 29 Working Party, WP 328 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, p. 24 et seq., point 2.2.4 (c).

<sup>17</sup> Compare Article 29 Data Protection Working Party, 536/14/EN, available at: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf).

operation is in conformity with data protection law. It is noteworthy that every option contains the word “necessary”. This leaves open the possibility to interpret the exceptions narrowly, which is in line with the general approach in EU law to which exceptions should not be interpreted too extensively.

The Privacy Shield does not know any such general limitation. Instead the Choice Principle contained in Privacy Shield provides only for an option to “opt out” (equivalent to the “right to object” in Article 21 of the GDPR) from data processing for two specific processing operations: (a) disclosure to a third party and (b) materially different purposes. All other processing operations fall under no restriction.

GDPR

**Article 6**  
**Lawfulness of processing**

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
  - (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
  - (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
  - (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
  - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
  - (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Privacy Shield

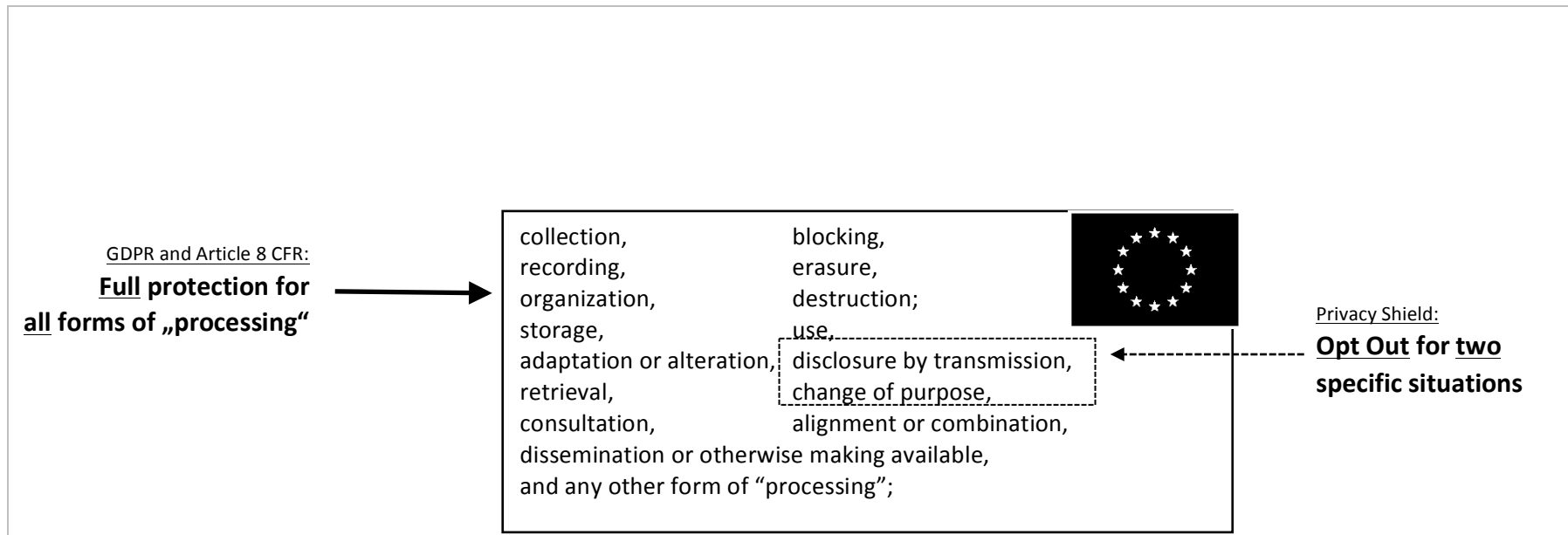
**Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce II. Principles (2) Choice**

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

### COMPARISON

The Privacy Shield follows a general processing approach, which differs in essential points from EU data protection rules. In the EU processing of personal data is prohibited unless one of the explicitly listed exemptions applies.<sup>18</sup> Under the Privacy Shield, it is exactly the opposite. When applying the (notice and) choice principle, the general prohibition to process personal data is replaced by a general permission.

