FACULTY OF LAW AND CRIMINOLOGY

Privacy Shield v GDPR, *Schrems* revisited?

Is Privacy Shield indeed Safe Harbour with flowers on it?[1]

Word count: 54678

Simon Gunst

Student number: 01405586

Supervisor: Prof. dr. Inge Govaere

Co-supervisor: Jolien Timmermans

A dissertation submitted to Ghent University in partial fulfilment of the requirements for the degree of Master of Laws.

Academic year: 2018 – 2019

[1] Schrems, M. (21 October 2016). Personal Interview.

GHENT UNIVERSITY

SAMENVATTING (abstract, in Dutch)

Het EU-VS Privacy Shield ligt vanuit verschillende hoeken onder vuur voor het Hof van Justitie van de Europese Unie. Zowel een annulatieberoep voor het Gerecht als een prejudiciële vraag van het Ierse High Court voor het Hof van Justitie zijn op dit moment (mei 2019) aanhangig. In deze masterproef zal de verenigbaarheid van het Privacy Shield met het EU-recht, in het bijzonder met het Handvest van de Unie en met de AVG, geëvalueerd worden. Eerst zullen de relevante bepalingen van het primair recht van de Unie, voornamelijk het Handvest, besproken worden. Dit zal voornamelijk gebeuren aan de hand van vier mijlpaalarresten van het Hof van Justitie: *Digital Rights Ireland*, *Tele2 Sverige*, *Schrems* en *PNR Canada*. Nadien zullen de relevante bepalingen uit de AVG geschetst worden. Vervolgens zal het vereiste beschermingsniveau in derde landen, voor doorgiften van persoonsgegevens op basis van adequaatheidsbesluiten naar die derde landen, besproken worden. Bij dit laatste zullen zowel conceptuele als praktische problemen met het interpreteren van 'passend' (adequate) als 'in grote lijnen overeenkomend' (essentially equivalent) aan bod komen. Als sluitstuk zal het Privacy Shield zelf op de rooster gelegd worden. Eerst zal uitgelegd worden hoe het Privacy Shield werkt. Nadien worden de Privacy Shield beginselen getoetst aan het vereiste beschermingsniveau in derde landen. Praktisch gezien betekent dit dat er nagegaan wordt of de bescherming geboden door de Privacy Shield beginselen 'essentially equivalent' is met de bescherming geboden door het Handvest en de AVG. Tot slot wordt de beperking van de toepassing van de Privacy Shield beginselen voor nationale veiligheidsdoeleinden getoetst aan het vereiste beschermingsniveau. Praktisch gezien wordt er nagegaan of de bepalingen van het Handvest worden geschonden. De conclusie van de masterproef is dat zowel de Privacy Shield beginselen als de beperking ervan voor nationale veiligheid de toets niet doorstaan. Het ligt dan ook in de lijn der verwachtingen dat het Hof van Justitie van de Europese Unie het besluit in verband met het EU-VS Privacy Shield zal vernietigen.

DANKWOORD

Ten eerste wens ik mijn promotor, professor dr. Inge Govaere, en mijn commissaris, Jolien Timmermans, te bedanken. De centrale onderzoeksvraag die ik in de eerste master initieel zelf in gedachten had voor mijn masterproef was achteraf gezien slechts matig interessant. Dankzij professor Govaere's sturing echter, groeide deze onderzoeksvraag uit tot dit huidige, erg boeiende onderwerp. Deze sturing bleek ook in de tweede master onontbeerlijk. Telkens wanneer er een probleem opdook hielpen zij mij deze problemen op te lossen. Tenslotte wil ik hen ook bedanken voor de oprechte, stimulerende interesse die ze toonden, door niet enkel tijdens de feedbackmomenten, maar ook daarbuiten eens te vragen of ik het nog zag zitten, of het vooruit ging…

Ten tweede wil ik mijn ouders bedanken: mijn papa, die mijn masterproef volledig heeft nagelezen op typo's en soms mijn te ingewikkelde zinsconstructies in stukken hakte tot meer behapbare zinnen en mijn mama, die alle voetnoten nakeek tot in de kleinste details.

Ten derde wil ik de rest van mijn familie en mijn vrienden bedanken. Mijn familie en niet-rechtenvriendjes, die zorgden dat ik ook eens niet aan mijn masterproef hoefde te denken. Mijn rechten vrienden, met wie ik zovele avonden in de bibliotheek heb doorgebracht dat zij tegelijk mijn bibbuddies werden. En last but certainly not least, Hanne en Tine, die ook bij Europees Recht schrijven, en waaraan ik zeker 1.001 vragen heb gesteld (en zij aan mij). Zonder hen was mijn masterproef nooit zo goed (?) geweest.

Simon Gunst
Teralfene, 15 mei 2019.

Contents

ABBREVIATIONS

AG	Advocate General
Board	European Data Protection Board
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Council	Council of the European Union
Commission	European Commission
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
DoC	U.S. Department of Commerce
DoT	U.S. Department of Transportation
DPA	National data protection authority
DPIA	Data protection impact assessment
DPO	Data Protection Officer
DRD	Data Retention Directive
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EO12333	Executive Order 12333

EU	European Union
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court of Review
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
LED	Law Enforcement Directive
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
Ombudsperson	Privacy Shield Ombudsperson
Parliament	European Parliament
PCLOB	Privacy and Civil Liberties Oversight Board
PNR	Passenger Name Record
PNR Agreement	Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data
PPD-28	Presidential Policy Directive 28
Principle 5	Data Integrity and Purpose Limitation principle
PSD	Privacy Shield Decision
PSP's	Privacy Shield Principles

SHD	Safe Harbour Decision
SCC Decisions	Standard Contractual Clauses Decisions
Sigint	Signals Intelligence
Supplemental Principle 2	Journalistic Exceptions Principle
Supplemental Principle 8	Supplemental principle concerning access
Supplemental Principle 14	Pharmaceutical and Medical Products Principle
Supplemental Principle 15	Public Record and Publicly Available Information Principle
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
USA / U.S.	United States of America
WP29	Article 29 Working Party

INTRODUCTION

1. In 1995, the European Parliament and the Council adopted Directive 95/46.[2] This Directive provided the legislative framework for the protection of personal data in the European Union ('EU'). Article 25(1) of this Directive[3] stated that personal data may only be transferred to third countries that ensure adequate protection of this data, thus preventing the creation of a loophole for escaping these data protection rules. It further stated that it is the European Commission ('Commission') that may find that a third country ensures an adequate level of protection of personal data.[4]

2. In 2000, the Commission adopted Decision 2000/520 (the Safe Harbour Decision, hereinafter: 'SHD') in which it determined that the United States of America ('USA' or 'U.S.') ensures an adequate level of protection of personal data.[5] The SHD survived for roughly 15 years until the Court of Justice of the European Union ('CJEU') invalidated the decision in 2015 in *Schrems*[6].

3. The *Schrems* case has a particular history as a strategic litigation case. In 2013, Max Schrems, an Austrian national, started proceedings against Facebook, in essence because Facebook transferred his personal data to the USA.[7] Mr. Schrems alleged that the USA did not ensure an adequate protection of personal data. He referred in this regard to revelations made by Edward Snowden concerning the surveillance activities of the United States intelligence services,[8] like the PRISM surveillance program of the National Security Agency ('NSA'). Mr. Schrems first made a complaint to the Irish Data Protection Commissioner. After the Commissioner decided that

---

[2] 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* L281/31 of 23 November 1995 (hereinafter: 'Directive 95/46').
[3] *Ibid*., article 25(1).
[4] *Ibid*., article 25(6).
[5] Recital 5 of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, *OJ* L215/7 of 25 August 2000 (hereinafter: 'SHD').
[6] Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650 (hereinafter: 'Judgment *Schrems*').
[7] *Ibid*., para 28.
[8] *Ibid*., para 28.

he was not required to investigate the matters raised by Mr. Schrems[9], the latter started judicial proceedings before the Irish Courts[10].

4. In 2014, the High Court of Ireland decided that Mr. Schrems in essence disputed the legality of the SHD[11] and accordingly asked the CJEU in two preliminary questions whether the SHD is valid or not[12]. The CJEU subsequently annulled[13] the decision as stated above.

5. Because of the importance of data flows between the EU and the USA,[14] the Commission started, soon after the abovementioned ruling, drafting a new decision that would replace the old SHD. Less than nine months after the judgment of the CJEU in *Schrems*[15], the Commission adopted Implementing Decision 2016/4176 (the Privacy Shield Decision, hereinafter: 'PSD').[16] This decision again states that the United States ensures an adequate level of protection of personal data[17] but, at the same time, tries to remedy the concerns expressed by the CJEU in *Schrems*[18]. The PSD thus replaced the older SHD.

6. This replacement is however not the only change in the relevant legislative framework. Last year, Directive 95/46 has been replaced in its entirety[19] by Regulation 2016/679, better known as the General Data Protection Regulation ('GDPR')[20]. The GDPR states, essentially in the same way as Directive 95/46 did, that transfers of personal data to third countries may take place where the Commission has decided that the third country in question ensures an adequate level of

[9] *Ibid*., para 29.
[10] *Ibid*., para 30.
[11] *Ibid*., para 35.
[12] *Ibid*., para 36.
[13] *Ibid*., para 106.
[14] Recital 7 of Commission Implementing Decision 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, *OJ* L207/1 of 1 August 2016, (hereinafter: 'PSD).
[15] Judgment *Schrems.*
[16] PSD.
[17] *Ibid*., recital 13.
[18] Judgment *Schrems.*
[19] Article 94(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ* L119/1 of 4 May 2016 (hereinafter: 'GDPR').
[20] GDPR.

protection.[21] The GDPR is however more specific than the older Directive, the Commission must now make a more rigorous assessment of this 'adequate level of protection'. Note that decisions adopted on the basis of Directive 95/46 (such as the PSD) shall remain in force, until amended, replaced or repealed.[22] Those decisions are subject to a monitoring scheme provided for by the GDPR.[23]

7. As stated above, the legal battle between Mr. Schrems and Facebook is to qualify as a form of strategic litigation and it is therefore unsurprising that their 'battle' did not end after the *Schrems* ruling. After the decision of the CJEU in *Schrems*, the High Court of Ireland quashed the decision of the Irish Data Protection Commissioner to refuse to investigate the complaint made by Mr Schrems.[24] The Irish Data Protection Commissioner then invited Mr. Schrems to reformulate his original complaint since this complaint focused upon the SHD and this decision had already been declared invalid.[25] Mr. Schrems then refocused his complaint upon the so-called 'Standard Contractual Clauses Decisions' ('SCC Decisions'). The Irish Data Protection Commissioner formed the view that, in order to investigate the new complaint made by Mr. Schrems, a ruling of the CJEU on the validity of the SCC Decisions was indispensable.[26] Therefore, the Irish Data Protection Commissioner initiated new proceedings before the High Court of Ireland. On the 9th of May 2018, the High Court of Ireland made a reference for a preliminary ruling, including several questions about the PSD. The case is currently pending before the CJEU as case C-311/18.[27] Even though the questions regarding the PSD do not directly challenge its legality, it cannot be ruled out that the CJEU would nonetheless invalidate it. Besides the possible challenge of the PSD coming from Mr. Schrems, the decision is also under attack by the French organisation La Quadrature du Net. This organisation has (together with other French organisations) initiated a direct action against the PSD before the General Court[28], which is also currently pending.