The structure of the choice principle brings up further questions regarding the effectiveness of data protection in the US. It requires US organizations to offer data subjects the opportunity to “opt out” of specific processing operations. It is applicable in only two situations, which are “usage for a materially different purpose” or “disclosure to a third party”. All other processing operations (e.g. collection, storage, processing) are not even subject to the “choices” of the data subject. In consequence, every other processing operation can be conducted by the organization. Thus, the data subject has quite often no influence on the use of its personal data. Consent is replaced by the possibility to “opt out”. The protection offered by the Choice Principle is therefore far away from being “essentially equivalent” to the protection offered by Art. 6 GDPR.



<sup>18</sup> Compare Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, p. 49.



### 3. Onward Transfer

Under the GDPR, the transfer of data to another entity falls under the general limitations of any “processing operation”. Transfers outside of the area that is governed by the GDPR (countries that are not members of the EU/EEA) fall under additional limitations under Articles 44 and 49 of the GDPR.

Compared to the former Safe Harbor rules, the provisions on onward transfer have been extended. Still, there are some differences between the EU and the Privacy Shield system, which should be mentioned here.

GDPR

**Article 3  
Territorial scope**

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
- (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

**CHAPTER IV**

**Controller and processor**

**Article 27**

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.
2. The obligation laid down in paragraph 1 of this Article shall not apply to:
  - (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
  - (b) a public authority or body.
3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to

Privacy Shield

**Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce II. Principles (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)

the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

#### Article 28

##### Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate

provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

statutory obligation of confidentiality;

- (c) takes all measures required pursuant to Article 32;
- (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
- (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
- (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
- (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and

the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

#### **Article 29**

##### **Processing under the authority of the controller or processor**

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

### **COMPARISON**

While the GDPR ensures that data is not leaving a sphere of “adequate protection”, the Privacy Shield obliges the controllers to enter into a contract with the third party controller obliging him to apply the “same level of protection as the Principles” of the Privacy Shield. This is clearly an advantage when compared to the former Safe Harbor rules. However, also with regard to this principle, the far-reaching exceptions (point I. 3.), mentioned above, apply. It is thus easily possible that US laws may allow or even require to forward data to entities that do not provide the same guarantees.

The Privacy Shield further foresees an exemption to the need of contract by allowing data transfers between controllers within a controller group of corporations or entities to “base such transfers on other instruments, such as EU Binding Corporate Rules or other intra-group instruments”.<sup>19</sup> The

---

<sup>19</sup> Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce III. Supplemental Principles (10) (b), obligatory contracts for onward transfer, transfers within a controlled group of cooperations or entities.

reference “other intra-group instruments” signifies amongst others “compliance and control programs”<sup>20</sup>, but can imply more than that. For instance, it is not clear whether such programs are legally binding commitments, which are favoured by EU law.

Moreover, according to Privacy Shield, personal data may be transferred to third party processors (agents) “only for limited and specified purposes” (II. Principles (3 (b) (i)) Accountability For Onward Transfer) without stipulating that these purposes have to be compatible with the initial purposes for which the data was collected and the instructions of the controller.<sup>21</sup> The purpose limitation requirement is therefore not involved in this context.

#### 4. SUMMARY: MATERIAL PROTECTION

The comparison of the provisions regulating the legitimacy of processing and the data quality principles led to the conclusion that the requirements are implemented in a very different and not comparable way. There is a considerable lack of essential protection elements, which are included in the protection offered by Art. 5 and 6 GDPR at EU level and constitute the fundamentals of EU data protection law.