---

[21] *Ibid*., article 45(1).
[22] *Ibid*., article 45(9).
[23] *Ibid*., recital 106 and article 45(4).
[24] High Court (IRL) 3 October 2017, *The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems*, No. 4809 P., para 26 (hereinafter: 'Judgment High Court (IRL)').
[25] *Ibid*., para 27.
[26] *Ibid*., paras 3, 42.
[27] Reference for a preliminary ruling from the High Court (Ireland) of 9 May 2018, *Facebook Ireland and Schrems*, C-311/18.
[28] Action brought on 25 October 2016, *La Quadrature du Net and Others* v *Commission*, T-738/16.

8. Given these challenges to the PSD, the compliance of the PSD with European Union law will be assessed. To phrase it differently, the different possible grounds on which the PSD could be annulled by the CJEU will be analysed. Firstly, the requirements set by the primary law of the EU, mostly the Charter of Fundamental Rights of the European Union ('Charter'),[29] as interpreted by the CJEU, will be zoomed in upon. Next, the requirements of the GDPR will be examined. Since there is no case law of the CJEU about the GDPR yet, guidance and inspiration will be sought in the old Directive 95/46 and the interpretation thereof by the CJEU. The requirements set by the GDPR will be compared to the requirements set by the Charter and Directive 95/46 to see whether the GDPR raises the level of protection of personal data in the EU. This comparison is needed since, in the scenario that the GDPR indeed raises the level of protection, the PSD will not only need to be more protective than the SHD as a result of the case law of the CJEU in *Schrems*, but will also need to raise protection compared to the SHD because of the enhanced protection in the EU itself. In other words, the PSD must try to meet a moving target. After discussing all these 'substantive' requirements, *i.e.* requirements that offer protection by itself, the level of protection of personal data which is required in third countries under EU law to lawfully transfer personal data to those countries will be examined. Lastly, the PSD itself will be assessed. Firstly, it will be explained how the PSD works, what the Privacy Shield Principles are and what their function is. Next, it will be analysed whether these principles meet the required level of protection for the transfer of personal data. Finally, the derogation for national security will be assessed, again to check whether that derogation meets the required level of protection.

[29] Charter of Fundamental Rights of the European Union, *OJ* 326/391 of 26 October 2012 (hereinafter: 'Charter').

CHAPTER I: THE PRIMARY LAW OF THE UNION

Section 1: Relevant provisions in the primary law of the Union

Subsection 1: Relevant articles in the Charter and the TFEU

9. The most important source of primary law in the context of compliance of the PSD with the primary law of the EU, is the Charter. Since one of the overarching objectives of the PSD is to offer protection to personal data, the first, and seemingly most relevant, article of the Charter that comes to mind is article 8 of the Charter.[30]

10. There are two ways of reading article 8. The first way takes the view that the structure of the article, contrary to the other articles in the Charter, includes possible interferences with the right it enshrines.[31] Therefore, only the first paragraph of article 8 would establish a right (the protection of personal data).[32] The second and the third paragraphs would then set the requirements applicable to the limitations of the right.[33] The second way construes article 8 as a 'normal' article, of which all three paragraphs jointly describe the right to the protection of personal data.[34] No matter how the article is read, six constituent elements of the right can be deduced. Data must be processed fairly (1), data must be processed for specified purposes (2), there must be a legitimate basis (consent or a basis laid down by law) for the processing of data (3), there is a right of access to data (4), there is a right to have data rectified (5) and there must be control by an independent authority (6).[35]

---

[30] Article 8 of the Charter is worded as follows:
"Protection of personal data
1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority.*"

[31] G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham, Springer, 2014, 203.
[32] *Ibid.*
[33] *Ibid.*
[34] *Ibid.*, 204.
[35] *Ibid.*, 204.

11. However, article 8 of the Charter is hardly the only relevant provision in the primary law. The right to a private life, the freedom of expression, the principle of non-discrimination, the right to an effective remedy and the possible justification for interferences with those rights (respectively article 7, 11, 21, 47 and 52 of the Charter) are also cited in the case law of the CJEU regarding data protection issues.[36] In addition, article 16 of the Treaty on the Functioning of the European Union ('TFEU')[37] is also sporadically cited by the CJEU.[38] Particularly relevant are article 7 and article 52(1) of the Charter.[39,40,41]

12. Article 52(1) sets out a whole list of distinct conditions to which a limitation of, or, to say it differently, an interference with, a fundamental right provided for in the Charter must adhere to in order to be justified. Interferences must be provided by law (1), respect the essence of the fundamental rights (2), have a legitimate aim *i.e.* correspond with the objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others (3), be necessary for genuinely reaching the legitimate aim (4) and respect to the principle of proportionality (5).[42]

---

[36] See *i.a.* Judgment of 9 November 2010, *Volker und Markus*, C-92/09, ECLI:EU:C:2010:662, paras 47, 50, 51; Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger*, C-293/12, ECLI:EU:C:2014:238, paras 29, 35, 38; Judgment of 17 July 2014, *YS and Others*, C-141/12, ECLI:EU:C:2014:2081, paras 66-69; Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970, paras 50, 93, 107, 108, 112; Opinion of 26 July 2017, *Accord PNR UE-Canada*, Opinion 1/15, ECLI:EU:C:2017:592, paras 125, 138, 165, 167, 219; Judgment of 27 September 2017, *Peter Puškár*, C-73/16, ECLI:EU:C:2017:725, paras 76, 82, 87, 88, 93, 98, 102.

[37] Article 16 Treaty on the Functioning of the European Union, *OJ* C326, 26 October 2012 (hereinafter: 'TFEU'). Article 16 is worded as follows:

"***Article 16***

1. *Everyone has the right to the protection of personal data concerning them.*
2. *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*

[…]"

[38] Opinion of 26 July 2017, *Accord PNR UE-Canada*, Opinion 1/15, ECLI:EU:C:2017:592, paras 120, 229.

[39] Articles 7 and 52 Charter.

[40] Article 7 of the Charter is worded as follows:

"*Article 7 Respect for private and family life*

Everyone has the right to respect for his or her private and family life, home and communications."

[41] Article 52(1) of the Charter is worded as follows:

"***Article 52 Scope and interpretation of rights and principles***

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

[42] T. OJANEN, "Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter", *European Constitutional Law Review* 2016, (318) 324.

13. It is clear from these provisions that some requirements regarding data protection directly stem from primary law and are therefore deeply entrenched in the law of the EU. Some provisions are remarkably precise, e.g. the requirement of the existence of an independent data protection authority is explicitly provided by the primary law of the EU in both article 8(3) of the Charter and article 16(2) *in fine* of the TFEU. However, other provisions are not that precise and need interpretation to become operative.

14. For this purpose, this chapter will look for guidance in the case law of the CJEU regarding these provisions. By analysing the case law of the CJEU, this chapter will distil the requirements stemming from primary law, to which the PSD should adhere. Before delving into the case law regarding these provisions, it is useful to deal with two preliminary questions. Firstly, are the right to a private life and the right to protection of personal data two distinct rights? Secondly, what is the role of the Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR') and the European Court of Human Rights ('ECtHR').

Subsection 2: Is there a distinction between the right to a private life and the right to protection of personal data?

15. It is a contested issue in the doctrine whether the right to a private life and the right to protection of personal data are two distinct rights, or whether the latter is rather a mere subset of the former.[43] Despite the fact that the Charter clearly distinguishes two rights, each being contained in a different article, this clear distinction is not always maintained by the CJEU.[44] In *Volker und Markus*[45], the CJEU declares that "*that fundamental right* (*i.e.* the right to protection of personal data) *is closely connected with the right to respect of private life* […]".[46] The CJEU also frequently deals with the two rights together, as if it is 'one fundamental right in two provisions',

[43] See also M. BRKAN, "The Court of Justice of the EU, Privacy and Data Protection: Judge-made law as a leitmotif in fundamental rights protection" in M. BRKAN and E. PSYCHOGIOPOULOU (eds), *Courts, privacy and data protection in the digital environment*, Cheltenham, Edward Elgar Publishing, 2017, 11-17 (hereinafter: 'M. BRKAN, Judge-made law as a leitmotif'); O. LYNSKEY, "Control over Personal Data in a Digital Age: *Google Spain* v *AEPD and Mario Costeja Gonzalez*", *Mod. Law Rev.* 2015, (522) 529; O. LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press, 2015, 266.
[44] M. BRKAN Judge-made law as a leitmotif, 11.
[45] Judgment of 9 November 2010, *Volker und Markus*, C-92/09, ECLI:EU:C:2010:662 (hereinafter: 'Judgment *Volker und Markus*').
[46] Judgment *Volker und Markus*, para 47.

e.g. in *Digital rights Ireland*[47]. According to one author, the CJEU even conflates the two rights consistently.[48] In some case law,[49] the CJEU did indeed little effort to distinguish the two rights.[50]

16. In other cases however, the CJEU makes a, albeit not crystal clear, distinction between the two rights. It appears that the right to protection of personal data, in the CJEU's view, partially overlaps with the right to a private life[51], but that it is nevertheless to be considered a right on its own.[52] The right to protection of personal data seems to play an additional role[53] as a self-standing right when the case is about an interference with data that is not private.[54] Sometimes, the CJEU even expressly states[55] that the right to protection of personal data is distinct from the right to a private life, echoing an earlier statement by Advocate General ('AG') Mengozzi[56]. One of the reasons of the rise of importance of the right to protection of personal data, and its emancipation vis-à-vis the right to a private life in the case law of the CJEU might be that the right to protection of personal data, unlike the right to a private life, is arguably not a general principle of EU law resulting from constitutional traditions common to the Member States.[57] Consequently, the CJEU has a 'freer hand' in interpreting the right to protection of personal data than the right to a private life.

[47] Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger*, C-293/12, ECLI:EU:C:2014:238, paras 32-71.
[48] O. LYNSKEY, "Control over Personal Data in a Digital Age: *Google Spain* v *AEPD and Mario Costeja Gonzalez*", *Mod. Law Rev.* 2015, (522) 529.
[49] See e.g. Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, para 63; Judgment of 24 November 2011, *ASNEF*, C-468/10 and C-469/10, ECLI:EU:C:2011:777, paras 40-42, 45; Judgment of 7 November 2013, *IPI*, C-473/12, ECLI:EU:C:2013:715, paras 28, 39; Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, para 28; Judgment of 20 December 2017, *Peter Nowak*, C-434/16, ECLI:EU:C:2017:994, para 57.
[50] M. BRKAN, Judge-made law as a leitmotif, 11.
[51] *Ibid.*, 15.
[52] See e.g. I. ANDOULSI, "L'arrêt de la Cour du 9 novembre 2010 dans les affaires jointes Volker und Markus Schecke GBR et Hartmut Eifert contre Land d'Hessen (C-92/09 et C-93/09): une reconnaissance jurisprudentielle du droit fondamental à la protection des données personnelles?", *Cah. dr. eur.* 2011, (471) 492, 495.
[53] O. LYNSKEY, "Control over Personal Data in a Digital Age: *Google Spain* v *AEPD and Mario Costeja Gonzalez*", *Mod. Law Rev.* 2015, (522) 529.
[54] M. BRKAN, Judge-made law as a leitmotif, 15.
[55] Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970, para 129.
[56] Opinion of Advocate General Mengozzi of 8 September 2016, *Accord PNR UE-Canada*, Opinion 1/15, ECLI:EU:C:2016:656, para 170 (hereinafter: 'Opinion of AG Mengozzi *PNR Canada*').
[57] M. BRKAN, Judge-made law as a leitmotif, 11; G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham, Springer, 2014, 206.

Subsection 3: What is the relevance of the ECHR and the case law of the ECtHR?