With regard to the legitimacy of processing, the Privacy Shield follows a general processing approach, which differs in essential points from EU data protection law. In the EU, processing of personal data is prohibited unless one of the explicitly listed exemptions applies. Under the Privacy Shield, it is exactly the opposite. When applying the (notice and) choice principle, the general prohibition to process personal data is replaced by a general permission. Choice is further applied only in two situations, which are “usage for a materially different purpose” or “disclosure to a third party”. The protection offered by the Choice Principle is therefore far away from being “essentially equivalent” to the protection offered by Art. 6 GDPR.

Similar fundamental differences can be found with regard to the data quality principles, which are enshrined in Art. 5 GDPR. The “data integrity and purpose limitation principle” of the Privacy Shield does not guarantee that the processing is limited only to the data necessary for the processing at stake.<sup>22</sup> It makes the purpose of retention depended on the relevancy of processing, which does not correspond to the EU understanding of purpose limitation. The same applies to the accuracy of data, which should depend on the purpose of processing, which is not comparable to EU law.

Further there are inconsistencies in the text of the Privacy Shield with regard to the application of the scope of the purpose limitation principle in comparison to the Notice and Choice principle. The Art. 29 Working Party referred rightly to the fact that the “data integrity and purpose

---

<sup>20</sup> 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 (notified under document C(2016) 4176), footnote (29).

<sup>21</sup> Compare to this point, with more arguments: Opinion 01/2016 of the Art. 29 Working Party, WP 328 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, p. 16, point 2.1.2.

<sup>22</sup> Compare to this point: Opinion 01/2016 of the Art. 29 Working Party, WP 328 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, p. 23 et seq., point 2.2.4 (a).

limitation” principle states that the data cannot be processed in a way that is incompatible with the purposes for which they were collected, while the other (Notice and Choice) provides for an opt-out mechanism in case the data are processed for a purpose that is materially different from the original purpose”.<sup>23</sup>

Finally, crucial elements like “fairness” and “lawfulness” are missing in data quality description of the Privacy Shield. Equally, the “adequacy” element is not mentioned in the data quality principles. The Privacy Shield also does not require the purpose to be “explicit”, “specified” or “legitimate”. It can therefore be observed that the “data integrity and purpose limitation” principle fundamentally from the requirements of Art. 5 GDPR and in this way from European data protection standards. Important minimum standards (fairness, lawfulness, adequacy, explicit purpose limitation) resulting from the GDPR, Article 7, 8 CFR and Article 8 ECHR are not applied at all or applied in a much less stringent way.

Considering these observations, one can conclude that the material protection granted by the Privacy Shield is far from being essentially equivalent to the level of protection in the EU.

### III. RIGHT OF ACCESS

The right of access is granted to individuals by virtue of Article 8(2) of the Charter. Art. 15 GDPR now explicitly provides for the categories of information a data subject should receive by the controller when exercising their right of access.

Under Privacy Shield, individuals have the right to obtain confirmation of whether an organization has processed their data and to have communicated to them the data being processed. Furthermore, under Privacy Shield, the right of access is restricted by a number of exceptions listed in Annex II, III. Supplemental Principles no. 8 (e).

#### GDPR

##### Article 15

##### Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
  - (a) the purposes of the processing;

#### Privacy Shield

Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce, III. Supplemental Principles, 8. Access

##### a. The Access Principle in Practice

- i. Under the Privacy Shield 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

<sup>23</sup> Opinion 01/2016 of the Art. 29 Working Party, WP 328 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, p. 24 et seq., point 2.2.4 (c).