17. Although the case law of the ECtHR will not be examined, and focus will solely be on the case law of the CJEU, it is nonetheless important to shortly indicate the relevance of it. Article 52(3) of the Charter states that "*in so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention*". As article 8 ECHR[58] provides for the right to private and family life, which the ECtHR has interpreted as including the right to protection of personal data [59],[60] article 52(3) of the Charter is applicable. The CJEU itself,[61] AG Cruz Villalón[62] and AG Mengozzi[63] indeed consider at least article 7 of the Charter to be corresponding with article 8 of the ECHR, as they refer in several cases to the case law of the ECtHR regarding this article. The case law of the ECtHR regarding article 8 ECHR is thus incorporated into the acquis of the EU through article 7 (and possibly 8) j° article 53(3) of the Charter. Consequently, the ECHR and the case law of the ECtHR become relevant in assessing the PSD.

[58] Article 8 Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950.
[59] ECtHR 4 December 2008, *S. and Marper v. the United Kingdom*, nos. 30562/04 and 30566/04, paras 66-67.
[60] M.-P. GRANGER and K. IRION, "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection", *ELR* 2014, (835) 837.
[61] Judgment *Volker und Markus*, para 52; Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger*, C-293/12, ECLI:EU:C:2014:238, paras 35, 55.
[62] Opinion of Advocate General Cruz Villalón of 12 December 2013, *Digital Rights Ireland and Seitlinger,* C-293/12, ECLI:EU:C:2013:845, paras 69, 109-112 (hereinafter: 'Opinion of AG Cruz Villalón *Digital Right Ireland*').
[63] Opinion of AG Mengozzi *PNR Canada*, paras 270-271.

Section 2: Case law of the CJEU regarding the primary law of the Union

Subsection 1: Influence of primary law provisions on secondary law

18. The case law of the CJEU regarding the primary law of the EU in the field of data protection is not only relevant *in se*, by setting standards to which all secondary and tertiary law, including the PSD, must adhere, but also for interpreting that secondary and tertiary law. When deciding on data protection issues that also invoke questions about primary law, mostly fundamental rights contained in the Charter, the CJEU almost always needs to interpret both those fundamental rights and pieces of secondary law, notably Directive 95/46. The CJEU has repeatedly stated that Directive 95/46, amongst other directives[64], must be read in the light of fundamental rights,[65] which are now set out in the Charter.[66] It may be expected that the same will be true for the GDPR. This section will first extensively look to a limited number of landmark cases. Thereafter, some other, less applicable, cases will be analysed to the extent they reinforce or supplement the analysed landmark cases.

Subsection 2: Landmark cases

19. In this subsection, four landmark cases about the above-mentioned primary law will be analysed. Every case will first be analysed on its own: *Digital Rights Ireland*,[67] *Tele2 Sverige*,[68] *Schrems*[69] and *PNR Canada*[70]. After these analyses, the reception of these cases by the doctrine will be examined and possible criticisms on the cases will be provided.

---

[64] See e.g. Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970, para 91; Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, para 48.
[65] Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, para 68; Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, para 51.
[66] Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, para 68; Judgment of 17 July 2014, *YS and Others*, C-141/12, ECLI:EU:C:2014:2081, para 54; Judgment *Schrems*, para 38; Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, para 39.
[67] Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger*, C-293/12, ECLI:EU:C:2014:238 (hereinafter: 'Judgment *Digital Right Ireland*').
[68] Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:9705 (hereinafter: 'Judgment *Tele2 Sverige*').
[69] Judgment *Schrems*.

§1 *Digital Rights Ireland*, *Tele2 Sverige* and the mass storage of data

20. *Digital Rights Ireland*[71] and *Tele2 Sverige*[72] are extremely important when considering the compatibility of the mass storage of data concerning the quasi entire population of a member state of the EU with the fundamental rights in the Charter. The judgment in *Digital Rights Ireland* is particularly significant, given the fact that this was the first time[73] that the CJEU declared a piece of secondary legislation, namely the Data Retention Directive ('DRD')[74], invalid in its entirety on the basis of incompatibility with the Charter.[75,76] In the follow-up case *Tele2 Sverige*, the CJEU declared that national (Swedish and UK) legislation previously based on the DRD, and essentially containing the same provisions, is equally incompatible with EU law, considering the fundamental rights enshrined in the Charter.[77] The DRD conferred an obligation upon the Member States to adopt measures to ensure that location and traffic data, such as the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services (all types of metadata), that are generated or processed by providers of publicly available electronic communications services or of a public communications network, are retained for a fixed minimum of 6 months.[78] The content of the communications was not to be stored.[79] The objective of the retention was to contribute to the fight against serious crime and thus, ultimately, to public security[80] by allowing the competent national authorities to access those data.

---

[70] Opinion of 26 July 2017, *Accord PNR UE-Canada*, Opinion 1/15, ECLI:EU:C:2017:592 (hereinafter: 'Opinion *PNR Canada*').
[71] Judgment *Digital Right Ireland*.
[72] Judgment *Tele2 Sverige*.
[73] O. LYNSKEY, "The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*", *CMLRev* 2014, (1789) 1798.
[74] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* L105/54 of 13 April 2006 (hereinafter: 'Directive 2006/24').
[75] Judgment *Digital Rights Ireland*, para 71.
[76] Advocate General Kokott already doubted the compatibility of the mass storage of data as required by the DRD with fundamental rights in her opinion in the case *Promusicae*, see Opinion of Advocate General Kokott of 18 July 2007, *Promusicae*, C-275/06, ECLI:EU:C:2007:454, para 82.
[77] Judgment *Tele2 Sverige*, para 125.
[78] Articles 3, 5 and 6 of Directive 2006/24.
[79] *Ibid*., article 1(2).
[80] Judgment *Digital Rights Ireland*, para 41.

a) Digital Rights Ireland

21. When assessing the DRD in *Digital Rights Ireland*, the CJEU declared that the retention of data and the possible access to them by the competent national authorities interfered with both the right to a private life and the right to protection of personal data.[81] It declared that the retained data "*taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*",[82] a phrase to be paraphrased in several other, later judgments[83]. The CJEU also stated that "*the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*".[84] The argument that since the retained data were not sensitive nor inconvenienced the persons concerned, there could be no interference with the right to a private life, was summarily rejected by the CJEU,[85] thereby referring to its older case law.[86] The CJEU then established that the access of the competent national authorities to the data constituted a *further* interference with article 7 of the Charter.[87] This indicates that the mere retention of the data, even without any access, would already amount to an interference with article 7 (and 8) of the Charter according to the CJEU.[88]

22. The CJEU and AG Cruz Villalón also considered that the DRD could have an impact on the freedom of expression guaranteed by article 11 of the Charter since the DRD could create a 'vague feeling of surveillance' amongst citizens of the EU. This could then in turn influence those citizens in exercising their freedom of expression.[89]

---

[81] *Ibid*., para 29.
[82] *Ibid*., para 27.
[83] Judgment *Tele2 Sverige*, para 99; Opinion *PNR Canada*, para 36; Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paras 54, 60.
[84] Judgment *Digital Rights Ireland*, para 37
[85] Judgment *Digital Rights Ireland*, para 33.
[86] Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, para 75.
[87] Judgment *Digital Rights Ireland*, para 35.
[88] See also O. LYNSKEY, "The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*", *CMLRev* 2014, (1789) 1804.
[89] Judgment *Digital Rights Ireland*, para 28; Opinion of AG Cruz Villalón *Digital Right Ireland*, para 52.

23. After establishing these interferences, the CJEU went on to see whether the interferences could be justified under article 52(1) of the Charter. It decided that although the DRD genuinely pursued an objective of general interest,[90] and did not adversely affect the essence of the affected rights,[91] it did not comply with the principle of proportionality enshrined in article 52(1) of the Charter.[92] The interferences could therefore not be justified.[93]

24. Before coming to this conclusion, the CJEU spelled out a whole list of problematic aspects of the DRD in the light of the principle of proportionality. These considerations can give a clue to which requirements data protection legislation in the EU, including the PSD, should adhere to.

25. The CJEU started by reiterating its settled case law: "*the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives*".[94] Next the CJEU specified this case law in several remarks. Firstly, it stated that the retention required by the DRD applied to "*all means of electronic communication*" of "*practically the entire European population*" in a generalised manner "*without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime*", "*even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime*" and "*persons whose communications are subject to the obligation of professional secrecy*".[95] The CJEU thus seems to have a problem with the wide (almost limitless) material and personal scope of the legislation concerned.

26. Secondly, the CJEU criticised the failure of the DRD to lay down objective criteria "*by which to determine the limits of the access of the competent national authorities to the data and their subsequent use*", notably the absence of prior review by a court.[96]

---

[90] Judgment *Digital Rights Ireland*, para 44.
[91] *Ibid*., paras 39-40.
[92] *Ibid*., para 69.
[93] *Ibid*., para 69.
[94] *Ibid*., para 46.
[95] *Ibid*., paras 56-58.
[96] *Ibid*., paras 60, 62.

27. Thirdly, the CJEU was highly critical of the indiscriminate nature of the data retention period. It stated that "*those data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective*", and criticised both the absence of an objective criterion that should ensure that the retention period is essentially as short as possible and the assurance that the retained data will be irreversibly destroyed at the end of the period.[97]

b) Tele2 Sverige

28. In *Tele2 Sverige*, the CJEU applied more or less the same reasoning vis-à-vis national data retention legislation as in *Digital Rights Ireland*. Again, the CJEU acknowledged interferences with article 7, 8 and 12 of the Charter, thereby repeating its phrases "*very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained*" and "*the persons concerned to feel that their private lives are the subject of constant surveillance*".[98]

29. The CJEU then went on to declare that the national legislation cannot be justified on the basis of article 52(1) of the Charter. Interestingly, the CJEU from there continued by summing up various requirements to which (national) legislation must adhere to in order to satisfy the provisions of the Charter.[99] While this stands in contrast to the judgment in *Digital Rights Ireland*, where the CJEU only listed what is *not* allowed under the Charter, the conclusions to be drawn from both judgments can be more or less the same.

30. First, the CJEU clarified that legislation providing for a targeted retention of traffic and location data must "*lay down clear and precise rules governing the scope and application of such a data retention measures*" and "*indicate in what circumstances and under which conditions a data retention measure may be adopted*".[100] This was further specified as meaning that data retention legislation, as a preventive measure, must be limited to what is strictly necessary with respect to 1) the categories of data, 2) the means of communication affected, 3) the persons

[97] *Ibid*., paras 63, 64, 67.
[98] Judgment *Tele2 Sverige*, paras 99-101.
[99] *Ibid*., paras 108-112, 120-123.
[100] *Ibid*., para 109.

concerned *and* 4) the retention period.[101] The retention of data must "*continue to meet objective criteria, that establish a connection between the data to be retained and the objective pursued*".[102] It must "*be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security*".[103]

31. The CJEU then expressly affirmed what could already be deduced from *Digital Rights Ireland*: "*general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication*" is not allowed.[104]

32. As regards the access of government authorities to the retained data, the CJEU again emphasised the importance of that access being subject to a prior review carried out either by a court or by an independent administrative body (except in cases of validly established urgency).[105] The authorities that have been granted access should also "*notify the persons affected, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities*" to enable the persons affected to exercise their right to a legal remedy.[106]

[101] *Ibid*., para 108.
[102] *Ibid*., para 110.
[103] *Ibid*., para 111.
[104] *Ibid*., para 112., see also F.-X. BRÉCHOT, "Clap de fin pour la conservation généralisée des données de connexion en Europe?", *RUE* 2017, (178) 182; S. PEYROU, "Arrêt «Tele2 Sverige» : l'interdiction du stockage de masse de données à caractère personnel réaffirmée par la Cour de justice de l'Union européenne", *JDE* 2017, (107) 108; *contra* N. FALOT and H. HIJMANS, "Tele2: de afweging tussen privacy en veiligheid nader omlijnd", *NtER* 2017, (44) 49.
[105] Judgment *Tele2 Sverige*, para 120.
[106] *Ibid*., para 121.

c) Possible criticisms

33. Two criticisms on this case law can be distinguished in the doctrine, both of which are essentially saying the CJEU was not stringent enough in its assessment of the challenged legislation.

34. Firstly, it is argued that the CJEU overlooked the 'provided by law' criterion of article 52(1) of the Charter. AG Cruz Villalón did look to this criterion in his opinion in the *Digital Rights Ireland* case and concluded that the DRD was invalid as it did not fulfil this criterion.[107]

35. Secondly, it is contended that the CJEU all too easily accepted that the challenged legislation did respect the essence of the affected rights. If the challenged legislation did not, it would have been *ipso facto* incompatible with the Charter. Especially the reasoning of the CJEU to come to this conclusion is rightly criticised by the doctrine.[108] The CJEU essentially reasoned that since the retention only covered metadata, which would be in itself less sensitive, there could be no disrespecting of the essence of the affected rights.[109] However, much information about someone's private life can be inferred from metadata such as e.g. internet addresses that someone visits, call history, location data associated with someone's use of a mobile phone etc.[110] Such data can reveal someone's religion or sexual orientation, that she or he uses telephone sex lines, has contemplated suicide or is addicted to gambling.[111] The authorities that have access to that information could then possibly obtain the power to blackmail that person.[112] It is therefore not obvious that the essence of the affected rights is respected and the CJEU should therefore at least have argued more extensively why the essence was indeed respected.

---

[107] Opinion of AG Cruz Villalón *Digital Right Ireland*, paras 108-132; O. LYNSKEY, "The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*", *CMLRev* 2014, (1789) 1803.
[108] M.-P. GRANGER and K. IRION, "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection", *ELR* 2014, (835) 847.
[109] Judgment *Digital Rights Ireland*, para 38; Judgment *Tele2 Sverige*, para 101.
[110] A. ROBERTS, "Privacy, Data Retention and Domination: *Digital Rights Ireland Ltd* v *Minister for Communications*", *Mod. Law Rev.* 2015, (535) 544.
[111] *Ibid*.
[112] *Ibid*.

36. One could also add a third criticism. The CJEU failed, in both *Digital Rights Ireland* and *Tele2 Sverige* to examine, whether the requirements provided by article 8 of the Charter itself - and in particular article 8(2) - were satisfied. It only established the existence of an interference with article 8 of the Charter and then proceeded to see whether this interference could be justified under article 52(1) of the Charter. The CJEU could have examined whether the legislation in question required the data to be "*processed fairly*" or "*for specified purposes*" rather than relying on article 52(1) of the Charter. An additional requirement of article 8(2), namely everyone's right of access to data which has been collected concerning him or her and the right to rectify those data, was overlooked as well as a requirement of primary law.

§2 *Schrems* and the annulment of the Safe Harbour

37. The circumstances and the outcome of the *Schrems* case are already explained above (*supra* 2-4). The SHD was annulled on the basis that it violated Directive 95/46, read in the light of the Charter. To the extent that *Schrems* is important for interpreting the requirements flowing from EU primary law (*in casu* the Charter), this paragraph will discuss those aspects. The interpretation of Directive 95/46 will however be addressed only later on.

38. *Schrems* extensively deals with fundamental right shortcomings to the SHD. From these shortcomings, it can *a contrario* be deduced which requirements should be met by the PSD in order to be found compatible with the Charter. Several provisions of primary law are in play in this case. Both the CJEU and AG Bot consider article 7, 8 and 47 of the Charter, and briefly mention article 16(2) TFEU. It is important to note that AG Bot explicitly stated that he did not examine all the shortcomings of the Safe Harbour Scheme exhaustively.[113] It is therefore entirely plausible that the CJEU could have annulled the SHD on additional grounds.

a) The right to a private life

39. Both the CJEU and the AG found that the SHD interfered with article 7 of the Charter.[114] The CJEU again stressed that it is irrelevant whether the data is sensitive or not, or whether the persons concerned have suffered any adverse consequences on account of that interference.[115] After that finding, the CJEU and the AG went on to assess whether the interference could be justified under article 52(1) of the Charter. Already from the beginning of this assessment, it is quite clear that the criticism on the SHD will be scathing.

[113] Opinion of Advocate General Bot of 23 September 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:627, para 129 (hereinafter: 'Opinion of AG Bot *Schrems*').
[114] *Ibid*., para 170; Judgment *Schrems*, para 87.
[115] Judgment *Schrems*, para 87.

40. The CJEU started by saying that the SHD "*does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights*",[116] which is already pointing to the obvious outcome of the case. The same is true for the AG who, already in his assessment of the existence of an interference, stated that the interference is 'extremely serious'.[117]

41. Next, the CJEU established that "*legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must* […] *lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards*",[118] echoing the condition set by article 52(1) of the Charter requiring interferences to be 'provided by law'. Combining this statement with the findings of AG Bot, criticising the SHD for "*the existence of a derogation* […] *in such general and imprecise terms*",[119] one could argue that this condition was not met by the SHD.

42. Whilst the non-fulfilment of the condition to be 'provided by law' can only indirectly be deduced from the CJEU's reasoning, the opposite is true for the conditions to 'be necessary for genuinely reaching the legitimate aim' and 'respect the essence'. The CJEU flat out stated that the SHD is not "*strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail*"[120] and that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life*".[121]

---

[116] *Ibid*., para 88.
[117] Opinion of AG Bot *Schrems*, para 171.
[118] Judgment *Schrems*, para 91.
[119] Opinion of AG Bot *Schrems*, para 183.
[120] Judgment *Schrems*, paras 92-93.
[121] *Ibid*., para 94.

43. Whereas the CJEU bluntly stated that the essence of the right to a private life is not respected, the AG did not explicitly,[122] but the converse is true for the conditions of 'pursuing an objective of general interest' and 'respecting the principle of proportionality'. AG Bot criticised the extremely wide scope of certain 'escape clauses' in the SHD, which state that "*adherence to the safe harbour 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 authorisations, provided that* […] *its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization*".[123] Of the objectives listed under (a), only the 'national security' objective was, according to AG Bot, sufficiently precise to be regarded as an objective of general interest.[124] Since the 'legitimate interests' under (b) are not further defined, the AG came to the conclusion that that provision also did not suffice since it did "*not pursue an objective of general interest defined with sufficient precision*".[125]

44. Concerning the proportionality condition, the AG stated, like already asserted by the CJEU in *Digital Rights Ireland* (*supra* 25), that access to all persons using electronic communications services, without any requirement that the persons concerned represent a threat to national security, is not allowed by the Charter.[126] To say it shortly: "*mass, indiscriminate surveillance is inherently disproportionate*".[127]

45. To conclude, the adherence by the SHD to article 52(1) of the Charter, regarding the interference with article 7 of the Charter, is problematic concerning every single condition of article 52(1), either according to the CJEU or according to the AG.

[122] Opinion of AG Bot *Schrems*, para 177.
[123] *Ibid*., paras 178, 184; Annex I, fourth paragraph, point (a) and (b) SHD.
[124] Opinion of AG Bot *Schrems*, para 184.
[125] *Ibid*., paras 179, 181.
[126] *Ibid*., paras 198-200.
[127] *Ibid*., para 200.

b) The right to protection of personal data

46. Both the CJEU and the AG identified interferences of the SHD with article 8 of the Charter.[128] However, the CJEU mostly ignored article 8 after establishing this and therefore did not find any additional grounds of annulment on that basis. For example, it did not state that the essence of the right to protection of personal data was compromised (as it did with the right to a private life). If the CJEU did find any incompatibilities of the SHD with article 8, then it was solely on the basis of article 8(3) of the Charter. According to the CJEU, article 8(3) and article 16 TFEU require the existence of supervisory authorities which "*must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him*"[129] and which must moreover be able to engage in legal proceedings[130].[131] Even though the CJEU does not explicitly expressed this, it can be deduced from its reasoning that, since the SHD does not ensure the existence of such an authority in the USA[132], data subjects who's personal data are transferred to the USA are deprived from a right stemming from primary law of the EU, which makes the SHD invalid. AG Bot also looked into the compliance of the SHD with the requirement of article 8(3) of the Charter. He thereby criticised the limited competences of the private dispute resolution bodies and the Federal Trade Commission ('FTC') as provided by the SHD.[133] He specifically had a problem with the fact that the FTC did not have jurisdiction over the collection and use of personal information for non-commercial purposes[134] and that the private dispute resolution bodies also did not have the power to rule on *i.a.* the lawfulness of the activities of the United States security agencies.[135] More in general, the AG stated that since the role of neither the FTC, nor the private dispute resolution bodies, is to guard the rights to a private life and the right to protection of personal data and that since both lack the power to monitor possible breaches of those rights by public actors in the USA, they cannot be considered to play a role comparable to that of the authorities foreseen by article

[128] The CJEU only did so implicitly, see *infra* 52.
[129] Judgment *Schrems*, para 99.
[130] *Ibid*., para 65.
[131] Opinion of AG Bot *Schrems*, paras 52, 67, 73.
[132] Judgment *Schrems*, para 89.
[133] Opinion of AG Bot *Schrems*, paras 204-207.
[134] *Ibid*., para 205.
[135] *Ibid*., para 206.

8(3).[136] Unlike the CJEU, the AG therefore explicitly finds that, already on that ground alone, the SHD is invalid.[137]

47. The AG further looked at article 8(1) and (2) of the Charter. He did not only cite both provisions[138] but also established the existence of a separate interference with article 8 of the Charter by the SDH[139] (as opposed to the CJEU, which identified an interference with article 7 and 8 together, see further *infra* 52). He even doubted[140] that the interference could be regarded as respecting the essence of article 8 of the Charter,[141] as opposed to the CJEU, which only stated that the SHD did not respect article 7 of the Charter and pointedly ignored article 8 in this respect. Furthermore, the AG also asserted that there are "*no opportunities for citizens of the Union to obtain access to or rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the United States surveillance programmes*",[142] which arguably indicates that, in his view, the SHD did not only compromise the essence of article 8(1), but also of article 8(2) of the Charter.

c) The right to effective judicial protection

48. Lastly, the possible violation of article 47 of the Charter by the SHD was examined. The CJEU was unusually straightforward with its assessment of this right. It almost immediately declared that the SHD did not respect the essence of the right to effective judicial protection. "*Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of* […] *Article 47 of the Charter.* […] *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*".[143] Besides a citation of article 47 itself, these considerations are the only words the CJEU spent on this issue. AG Bot however did elaborate a bit more. He stated

[136] *Ibid*., paras 205, 207.
[137] *Ibid*., para 207.
[138] *Ibid*., para 52.
[139] *Ibid*., para 170.
[140] This rather weak phrasing can be deplored.
[141] Opinion of AG Bot *Schrems*, para 177.
[142] *Ibid*., para 212.
[143] Judgment *Schrems*, para 95.

that although there is oversight on the surveillance and interception of data of citizens of the Union by the USA Foreign Intelligence Surveillance Court ('FISC'), the proceedings before this court are secret (*in camera*) and *ex parte*.[144] Moreover, procedures providing in judicial remedies for data subjects against surveillance by government services before the FISC are restricted to U.S. citizens and to foreign citizens legally resident on a permanent basis in the USA.[145] Therefore the interference by the SHD with article 47 cannot be justified according to the AG.

d) Possible criticisms

49. Whereas the outcome in *Schrems* was almost universally received well in the doctrine,[146] certain aspects of the reasoning are persuasively criticised.