<p>(b) the categories of personal data concerned;</p> <p>(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;</p> <p>(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;</p> <p>(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;</p> <p>(f) the right to lodge a complaint with a supervisory authority;</p> <p>(g) where the personal data are not collected from the data subject, any available information as to their source;</p> <p>(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.</p> <p>Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject</p> <p>1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.</p> <p>2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.</p> <p>3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data</p>	<p>have the right to:</p> <ol style="list-style-type: none"> <li>1. obtain from an organization confirmation of whether or not the organization is processing personal data relating to them;</li> <li>2. have communicated to them such data so that they could verify its accuracy and the lawfulness of the processing; and</li> <li>3. have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.</li> </ol> <p>d. Organization of Data Bases</p> <p>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.</p> <p>e. When Access May be Restricted</p> <p>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 Directive, 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:</p> <ol style="list-style-type: none"> <li>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;</li> <li>2. disclosure where the legitimate rights or important interests of others would be violated;</li> <li>3. breaching a legal or other professional privilege or obligation;</li> <li>4. prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or</li> <li>5. prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.</li> </ol> <p>ii. An organization which claims an exception has the burden of demonstrating its necessity, and the reasons for restricting access and a point</p>
--	--

subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

#### Article 23, Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and

for further inquiries should be given to individuals.contact



proportionate measure in a democratic society to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
- (f) the protection of judicial independence and judicial proceedings;
- (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- (i) the protection of the data subject or the rights and freedoms of others;
- (j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

- (a) the purposes of the processing or categories of processing;
- (b) the categories of personal data;
- (c) the scope of the restrictions introduced;
- (d) the safeguards to prevent abuse or unlawful access or transfer;
- (e) the specification of the controller or categories of controllers;
- (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- (g) the risks to the rights and freedoms of data subjects; and
- (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

**COMPARISON**

The right of access in the Privacy Shield is formulated similar to Article 15 of the GDPR, but is limited to organisations that *store* individuals' data, instead of applying it to any kind of personal data processing carried out by organizations. This might be a small change of wording when compared to the GDPR guarantees, but can have serious consequences, when the companies proceed on the assumption that they do not “store”, but “only” process data, for instance in real time without “storing” the information for longer periods. In addition, Annex II, III. Supplemental Principles of the Privacy Shield no. 8 (c) and (e) provide for a wide variety of exceptions and limitations to the right of access. This is not unusual and also the GDPR provides for exceptions to the right of access. However, the GDPR restrictions are only lawful, when they “respect the essence of the fundamental rights and freedoms” and are “a necessary and proportionate measure in a democratic society” (Art. 23 para 1 GDPR). The Privacy Shield does not include any balancing of rights and interest, but leave the decision to restrict access entirely to the company concerned. The latter is not obliged to act also in the interest of the data subject, it can decide based solely on own interests. In practice, this could mean that in situations that are covered by the exemptions enumerated in Annex II, III. Supplemental Principles no. 8 (e) of the Privacy Shield, the individual does never receive the information requested, as the interests of the company will always prevail.<sup>24</sup>

## IV. ENFORCEMENT

### 1. Remedies

The **effective** enforcement of the fundamental right to data protection is one of the essential guarantees in EU law. It in relates to the possibility to claim a remedy before independent courts in cases of violations of the respective rights. This right is entailed in the ECHR, in the CFR and concretized in Articles 77 et seq. GDPR which guarantee a right for judicial remedies before a court for violations of the right to data protection, including a right to injunctive relief and damages before a court (in particular Art. 79 GDPR). Details are left to the civil law system of each member state. As the CJEU in the Schrems case stated: “the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law”.<sup>25</sup>

The Privacy Shield addresses remedy and redress, but the system includes many different layers and is in itself very complex.<sup>26</sup> The Art. 29 Working Party criticises “the lack of clarity of the overall architecture of the mechanism”<sup>27</sup> as well as a lack of information “in an accessible and easily

---

<sup>24</sup> Compare also Opinion 01/2016 of the Art. 29 Working Party, WP 328 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, p. 26, point 2.2.5.

<sup>25</sup> C-362/14 – Schrems, Judgment of the Court (Grand Chamber) of 6 October 2015 ECLI:EU:C:2015:650, para 95.