50. Firstly, the criticism about the distinction between 'content' and 'metadata' in *Digital Rights Ireland* and *Tele2 Sverige* can be repeated.[147] While the CJEU did state that generalised access to content compromises the essence of the fundamental right to a private life, it did not specifically state this regarding the generalised storage of and access to metadata. *A contrario*, one could thus argue that generalised storage of and access to metadata still, in the CJEU's view, does not compromise the essence of any fundamental right (which is not obvious and needs therefore more argumentation as already stated *supra* 35). The CJEU should rather do away with the, some argue, obsolete,[148] distinction between these two categories of data.

---

[144] Opinion of AG Bot *Schrems*, para 173.
[145] *Ibid*., para 211.
[146] See *i.a.* L. AZOULAI and M. VAN DER SLUIS, "Institutionalizing personal data protection in times of global institutional distrust: Schrems", *CMLRev* 2016, (1343) 1370; B. CAROTTI, "Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa", *Giornale di diritto amministrativo* 2016, (333) 343; T. OJANEN, "Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter", *European Constitutional Law Review* 2016, (318) 329; S. PEYROU, "La Cour de justice de l'Union européenne, à l'avant-garde de la défense des droits numériques", JTDE 2015, 395-398; M. SCHEININ, "Towards evidence-based discussion on surveillance: A Rejoinder to Richard A. Epstein", *European Constitutional Law Review* 2016, 341-348; W. STEENBRUGGEN and S. VAN HARTEN, "Safe Harbour is dood. Lang leve Safe Harbour 2.0?", *Mediaforum* 2015, 281-285; X. TRACOL, ""Invalidator" strikes back: The harbour has never been safe", *CLSR* 2016, (345) 356, 362; *contra* R. A. EPSTEIN, "The ECJ's Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices", *European Constitutional Law Review* 2016, 330-340.
[147] X. TRACOL, ""Invalidator" strikes back: The harbour has never been safe", *CLSR* 2016 (345) 357.
[148] T. OJANEN, "Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter", *European Constitutional Law Review* 2016, (318) 328.

51. Secondly, the omission of article 8 of the Charter in several parts of the judgment is a flaw. The statement by TRACOL that "*although the judgment of the Grand Chamber contains many references to personal data, it does not really consider the right to the protection of personal data as a distinct fundamental right*"[149] should be endorsed. Especially the failure by the CJEU to state that the essence of article 8 of the Charter was compromised is regrettable,[150] all the more since the same finding about article 7 of the Charter is the part of the judgment that is the most applauded.[151]

52. A third, more general critique on the structure of the judgment can be made. The CJEU, and to a lesser extent the AG, fail to systematically analyse the different relevant provisions of the Charter. Rather than first establishing an interference with one provision of the Charter, e.g. article 7 or article 8(3), then continuing to see whether this interference can be justified under article 52(1) by checking each and every condition of that article, the CJEU does all kinds of things at the same time. For example, it establishes an interference with article 7 of the Charter[152] and then goes on to state that legislation involving interferences with the fundamental rights guaranteed by articles 7 ánd 8 of the Charter must comply with the condition 'provided by law' in article 52(1) of the Charter,[153] without first explicitly establishing that there is an interference with article 8 of the Charter. Further in the judgment, the CJEU criticises aspects of the SHD concerning the absence of an independent supervisory authority.[154] However, it never establishes that there is an interference with article 8(3) of the Charter, even though that would be a rather obvious observation. Consequently, the CJEU also does not deal with a possible justification of this absence in the light of article 52(1) the Charter. In addition, the CJEU systematically blurs the line between some rights contained in the Charter. The CJEU does not consistently differentiate between article 7 and 8[155] (whereby it probably even means article 8(1)), nor between article 8(2)

[149] X. TRACOL, ""Invalidator" strikes back: The harbour has never been safe", *CLSR* 2016 (345) 355.
[150] M. SCHEININ, "Towards evidence-based discussion on surveillance: A Rejoinder to Richard A. Epstein", *European Constitutional Law Review* 2016, (341) 342.
[151] T. OJANEN, "Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter", *European Constitutional Law Review* 2016, (318) 324.
[152] Judgment *Schrems*, para 87.
[153] *Ibid*., para 91.
[154] *Ibid*., paras 65, 89, 99, 205, 207.
[155] *Ibid*., paras 78, 81, 91, 92.

and 47.[156] The AG on the other hand could have been more clear in his reasoning whether he is examining article 8(3) or 47.[157] The judgment is therefore rather sloppy in some respects, which might also explain why the CJEU failed to state that the essence of article 8 of the Charter was compromised. This sloppiness on the part of the CJEU is not only criticisable from an academic viewpoint but also because it results in a lack of guidance regarding the exact problems with the SHD from a fundamental right perspective.

[156] *Ibid*., para 95.
[157] Opinion of AG Bot *Schrems*, paras 207-212.

§3 *PNR Canada* and mass storage of some data under strict conditions

53. Opinion 1/15 (*PNR Canada*)[158] is the last landmark case that will be examined in this Chapter. Since this case is all about Passenger Name Record ('PNR') data, it is important to first explain this concept. PNR is information provided by passengers when they book tickets and check-in for flights, which is necessary for airlines to run their operations and to track passenger requests and preferences.[159] It usually includes names, addresses, payment and credit card details, seating and luggage information but may also include more conspicuous information such as dietary preferences.[160] While PNR data is primarily collected for commercial purposes, it has also been used by law enforcement authorities tasked with fighting serious crime and terrorism.[161]

54. In 2013, the EU and Canada concluded an agreement about the transfer and use of PNR data ('PNR Agreement').[162] Subsequently, the Council adopted a decision[163] on the signature of that agreement and decided to seek the European Parliament's approval on this decision.[164] The European Parliament ('Parliament') in turn asked the CJEU to give an Opinion about the compatibility of the PNR Agreement with article 16 TFEU and articles 7, 8 and 52(1)) of the Charter.[165] Note that the Parliament also asked whether the appropriate legal basis was used for the agreement, but this part of the judgment will not be discussed.[166]

55. Both the CJEU and the AG, AG Mengozzi, relied to a great extent to the three above-discussed cases. Both however refined their considerations and developed new arguments. Statements included in *PNR Canada* that solely repeat earlier statements from the CJEU will only be dealt with briefly, other aspects will be more extensively discussed.

---

[158] Opinion *PNR Canada*.
[159] C. KUNER, "International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR", *CMLRev* 2018, (857) 859; M. ZALNIERIUTE, "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement", *Mod. Law Rev.* 2018, (1046) 1048.
[160] M. ZALNIERIUTE, "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement", *Mod. Law Rev.* 2018, (1046) 1048.
[161] *Ibid*.
[162] Opinion *PNR Canada*, paras 19-20.
[163] Proposal for a Council Decision on the conclusion of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, COM(2013) 0528 final of 18 July 2013.
[164] Opinion *PNR Canada*, para 23.
[165] *Ibid*., para 2.
[166] *Ibid*., para 2.

a) Interferences with the right to a private life and the right to protection of personal data

56. Departing from its earlier practice in *Schrems*, the CJEU in *PNR Canada* explicitly differentiated between articles 7 and 8 of the Charter. It started by stating that, when it assesses the compatibility of the PNR Agreement with the right to the protection of personal data, enshrined in both article 16(1) TFEU and article 8 of the Charter, it will refer solely to the second of those provisions since that provision is more specific.[167] The CJEU therefore recognised article 16(1) TFEU as a separate relevant provision, even though it did not make use of that provision in the present case and, at the same time, recognised the right to protection of personal data as a separate fundamental right. Next, the CJEU established interferences with the right to a private life[168] and the right to protection of personal data[169] in separate paragraphs of its opinion, thereby putting its differentiation between the two rights immediately to practice.

57. Regarding article 7 of the Charter, the CJEU stated that even though that some of the PNR data "*taken in isolation, does not appear to be liable to reveal important information about the private life of the persons concerned*", that data "*taken as a whole* […] *may, inter alia, reveal* […] *relationships existing between air passengers and* […] *may even provide sensitive information about those passengers*".[170] The claim by the French Government that the data does not allow very precise conclusions concerning the private life of passengers to be drawn[171] is thus rebuffed by the CJEU. The fact that the persons affected will not suffer any inconvenience is once again put aside as irrelevant.[172] One can therefore conclude that the CJEU interprets the right to a private life broadly and that transfers of less data than e.g. in *Digital Rights Ireland* still fall under article 7 of the Charter, which is also the view taken by AG Mengozzi.[173]

[167] *Ibid*., para 120.
[168] *Ibid*., paras 122, 124, 125, 128, 131, 132.
[169] *Ibid*., paras 123, 126.
[170] *Ibid*., para 128.
[171] Opinion of AG Mengozzi *PNR Canada*, para 148.
[172] *Ibid*., para 172.
[173] *Ibid*., para 170.

b) Article 8(2): the basis for the processing

58. After the establishment of an interference with article 7 and 8 of the Charter, the CJEU, for the first time, looked to article 8(2) of the Charter to justify the interference with the right to protection of personal data. AG Mengozzi does the same thing, albeit that he immediately stated that article 8(2) and 52(1) partially overlap.[174] The CJEU asserted that under article 8(2), personal data must be processed "*for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*".[175] Both the CJEU and AG then stated that the PNR Agreement did not base the processing of the data concerned on the consent of the air passengers.[176] The CJEU thereby specified that the processing of PNR data under the envisaged agreement pursues a different objective from that for which that data is collected by air carriers and that it therefore requires either the air passengers' own additional consent or some other legitimate basis laid down by law.[177] The CJEU concluded its assessment of article 8(2) of the Charter by saying that the PNR Agreement constitutes 'some other basis' that is 'laid down by law'.[178] The requirement of that basis being legitimate will however only be dealt with later on, in the assessment whether the PNR Agreement pursues an objective of general interest under article 52(1) of the Charter.[179] The requirement 'some other legitimate basis' under article 8(2) of the Charter therefore seems to be one and the same as the requirement of 'an objective of general interest' under article 52(1) of the Charter. The same is true for the requirement 'laid down by law' under article 8(2) of the Charter and 'provided for by law' under article 52(1) of the Charter.

[174] *Ibid*., para 188.
[175] Opinion *PNR Canada*, para 137.
[176] Opinion *PNR Canada*, paras 143-144; Opinion of AG Mengozzi *PNR Canada*, para 184.
[177] Opinion *PNR Canada*, paras 142-143.
[178] *Ibid*., para 147.
[179] *Ibid*., para 147.

c) Justification of the interferences with the right to a private life and the right to protection of personal data under article 52(1)

(1) Provided by law

59. In its reasoning concerning article 8(2) of the Charter, the CJEU already accepted that the requirement 'provided for by law' was met. The AG considered that some aspects of the PNR Agreement (*i.a.* the precise establishment of methods relating to the identification of passengers on the basis of patterns of behaviour) grant quite much discretion to the Canadian authorities.[180] Furthermore he questioned whether the agreement itself should not more exhaustively regulate these aspects.[181] Nonetheless, the AG also readily accepted that the requirement 'provided for by law' was met[182], since, "*overall, the agreement is drafted in sufficiently clear terms to enable all those concerned to understand, to the requisite standard, the circumstances in which and the conditions on which the data are transferred to the Canadian authorities, processed, retained and possibly subsequently disclosed by those authorities, and to regulate their conduct accordingly*".[183]

60. However, later on, under the section "*The necessity of the interferences* […]" the CJEU made various statements regarding the imprecise nature of some provisions of the PNR Agreement. Even though the CJEU made these statements in the context of the assessment whether the PNR Agreement is 'strictly necessary', it is useful to discuss those statements here, since, one could argue, they rather undermine the requirement 'provided for by law' than the necessity requirement. The CJEU for example stated that "*EU legislation cannot be limited to requiring that access to such data should be for one of the objectives pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use*".[184] The CJEU also remarked that the agreement should "*define in a clear and precise manner the PNR data which the air carriers are required to transfer to Canada under the agreement*".[185] Putting

[180] Opinion of AG Mengozzi *PNR Canada*, para 164 j° 193.
[181] *Ibid.*
[182] *Ibid.*, paras 190-193.
[183] *Ibid.*, para 193.
[184] Opinion *PNR Canada*, para 192.
[185] *Ibid.*, para 155.

this test to practice, the CJEU next decided that, e.g., the data categories 'available frequent flyer and benefit information (free tickets, upgrades, etc.)' and 'all available contact information (including originator information)' are not sufficiently clear.[186] Specifically, the terms 'etc' and 'all available contact information' are too broad.[187] Some of the provisions concerning the purposes for which Canada may process the data, e.g. to 'ensure the oversight or accountability of the public administration' are also not sufficiently precise.[188] AG Mengozzi furthermore was of the opinion that the use of the term 'Canada' in several provisions of the PNR Agreement was not sufficiently precise and that this should rather be 'the Canadian competent authority'.[189] The same is true for the term 'serious transnational crime' which was defined by referring to domestic Canadian legislation ("*any offence punishable in Canada by a maximum deprivation of liberty of at least four years*").[190] AG Mengozzi considered that, the PNR Agreement should have been "*accompanied by an exhaustive list of the offences coming within the definition of 'serious transnational crime*'". [191] The CJEU however declared that the terms 'serious transnational crime' and 'Canada' are sufficiently precise.[192]

(2) Respect the essence

61. Both the CJEU and the AG fairly rapidly concluded that the PNR Agreement did not compromise the essence of the fundamental rights contained in either article 7 and 8 of the Charter.[193] They both established this in separate findings for each fundamental right. By this practice, they made clear that, at least in theory, the finding that the essence of the right to a private life is not compromised does not *ipso facto* mean that the same will be true for the right to protection of personal data or *vice versa*.

[186] *Ibid*., para 156.
[187] *Ibid*., paras 157-158.
[188] *Ibid*., para 181 j° 30.
[189] Opinion of AG Mengozzi *PNR Canada*, paras 249-251.
[190] *Ibid*., para 237.
[191] *Ibid*., para 237.
[192] Opinion *PNR Canada*, paras 177, 178, 185.
[193] Opinion *PNR Canada*, paras 150-151; Opinion of AG Mengozzi *PNR Canada*, paras 185-187.

(3) Objective of general interest

62. The CJEU and the AG likewise concluded without much elaboration that the PNR Agreement meets an objective of general interest, whereby the CJEU also cited the right to security of article 6 of the Charter.[194]

(4) Strict necessity and proportionality

63. After establishing all the above, both the CJEU and the AG very extensively evaluated a whole list of aspects of the PNR Agreement, e.g. the categories of data, the scope *ratione personae*, the purpose of the data processing, the competent Canadian authority responsible for the processing, the retention and disclosure of the data.[195] Interestingly, the CJEU reviewed all these aspects from the angle of necessity (without once using the term 'proportionality' in this part of the Opinion), while the AG used the term 'proportionality' in the relevant heading of his opinion and also used this term later on in his assessment. The AG nonetheless also used a subheading 'strict necessity' which covered the biggest part of his assessment. It is therefore really hard to determine exactly which condition of article 52(1) of the Charter (proportionality or necessity) is assessed. This is further complicated by the already mentioned settled case law of the CJEU that uses the term 'necessary' in its definition of proportionality: "*the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives*".[196] Therefore, the conditions 'be necessary for genuinely reaching the legitimate aim' and 'respect to the principle of proportionality' will here be treated together since they are inextricably linked in this case. Furthermore, since there is a big overlap between the reasoning of the CJEU and AG Mengozzi, the reasoning of the latter will only be analysed to the extent that it differs from that of the CJEU.

[194] Opinion *PNR Canada*, paras 148, 149, 151; Opinion of AG Mengozzi *PNR Canada*, para 194.
[195] Opinion *PNR Canada*, paras 154-217; Opinion of AG Mengozzi *PNR Canada*, paras 196-327.
[196] See Judgment *Digital Rights Ireland*, para 46 and the case law cited there.

64. The appropriateness (see the settled case law of the CJEU regarding the definition of proportionality, also *supra* 25) of the PNR Agreement was readily accepted by the CJEU.[197]

65. The CJEU next however found that several provisions were not 'strictly necessary', to use its own terminology. Some of these provisions, and the assessment thereof by the CJEU, are already analysed *supra* 59-60, where it is argued that these provisions rather infringe upon the condition 'provided by law' than upon the conditions examined here. This is true for the categories of data, the purpose of the data processing and the competent Canadian authority, which will therefore not be examined again.

66. Regarding the scope *ratione personae* of the PNR Agreement, the CJEU first found that the "*envisaged agreement covers the PNR data of all air passengers flying between the European Union and Canada*" and this "*regardless of whether there is any objective evidence permitting the inference that the passengers are liable to present a risk to public security in Canada*".[198] Somewhat surprisingly in the light of its above-discussed, earlier case law, the CJEU then stated that the PNR Agreement "*does not exceed the limits of what is strictly necessary in so far as it permits the transfer of the PNR data of all air passengers to Canada*".[199] The reasoning behind this statement might also be found in the remarks of the AG concerning this issue. AG Mengozzi indeed stated that unlike the situation in *Digital Rights Ireland*, all persons coming under the PNR Agreement voluntarily take a means of international transport to or from a third country.[200]

67. As regards to the retention and use of the data, the CJEU differentiated between several situations but nevertheless applied the same test to these different situations. It asserted that "*the legislation in question must, i.a., continue to satisfy objective criteria that establish a connection between the personal data to be retained and the objective pursued*".[201]

[197] Opinion *PNR Canada*, paras 152-153.
[198] *Ibid*., para 186.
[199] *Ibid*., para 189.
[200] Opinion of AG Mengozzi *PNR Canada*, para 242.
[201] Opinion *PNR Canada*, para 191.

68. The CJEU was convinced that as long as the air passengers are in Canada, that necessary connection exists and that "*the agreement therefore does not exceed the limits of what is strictly necessary merely because it permits the systematic retention and use of the PNR data of all air passengers*".[202] Regarding the use of the detained data, the CJEU first stated that the data could be used for border control purposes, even without prior review by a court.[203] For other uses of the data, the CJEU did require 1) new circumstances justifying that use ("*objective evidence from which it may be inferred that the PNR data of one or more air passengers might make an effective contribution to combating terrorist offences and serious transnational crime*" is given as an example), 2) a reasoned request by the competent authorities asking to use the data and 3) prior review by a court, or by an independent administrative body.[204] All of this must moreover happen within the framework of procedures for the prevention, detection or prosecution of crime.[205] The CJEU concluded that in so far the PNR Agreement does not meet these requirements, it is not 'strictly necessary'.[206]

69. As regards air passengers that have left Canada, and in respect of whom no objective evidence has been established that they present a risk as regards terrorism or serious transnational crime, the CJEU was not convinced that there exists a connection between the personal data to be retained and the objective pursued (*supra* 67).[207] Consequently, the retention of the PNR data of those air passengers after they have left Canada is not strictly necessary according to the CJEU.[208] PNR data of air passengers in respect of whom a risk of a nature as stated above has been established, can however be retained,[209] even for up to five years.[210] The use of that data needs to be subject to the conditions explained *supra* 68.[211]

[202] *Ibid*., para 197.
[203] *Ibid*., para 197.
[204] *Ibid*., paras 200-202.
[205] *Ibid*., para 202.
[206] *Ibid*., para 203.
[207] *Ibid*., para 205.
[208] *Ibid*., para 206.
[209] *Ibid*., para 207.
[210] *Ibid*., para 209.
[211] *Ibid*., para 208.

70. Lastly, when assessing the disclosure of the PNR data by Canada to third countries, the CJEU decided that Canada may only transfer the data to third countries that ensure an essentially equivalent level of protection of fundamental rights than the EU (see also *infra* 174-178).[212] Moreover, the Canadian competent authorities cannot have a discretionary power such as provided for by the PNR Agreement to establish this 'equivalent level of protection' but this requires an agreement between the EU and the third country concerned or an adequacy decision by the Commission (such as the SHD or PSD).[213] As regards the disclosure by Canada to individuals, the CJEU likewise concluded that the PNR Agreement is not strictly necessary (or, one could argue, not proportionate) since there is no delimitation at all of the persons to whom the data may be disclosed, of exactly which data may be disclosed nor of the use that may be made of that data.[214]

d) The right of access and rectification

71. Unlike in *Digital Rights Ireland* and *Schrems*, the CJEU referred to article 8(2) of the Charter[215] and moreover assessed whether the contested legislation complies with that provision. The CJEU also repeated its case law from *Rijkeboer*[216], essentially stating that the right of access and rectification might also be derived from article 7 of the Charter.[217] Although the CJEU next acknowledged that the PNR Agreement does provide for those rights,[218] it held that to ensure those rights, the PNR Agreement should specify that "*air passengers must be notified of the transfer of their PNR data to Canada and of its use as soon as that information is no longer liable to jeopardise the investigations being carried out by the government authorities referred to in the envisaged agreement*".[219] One could argue that the CJEU created here a separate right to transparency, a right which the PNR Agreement should include in its provisions in order not be found incompatible with the Charter.[220]

---

[212] *Ibid*., para 214.
[213] *Ibid*., paras 213-215.
[214] *Ibid*., paras 216-217.
[215] *Ibid*., para 218.
[216] Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, para 49.
[217] Opinion *PNR Canada*, para 219.
[218] *Ibid*., para 221.
[219] *Ibid*., para 220 j° 225.
[220] See N. LE BONNIEC, "L'avis 1/15 de la CJUE relatif à l'accord PNR entre le Canada et l'Union européenne : une délicate conciliation entre sécurité nationale et sécurité numérique", *RTD Eur* 2018, 617-628.

e) The right to an independent supervisory authority

72. The CJEU also looked to article 8(3) of the Charter, providing for an independent supervisory authority. It firmly asserted the importance of this provision, stating that such an authority is "*an essential component of the protection of individuals with regard to the processing of personal data*".[221] Note that this view is a reiteration of earlier case law and is also reinforced by the CJEU in later cases (*infra* 147-152),[222] where the CJEU stated that "*the supervisory authorities* […] *are to act with complete independence in exercising the functions entrusted to them*".[223] The PNR Agreement provided for oversight by an 'independent public authority' or by an 'authority created by administrative means that exercises its functions in an impartial manner and that has a proven record of autonomy'.[224] Whereas the CJEU did not have a problem with the phrase 'independent public authority', it did with the alternative.[225] It stated that the second formulation "*seems to permit the oversight to be carried out, partly or wholly, by an authority which does not carry out its tasks with complete independence, but which is subordinate to a further supervisory authority, from which it may receive instructions, and which is therefore not free from any external influence liable to have an effect on its decisions*".[226] The AG specified this further, by stating that such a body could be "*directly subordinate to the responsible Minister*", and could therefore not "*be regarded as an independent supervisory authority for the purposes of Article 8(3) of the Charter*".[227] He nevertheless seemed to keep the door open to the acceptance of such a body, provided that an administrative appeal to another, this time genuinely independent supervisory authority, is provided for.[228] The AG also specified that the PNR Agreement should explicitly "*state that requests for access, correction and annotation submitted by passengers not present on Canadian territory may be brought before an independent public authority*".[229]