<sup>26</sup> Compare also Opinion 01/2016 of the Art. 29 Working Party, WP 328 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, p. 26 et seq. point 2.2.6.

understandable form to the individuals regarding their rights and available recourses and remedies”.<sup>28</sup> The Privacy Shield does not expressly establish a new cause of action for damages or an injunctive relief. The redress mechanism focuses on private dispute resolution bodies and rather not on injunctive relief and/or an independent cause of action before a court. There is the possibility for an individual to contact the company concerned, which must then designate an independent dispute resolution body in the US.<sup>29</sup> There are several “pre-arbitrations requirements” for the individual to fulfil before initiating the arbitration claim, which are, however, of no cost to the individual.<sup>30</sup>

Alternatively, the individual can involve the Federal Trade Commission (FTC). The FTC, however, has no obligation to deal with the claim. Further its competency is limited to examine “unfair or deceptive acts or practices in commerce” (compare FTC letter point I. A, Section 5 FTC Act), which leaves all claims against governmental actions aside. As this point is already addressed in the written observations, it will not be further elaborated here. But also within the commercial context, the FTC will rather focus on four “key areas” mentioned in the annexed letter to the Privacy Shield, which do not include the investigation of individual claims.<sup>31</sup> EU DPAs could also refer a case to the FTC, but in general, there is no guarantee that the FTC will deal with such individual claims.

In terms of individual remedies, the Privacy Shield does refer to “compensation for losses” only as one possible way of sanctioning/remedies.<sup>32</sup> It is not obligatory and preferred ways are “publicity for findings of non-compliance and the requirement to delete data in certain circumstances”.<sup>33</sup> Further “sanctions” include the “suspension and the removal of a seal”,<sup>34</sup> but no individual damages.

GDPR

**Chapter 8: Remedies, liability and penalties**

**Article 77: Right to lodge a complaint with a supervisory authority**

**Article 78: Right to an effective judicial remedy against a supervisory authority**

**Article 79: Right to an effective judicial remedy against a controller or a**

Privacy Shield

**Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce, II. Principles, 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:

<sup>27</sup> Ibid.

<sup>28</sup> Art. 29 Working Party, First annual joint review of the functioning of the EU-U.S. Privacy Shield of 28 November 2017, WP 255, I. B. 1.

<sup>29</sup> Annex I EU-US Privacy Shield, Arbitral model and Annex II, III. Supplemental Principles, 11 d.

<sup>30</sup> Annex I EU-US Privacy Shield Framework Principles issued by the Department of Commerce, Arbitral model, I. C.

<sup>31</sup> Annex I EU-US Privacy Shield Framework Principles issued by the Department of Commerce, Arbitral model, last paragraph of the introduction.

<sup>32</sup> Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce, II. Principles, 11, Dispute resolution and enforcement, (e) Remedies and Sanctions.

<sup>33</sup> Ibid.

<sup>34</sup> Ibid.

processor

**Article 82: Right to compensation and liability**

- 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 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.

**Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce, II. Principles, 11. Dispute resolution and enforcement e. Remedies and Sanctions.**

The result of any remedies provided by the 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 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.** 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 dispute resolution bodies and self-regulatory bodies must notify failures of Privacy Shield organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department.

**See also Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce, III. Supplemental Principles, 11. Dispute Resolution and Enforcement**

**See also Annex I** EU-US Privacy Shield Framework Principles issued by the Department of Commerce, **Arbitral model**  
**See also Annex IV** EU-US Privacy Shield Framework Principles issued by the Department of Commerce, **Letter from the Federal Trade Commission.**

## COMPARISON

In view of the very complex remedy and redress procedure, the question can be asked how “effective” the enforcement of the fundamental right to data protection in the Privacy Shield truly is. While the GDPR establishes a clear legal basis for injunctive relief and damages and specifies an important number of available avenues to seek redress, the Privacy Shield mechanism is very complex and not necessarily effective from a EU law point of view. Easy understandable and accessible guidance on how individuals can effectively enforce their rights is clearly missing. The enforcement in “normal” US civil law courts is further subject to factual limitations (e.g. travel, costs and language barriers), which makes such civil law claims practically unfeasible.