---

[221] Opinion *PNR Canada*, para 229.
[222] See e.g. Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, para 23 (hereinafter: 'Judgment *Commission v Germany*'); Judgment of 16 October 2012, *Commission v Austria*, C-614/10, ECLI:EU:C:2012:631, para 37 (hereinafter: 'Judgment *Commission v Austria*'); Judgment of 8 April 2014, *Commission v Hungary*, C-288/12, ECLI:EU:C:2014:237, para 48 (hereinafter: 'Judgment *Commission v Hungary*'); Judgment of 5 June 2018, *ULD Schleswig-Holstein v Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388.
[223] Judgment of 5 June 2018, *ULD Schleswig-Holstein v Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388., para 68.
[224] Article 10(1) of the PNR Agreement.
[225] Opinion *PNR Canada*, paras 230-231.
[226] *Ibid*., para 230.
[227] Opinion of AG Mengozzi *PNR Canada*, para 315.
[228] *Ibid*., para 320.
[229] *Ibid*., para 321.

f) The principle of non-discrimination

73. Lastly, the CJEU made use of article 21 of the Charter, containing the principle of non-discrimination. The CJEU first determined that the categories of data as described by the PNR Agreement could cover sensitive data, meaning data that reveals information such as 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or information concerning 'a person's health or sex life'.[230] Then it went on to state that measures based on the premise that such data may in itself be relevant to combat terrorism or serious transnational crime "*regardless of the individual conduct of the traveller concerned*", would infringe article 7 and 8, read in conjunction with article 21 of the Charter.[231] The CJEU thus rightly ruled out practices such as racial profiling. It decisively stated that the transfer of the above-mentioned data to Canada and the framework concerning the use and retention of such data by the authorities of Canada is not allowed under the Charter.[232] In addition, regarding automated processing, the AG considered that scenarios, predetermined assessment criteria or databases used for automated processing cannot be based on such sensitive data.[233]

g) Remarks and possible criticisms

74. *PNR Canada* is, quite obviously, an extremely important case regarding a possible future clash between the Charter and the PSD. This was also immediately recognised by the doctrine.[234] The Opinion has by and large been received positively,[235] despite the existence of essentially two criticisms.

---

[230] Opinion *PNR Canada*, para 164.
[231] *Ibid*., para 165.
[232] *Ibid*., paras 167, 172.
[233] Opinion of AG Mengozzi *PNR Canada*, para 258.
[234] C. DOCKSEY, "Opinion 1/15 Privacy and security, finding the balance", *MJECL* 2017, (768) 770; H. HIJMANS, "PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators", *EDPL* 2017, (406) 406, 411.
[235] See *i.a.* C. DOCKSEY, "Opinion 1/15 Privacy and security, finding the balance", *MJECL* 2017, 768–773; C. FORGET, "L'avis de la C.J.U.E. sur l'accord PNR Union européenne-Canada : une occasion ratée de réaffirmer le principe de finalité?", *JDE* 2018, 87-89; H. HIJMANS, "PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators", *EDPL* 2017, 406-412; C. KUNER, "International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR", *CMLRev* 2018, 857–882; N. LE BONNIEC, "L'avis 1/15 de la CJUE relatif à l'accord PNR entre le Canada et l'Union européenne : une délicate conciliation entre sécurité nationale et sécurité numérique", *RTD Eur* 2018, 617-628.

75. The first criticism basically alleges that the CJEU in this Opinion usurped the role of the legislative branch of government and that it therefore hampers future negotiations. It is alleged that the rigorous scrutiny by the CJEU, reviewing the PNR Agreement almost article-by-article, giving detailed guidelines about what is allowed and what is not, amounts to the CJEU acting as 'a sort of co-legislator'.[236] This intense screening would make it harder for the EU to negotiate since it curtails the room for manoeuvre.[237] This criticism is undeserved. It has already been argued (*supra* 52) that the CJEU should on the contrary be very precise in its judgments, this way providing the Commission clear guidelines of what is allowed under the Charter. This is *a fortiori* true for an Opinion by the CJEU. What use has a broad room for manoeuvre when the CJEU subsequently annuls the negotiated agreement on the basis of incompatibility with the Charter? Indeed, it has even been argued that *PNR Canada* strengthens the hand of EU negotiators since they can insist to include some provisions considering the CJEU will otherwise invalidate the negotiated agreement.[238]

76. The second criticism is on the substance of the Opinion and concerns the apparent acceptance of generalised retention of data, albeit under strict conditions, by the CJEU. Several authors argue that while the outcome of the Opinion is laudable, the reasoning opens the door to mass surveillance.[239] While this development can be criticised on its own, it can also be construed as contravening earlier case law, notably the above-discussed cases *Digital Rights Ireland*, *Tele2 Sverige* and *Schrems*. For example, in *Schrems*, the CJEU ruled that generalised access to content compromised the essence of the right to a private life (see also *supra* 42), but in *PNR Canada* the same generalised access could nonetheless be, in the CJEU's view, compatible with fundamental rights in the EU.[240] The CJEU thus distinguishes between several mass-surveillance schemes, depending on the data collected,[241] which means that, in general, such a scheme is no longer necessarily unacceptable. The Opinion seems to contradict the CJEU's statements analysed *supra*

[236] H. HIJMANS, "PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators", European Data Protection Law Review 2017, (406) 410.
[237] *Ibid*.
[238] C. DOCKSEY, "Opinion 1/15 Privacy and security, finding the balance", *MJECL* 2017, (768) 771.
[239] *Ibid*., 772; J. EYNARD, "D'une ingérence généralisée à une autre : deux poids, deux mesures ?", *R.T.D.H.* 2018, 761-783; C. FORGET, "L'avis de la C.J.U.E. sur l'accord PNR Union européenne-Canada : une occasion ratée de réaffirmer le principe de finalité?", *JDE* 2018, (87) 89.
[240] M. ZALNIERIUTE, "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement", *Mod. Law Rev.* 2018, (1046) 1058;
[241] *Ibid*.

25 of *Digital Rights Ireland* as well. EYNARD describes it as follows: "*La comparaison des décisions laisse penser qu'un double régime est instauré par la Cour. Une conservation généralisée et indifférenciée des données peut être mise en œuvre en matière de données PNR là où elle est prohibée en matière de données de connexion.*"[242] She next criticises this distinction as 'deux poids, deux mesures'. The argument that less people are affected by the PNR Agreement than by the DRD, and that this difference explains the differing case law of the CJEU is indeed not convincing.[243] The argument put forward by AG Mengozzi, that persons taking a flight to Canada voluntarily do this, also does not convince.[244] What is the difference, between someone who – voluntarily – takes a flight and someone who, in the context of the DRD, – voluntarily – uses a smartphone or a tablet?[245] According to EYNARD, the true reason behind the differentiating treatment by the CJEU is rather pragmatic or even political.[246] That view should be seconded. The reference to the Convention of Chicago (a treaty which states that air passengers must abide by a country's laws regarding entry or exit of that country, when entering or exiting that country) by the CJEU and the remark of AG Mengozzi that without an agreement, Canada would still, unilaterally, apply its PNR scheme, point in that direction.[247] The CJEU might have thought that allowing a PNR scheme under strict conditions, rather than rejecting any PNR scheme out of hand, will ensure a higher protection of fundamental rights.

[242] J. EYNARD, "D'une ingérence généralisée à une autre : deux poids, deux mesures ?", *R.T.D.H.* 2018, (761) 772.
[243] *Ibid*., 773.
[244] *Ibid*., 774-775.
[245] *Ibid*., 775.
[246] *Ibid*., 775.
[247] *Ibid*., 775.

Subsection 3: other relevant case law

§1 The scope of the protection provided by article 7 and 8 of the Charter

77. It already has been explained that it is not required for data to be sensitive or for its retention to inconvenience the persons concerned, in order for the right to a private life to come into play (*supra* 21 and 57). In addition, CJEU has ruled that data concerning professional activities also fall under the right to a private life,[248] and therefore under the protection of article 7 of the Charter.[249] In general, any information relating to an identified or identifiable individual is protected both by article 7 and article 8 of the Charter.[250] The CJEU has also clarified that legal persons can claim the protection of Articles 7 and 8 of the Charter, only in so far the official title of the legal person identifies one or more natural persons.[251]

§2 *Volker und Markus* and privacy and data protection v transparency

78. It is easy to understand that the right to a private life and the right to the protection of personal data can clash with transparency objectives. In *Volker und Markus*[252], the CJEU needed to deal with exactly such a clash. The applicants in that case were a farmer (a natural person) and an agricultural undertaking (a legal person), both applying for (and eventually obtaining) agricultural subsidies from two European funds.[253] The regulation governing these funds stated that the member states needed to ensure annual *ex-post* publication of the beneficiaries of the subsidies and the amounts received per beneficiary.[254] The CJEU ruled that this constituted an interference with article 7 and 8 of the Charter.[255] Whilst the CJEU accepted the aim to increase

[248] Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, para 68.
[249] Judgment *Volker und Markus* para 59.
[250] *Ibid*., para 52.
[251] *Ibid*., para 53.
[252] Judgment *Volker und Markus*.
[253] *Ibid*., para 25.
[254] Article 44a of Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, as amended by Council Regulation (EC) No 1437/2007 of 26 November 2007, and Commission Regulation (EC) No 259/2008 of 18 March 2008 laying down detailed rules for the application of Regulation No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD), *OJ* L209/01 of 11 August 2005.
[255] Judgment *Volker und Markus*, paras 58, 64.

transparency as an objective of general interest,[256] it stated that "*no automatic priority can be conferred on the objective of transparency over the right to protection of personal data*".[257] It concluded that the interference with the fundamental rights of the agricultural undertaking could be justified,[258] but that the interference with the fundamental rights of the farmer could not.[259] The CJEU however did not declare that any publication of personal data of natural persons is *per se* impermissible, it only asserted that legislation providing for this should be properly balanced and properly justified.[260]

§3 The cost of the right of access

79. Regarding the right of access to personal data enshrined in article 8(2) of the Charter, the CJEU has ruled that fees may be levied when that right is exercised, but that such fees "*may not be fixed at a level likely to constitute an obstacle to the exercise of the right of access*".[261] Moreover, "*where a public authority levies a fee on an individual exercising the right to access personal data relating to him, the level of that fee should not exceed the cost of communicating such data*".[262]

§4 *Google Spain* and the right to be forgotten

80. Another interesting facet of the case law of the CJEU is its *de facto* elevation of the right to be forgotten (one way to conceptualise the right to erasure)[263] to a fundamental right which can be directly inferred from the Charter.[264] In *Google Spain*[265], a Spanish citizen had asked Google to remove or conceal links to pages of the La Vanguardia newspaper dating from 1998, in which an

---

[256] *Ibid*., para 71.
[257] *Ibid*., para 85.
[258] *Ibid*., para 88.
[259] *Ibid*., para 86.
[260] M. BOBEK, "Joined Cases C-92 & 93/09, *Volker und Markus Schecke GbR and Hartmut Eifert*, Judgment of the Court of Justice (Grand Chamber) of 9 November 2010", *CMLRev* 2011, (2005) 2013.
[261] Judgment of 12 December 2013, *X*, C-486/12, ECLI:EU:C:2013:836, para 29.
[262] *Ibid*., para 30.
[263] J. AUSLOOS, *The Right to Erasure: Safeguard for Informational Self-Determination in a Digital Society?*, Dissertation for the degree of Doctor of Laws (PhD) KU Leuven, 2018, 91-92.
[264] M. KRZYSZTOFEK, *Post-reform Personal Data Protection In the European Union : General Data Protection Regulation (eu) 2016/679***,** Alphen aan den Rijn, Kluwer Law International B.V., 2017, 119 (hereinafter: 'KRZYSZTOFEK, *Post-reform Personal Data Protection*').
[265] Judgment of 13 May 2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317 (hereinafter: 'Judgment *Google Spain*').

announcement mentioning his name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.[266] This way, these pages would cease to be included in google search results.[267] The CJEU established an interference with article 7 and 8 of the Charter[268] and stated that this interference could not be justified.[269] The CJEU held that the rights of a data subject under article 7 and 8 of the Charter override, as a rule, "*not only the economic interest of the operator of the search engine*"[270] but also the interest of the internet users "*in finding that information upon a search relating to the data subject's name*".[271] Exceptions can only exist for particular reasons, e.g. when the data subject plays an important role in public life.[272]

81. Although the *Google Spain*[273] case has no direct connection to the string of landmark cases analysed in subsection 2, it can be viewed as a part of a broader pushback against mass-surveillance programmes.[274] The CJEU in this case strengthened data subjects' rights by implicitly supporting the recognition of individual control over personal data as an aspect of the right to protection of personal data.[275] It emphasised that data subjects enjoy these rights, irrespective of whether these personal data are 'private', or whether the processing of personal data causes prejudice to them.[276]

[266] *Ibid*., para 14.
[267] *Ibid*., para 15.
[268] *Ibid*., para 80.
[269] *Ibid*., para 81.
[270] *Ibid*., para 97.
[271] *Ibid*., paras 81, 97.
[272] *Ibid*., paras 81, 97, 99.
[273] Judgment *Google Spain*.
[274] M. ZALNIERIUTE, "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement", *Mod. Law Rev*. 2018, (1046) 1055.
[275] O. LYNSKEY, "Control over Personal Data in a Digital Age: *Google Spain* v *AEPD and Mario Costeja Gonzalez*", *Mod. Law Rev*. 2015, (522) 529.
[276] *Ibid*., 527.