## 2. Sanctions

The GDPR empowers European data protection authorities to impose significant administrative fines on both data controllers and data processors (Art. 83 et seq.). Fines may be imposed instead of, or in addition to, measures that may be ordered by supervisory authorities. They may be imposed for a wide range of contraventions, including purely procedural infringements. Administrative fines are discretionary; they must be imposed on a case by case basis and must be “effective, proportionate and dissuasive” (Art. 81 para 1 GDPR). The highest administrative fines available under the GDPR amount to up to €20,000,000 or, in the case of undertakings, 4% of global turnover, whichever is higher.

The Privacy Shield includes sanctions in the framework of the dispute resolution bodies and possibly through the FTC. Possible “sanctions” by the dispute resolution bodies include the “publicity for findings of non-compliance and the requirement to delete data in certain circumstances”.<sup>35</sup> Further “sanctions” include the “suspension and the removal of a seal”.<sup>36</sup> In addition such bodies miss investigative powers and language barriers may hinder individuals to bring their case in front of such bodies.

Additional, Privacy Shield violations can also be indirectly sanctioned by the FTC through its authority under Section 5 of the FTC act, but the FTC is not obliged to act in cases of individual claims.

<sup>35</sup> Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce, II. Principles, 11, Dispute resolution and enforcement, (e) Remedies and Sanctions.

<sup>36</sup> Ibid.

<p style="text-align: center;"><b>Article 83</b></p> <p style="text-align: center;"><b>General conditions for imposing administrative fines</b></p> <p>1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation (...) shall in each individual case be effective, proportionate and dissuasive. (...)</p> <p>5. Infringements of the following provisions shall (...) be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; the data subjects' rights pursuant to Articles 12 to 22; the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; any obligations pursuant to Member State law adopted under Chapter IX; non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.</p>	<p style="text-align: center;"><b>Annex II EU-US Privacy Shield Framework Principles issued by the Department of Commerce, II. Principles, 11. Dispute resolution and enforcement</b></p> <p><b>e. Remedies and Sanctions.</b> The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, <b>insofar as feasible</b>, 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 cease. <b>Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles.</b> 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 <b>publicity for findings of non-compliance and the requirement to delete data in certain circumstances.</b> Other sanctions could include <b>suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive awards.</b> Private sector dispute resolution bodies and self-regulatory bodies must notify failures of Privacy Shield organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department.</p>
--	---

**COMPARISON:**

Both systems provide for sanctions. While the GDPR includes a robust and obligatory framework of sanctions (they must be effective, proportionate and dissuasive), the Privacy Shield offers rather vague possibilities of sanctioning in the framework of the dispute resolution bodies. The sanctions in this framework are hardly dissuasive (publicity for findings of non-compliance, to deletion of data in certain circumstances, suspension and removal of a seal<sup>37</sup>) and may not be that effective.

However, if the FTC is involved, more severe actions can be initiated, but this option is not obligatory and cannot be initiated by individuals.

---

<sup>37</sup> Ibid.

### 3. Supervisory Authority / Enforcement

CHAPTER VI of the GDPR (Art. 51 et seq.) together with the general principles of EU law, national laws and Article 8 III CFR provides for the establishment of independent supervisory authorities in each member state of the EU. Such authorities must be equipped with enforcement and investigations powers and must process complaints filed by data subjects. The supervisory authorities are described by the Court of Justice as “the guardians of [...] fundamental rights and freedoms, and their existence in the Member States is considered, as is stated in the 62nd recital in the preamble to Directive 95/46, as an essential component of the protection of individuals with regard to the processing of personal data.”<sup>38</sup> They must be completely independent meaning that they must be free from any external influence. The mere risk that such influence could be exercised over the decisions of the supervisory authorities is “enough to hinder the latter authorities’ independent performance of their tasks”.<sup>39</sup>

The Privacy Shield only foresees the FTC as investigative authority, while “dispute resolution bodies” can only decide over complaints but lack power to investigate the facts. The dispute resolution bodies are chosen and paid by the companies and therefore not independent in the sense of EU data protection law. Data subjects may also direct their requests to the FTC, but the FTC is not obliged to investigate consumer complaints.<sup>40</sup>

GDPR	Privacy Shield
<b>Article 51, Supervisory authority</b>	<p style="text-align: center;"><b>11. Dispute resolution and enforcement</b></p> <p>(...) Sanctions must be sufficiently rigorous to ensure compliance by organizations.</p> <p><b>e. Remedies and Sanctions.</b></p> <p>The result of any remedies provided by the 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 cease. Sanctions need to be rigorous enough</p>
<b>Article 52, Independence</b>	
<b>Article 53, General conditions for the members of the supervisory authority</b>	
<b>Article 54, Rules on the establishment of the supervisory authority</b>	
<b>Article 55, Competence</b>	
<b>Article 57, Tasks</b>	

<sup>38</sup> C-518/07, Commission v. Germany of 9 March 2010, para 23.

<sup>39</sup> C-518/07, Commission v. Germany of 9 March 2010, para 36.

<sup>40</sup> Compare: A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority: <http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority> and <https://www.ftccomplaintassistant.gov/#crnt&panel1-1> that says: “The FTC cannot resolve individual complaints, but we can provide information about what next steps to take”.

**Article 58, Powers**

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. 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 dispute resolution bodies and self-regulatory bodies must notify failures of Privacy Shield organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department.

**COMPARISON**

While the GDPR as well as Article 8(3) CFR require a completely independent supervisory authority equipped with strong investigation and enforcement powers, the Privacy Shield provides for the dispute resolution mechanism which shifts the control of the Privacy Shield principles to private US organizations that are chosen and paid by the respective companies. These organizations do not have investigative powers and cannot be regarded as independent within the meaning of EU law. Moreover, they do not exercise an active control over data processing activities of the Privacy Shield companies; they only react to complaints of consumers. This concept is fundamentally different from the EU understanding of independent control, which is in various cases a proactive control to prevent fundamental rights' violations before they arise.

There is also the possibility to refer a complaint to the FTC, which usually does not investigate consumer complaints.

**4. SUMMARY: ENFORCEMENT**

The Privacy Shield includes a very complex and complicated remedy and redress procedure. The effectiveness of this mechanism can be therefore questioned, in particular compared to the mechanism provided for in the GDPR.

With regard to sanctions, both instruments include this possibility. However while the GDPR includes a robust and obligatory framework of sanctions ("effective, proportionate and dissuasive"), the Privacy Shield offers sanctioning in the framework of the dispute resolution bodies. The



sanctions in this framework are hardly dissuasive (publicity for findings of non-compliance, to deletion of data in certain circumstances, suspension and removal of a seal<sup>41</sup>) and may not be effective. However, FTC sanctions might be more effective, but the FTC is not obliged to act on claims initiated by individuals.

Fundamental differences can also be observed with regard to supervision. The US dispute resolution bodies are not equipped with investigation powers and cannot be regarded as independent within the meaning of EU law. Further they do not exercise an active control over data processing activities of the Privacy Shield companies. The supervision of the FTC is also limited, as it usually does not investigate consumer complaints.

## V. CONCLUSION

The comparison between the guarantees of Privacy Shield and the GDPR shows considerable differences concerning the protected rights of individuals.

The Privacy Shield rules do not apply, if a “statute, government regulation, or case law that create conflicting obligations or explicit authorizations” in the US exist. All of such US instruments can then **override** the guarantees of the Privacy Shield. Other explicit “authorizations” may even limit the scope further. In consequence, in particular the provisions of Annex II EU-US Privacy Shield Framework Principles (I. Overview, principle (5) are capable of broadly restricting the rights of the persons whose data have been transferred. Also the **applicability of US law** when it comes to questions of interpretation of the Privacy Shield lead to a lack of protection for EU citizens, if their data is transferred under the Privacy Shield.

The **most striking differences** however, concern the comparison of the provisions regulating the legitimacy of processing and the data quality principles. There is a **considerable lack of essential protection elements**, which are included in the **protection offered by Art. 5 and 6 GDPR** at EU level and constitute the fundamentals of EU data protection law. The “data integrity and purpose limitation principle” of the Privacy Shield does not guarantee that the processing is limited only to the data necessary for the processing at stake.<sup>42</sup> It makes the purpose of retention depended on the relevancy of processing, which does not correspond to the EU understanding of purpose limitation. The same applies to the accuracy of data, which should depend on the purpose of processing, which is not comparable to EU law.

---

<sup>41</sup> Ibid.

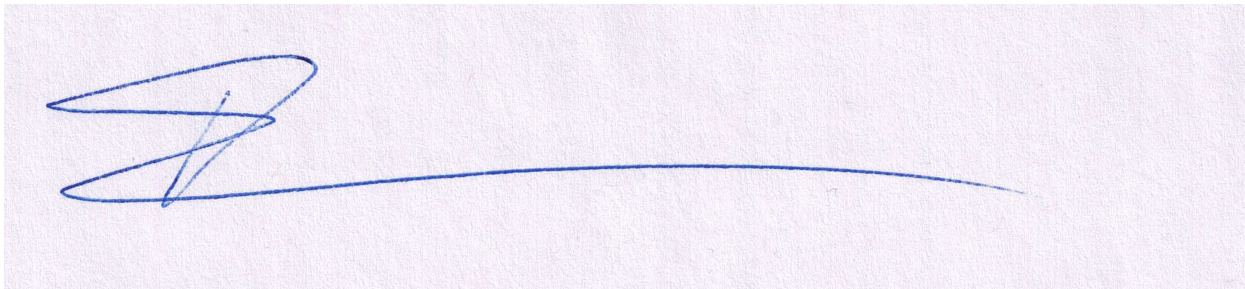
<sup>42</sup> Compare to this point: Opinion 01/2016 of the Art. 29 Working Party, WP 328 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, p. 23 et seq., point 2.2.4 (a).

When applying the (notice and) choice principle, the general prohibition to process personal data is replaced by a general permission. Choice is further applied only in two situations, which are “usage for a materially different purpose” or “disclosure to a third party”. The protection offered by the Choice Principle is therefore far away from being “essentially equivalent” to the protection offered by Art. 6 GDPR.

Additionally, crucial elements like “fairness” and “lawfulness” are missing in data quality description of the Privacy Shield. Equally, the “adequacy” element is not mentioned in the data quality principles. The Privacy Shield also does not require the purpose to be “explicit”, “specified” or “legitimate”. It can therefore be observed that the “data integrity and purpose limitation” principle fundamentally from the requirements of Art. 5 GDPR and in this way from European data protection standards. Important minimum standards (fairness, lawfulness, adequacy, explicit purpose limitation) resulting from the GDPR, Article 7, 8 CFR and Article 8 ECHR are not applied at all or applied in a much less stringent way.

Comparing the enforcement mechanisms of the GDPR and the Privacy Shield rules, doubts arise regarding the effective enforcement of remedies, sanctions and the establishment of independent supervisory bodies within the Privacy Shield framework. It is very doubtful whether the (limited) jurisdiction of the FTC and the dispute resolution mechanism, which faces various complexities and difficulties, can be classified as essentially equivalent.

In summary, there are serious doubts the guarantees of the Privacy Shield are essentially equivalent to the protection in the EU. It could be observed that the Privacy Shield is differing in essential points from minimum European data protection standards that are laid down in the GDPR and higher ranking EU law.

A handwritten signature in blue ink on a light-colored, textured background. The signature is stylized, starting with a large, looped initial 'F' that extends into a long, horizontal stroke across the page.

Signature, Prof. Dr. Franziska Boehm