CHAPTER II: THE PROTECTION OFFERED BY THE GDPR

Section 1: Scope of the GDPR

82. *Ratione materiae*, the GDPR is applicable to the processing of personal data,[277] subject to several exceptions (*infra* 84).[278] The material scope of the GDPR is almost the same as that of the old Directive 95/46, since the scope of the Directive was defined in the same way and, moreover, the definitions of the terms 'processing' and 'personal data' are extremely alike as well.[279] The case law of the CJEU regarding the scope *ratione materiae* of Directive 95/46 can therefore be used to delineate the scope *ratione materiae* of the GDPR. The definition of 'processing' as interpreted by the CJEU basically covers any use or handling of personal data, the duration or intensity of the processing is completely irrelevant.[280] 'Personal data' means "*any information relating to an identified or identifiable natural person (data subject)*".[281] Note that, as could already be deduced from the examined case law of the CJEU regarding the Charter (*supra* 19-81), 'personal data' is interpreted very widely by the CJEU.[282] Also note that even though the definition of 'data subject' in the GDPR clearly excludes legal persons, which has as a consequence that legal persons cannot claim the protection provided by the GDPR, some legal persons can still claim some protection on the basis of the Charter (*supra* 77).

[277] Article 2(1) GDPR.
[278] *Ibid*., article 2(2).
[279] Articles 1, 2(a) and 2(b) of Directive 95/46; articles 2(1), 4(1) and (2) GDPR.
[280] D. RÜCKER, "Scope of application of the GDPR, I." in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 10 (hereinafter: 'RÜCKER, Chapter B, I.')
[281] See further RÜCKER, Chapter B, I., 12-21.
[282] See also Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, para 88; Judgment of 22 December 2017, *Peter Nowak*, C-434/16, ECLI:EU:C:2017:994, para 33, where the CJEU itself states that the scope of Directive 95/46 is very wide.

83. *Ratione personae*, the GDPR is applicable to data controllers, data processers and third parties (as defined by the GDPR). To summarise, this means that whoever determines the purposes and means of the processing of personal data or processes personal data is subject to the GDPR.[283]

84. There are a number of important exceptions to the scope of the GDPR. The Regulation does not apply to the processing of personal data 1) in the course of an activity which falls outside the scope of EU law, 2) by the Member States when carrying out activities which fall within the scope of the Common Foreign and Security Policy, 3) by a natural person in the course of a purely personal or household activity and 4) by competent authorities for the purposes of 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.[284] In the context of the PSD, the first and the last exception are the most important. The first exception is important since this means that the activities of security services do not fall under the GDPR.[285] The importance of the last exception is self-evident in the context of mass-surveillance. The significance of these exceptions will be discussed *infra* 179-182.

[283] Article 4(7) and (8) GDPR; see further D. RÜCKER, "Scope of application of the GDPR, II." in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 23-37.
[284] Article 2(2) GDPR.
[285] Article 4(2) Treaty on European Union, *OJ* C326 of 26 October 2012 (hereinafter: 'TEU').

Section 2: Requirements set by the GDPR, compared with the requirements already set by Directive 95/46 and the Charter

85. This section will examine the relevant requirements to be found in the GDPR. In order to see if the GDPR really provides additional protection, its requirements will be compared to the requirements already laid down by the Charter. The requirements of the GDPR will, where relevant, be compared to the requirements already offered by the now repealed Directive 95/46, to see whether the GDPR has increased protection. Case law of the CJEU will be included where necessary.

Subsection 1: 'Open' norms and 'key principles'

86. Article 5 GDPR establishes several principles relating to the processing of personal data. These principles are mostly quite vague, open legal terms. Most principles do not explicitly instruct which concrete conditions need to be adhered to in order not to breach the principle,[286] although some principles are further specified in other articles. They should rather be seen as overarching norms, further specified in other chapters of the GDPR, providing the basic framework of data protection law.[287]

§1 Lawfulness

87. Article 5 GDPR states in general terms that personal data must be processed lawfully.[288] A further explanation is provided for in article 6 GDPR, which lays down several scenarios in which the processing is 'lawful'.[289,290] Article 6 GDPR states very clear that *only* the scenarios provided

[286] S. DIENST, "Lawful processing of personal data in companies under the GDPR" in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 49 (hereinafter: 'DIENST, Chapter C').
[287] *Ibid*., 50.
[288] Article 5(1)(a) GDPR. The principle of lawfulness was already established by Directive 95/46 and has stayed virtually the same under the GDPR, see Recitals 30, 31 j° articles 5 and 6 Directive 95/46.
[289] Article 6 GDPR.
[290] The construction where there is 1) a principle of lawfulness and 2) a separate article which sets out the scenarios in which processing is lawful, stems from Directive 95/46. The connection between these two elements is also accepted by the CJEU, see e.g. Judgment of 16 December 2008, *Huber*, C-524/06, ECLI:EU:C:2008:724, para 48; Judgment of

for in that article can make the processing lawful, thereby implicitly specifying that processing of personal data is generally not lawful. Processing of personal data can hence only be lawful by exception. Article 6 GDPR considers as lawful the scenario where on the one hand the data subject has given consent, and on the other hand the scenario where the processing is necessary for 1) "*the performance of a contract to which the data subject is party*", 2) "*compliance with a legal obligation*", 3) protecting the "*vital interests*" of a natural person 4) "*the performance of a task carried out in the public interest*" or 5) "*the purposes of the legitimate interests pursued by the controller or by a third party*".[291] The scenarios under 2) and 4) must moreover be provided by law.[292] The requirements under which it is accepted that data subjects have consented to the processing are strict and the onus is on the controller to prove that there is indeed 'consent'.[293,294] In addition, there are separate requirements for children's consent in relation to information society services.[295] Austria strongly criticised the wording of the fifth scenario. The general rule under the GDPR that processing is lawful if the processing is necessary for legitimate interests of the controllers, was considered unacceptable by Austria.[296] Admittedly, the GDPR provides that the general rule only applies "*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject*".[297] Nonetheless, in Austria's view, this means that the burden of proof is placed on the data subject, whereas it should be the other way around.[298]

88. The Charter provides that personal data must be "*processed* […] *on the basis of the consent of the person concerned or some other legitimate basis laid down by law*".[299] The requirement of 'lawfulness' as defined in the GDPR hence partially corresponds to and specifies this first sentence of article 8(2) of the Charter. Additionally, the requirement 'laid down by law' must be interpreted in accordance with the case law of the CJEU (e.g. the case law analysed *supra* 59-60

---

24 November 2011, *ASNEF*, C-468/10 and C-469/10, ECLI:EU:C:2011:777, para 26, Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, para 41; Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:336, para 25; Judgment of 16 January 2019, *Deutsche Post*, C-496/17, ECLI:EU:C:2019:26, para 57.
[291] Article 6(1) GDPR.
[292] *Ibid*., article 6(3).
[293] *Ibid*., article 7; KRZYSZTOFEK, *Post-reform Personal Data Protection*, 8-9.
[294] See also e.g. DIENST, Chapter C, 90-96, in which all the requirements are exhaustively listed.
[295] Article 8 GDPR.
[296] Voting result 2012/0011 (COD) of 8 April 2016 concerning the adoption of the Council's position at first reading and the statement of the Council's reasons concerning the GDPR, ST 7920 2016 INIT, 2012/011 (OLP), 7920/16 of 14 April 2016, 5-6 (hereinafter: 'Voting result Council GDPR').
[297] Article 6(1)(f) GDPR.
[298] Voting result Council GDPR, 5-6.
[299] Article 8 Charter.

can be relevant for interpreting this requirement).[300] It can therefore be concluded that this requirement does not really add protection to data subjects, but rather specifies the protection already provided for by article 8 of the Charter.

89. In addition, the processing of sensitive data (see also *supra* 73 and *infra* 131) is, in principle, prohibited,[301] and hence unlawful. Sensitive data in this context is any personal data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership* […;] *genetic data and biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*".[302] Certain exceptions apply,[303] such as explicit consent of the data subject and processing of personal data "*which are manifestly made public by the data subject*".[304] The GDPR here partially executes, in a very strict way, the protection offered by article 21 of the Charter. However, the GDPR does not prohibit the processing of personal data revealing sex, social origin, language, property, birth, or age (all grounds for discrimination which are prohibited under the Charter; note that the Parliament did want to include 'gender identity' as a sensitive category of data but this did not end up in the final version)[305]. Processing of personal data revealing colour, membership of a national minority or disability is likewise not explicitly prohibited by the GDPR, but these concepts could possibly be placed under 'racial origin', 'ethnic origin' and 'data concerning health'. The Czech Republic argued that the category of sensitive data is casuistic and should have been replaced by a more general risk-based approach,[306] without using an exhaustive list of categories of sensitive data. Such an approach could indeed protect data subjects in a more general way. However, it would also create more legal uncertainty as the current approach is clearer about what is allowed and what is not.

[300] Recital 41 GDPR.
[301] *Ibid*., article 9(1).
[302] *Ibid*., article 9(1).
[303] *Ibid*., article 9(2) and (3); see also article 91 concerning processing by churches and religious associations.
[304] *Ibid*., article 9(2)(a) and (e).
[305] European Parliament legislative resolution P7_TA(2014)0212 of 12 March 2014 on the proposal for the GDPR and the position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of the GDPR, *OJ* C378/399 of 9 November 2017, amendment 103 (hereinafter: 'Legislative resolution of the Parliament GDPR').
[306] Voting result Council GDPR, 3.

90. Finally, special protection is offered by the GDPR to personal data relating to criminal convictions and offences. Firstly, "*any comprehensive register of criminal convictions shall be kept only under the control of official authority*".[307] Secondly, any processing of such personal data can only be carried out under the control of an official authority or on the basis of an explicit legal basis "*providing for appropriate safeguards for the rights and freedoms of data subjects*".[308]

§2 Fairness

91. The second principle established by article 5 GDPR is the principle that personal data must be processed fairly.[309] Again, this reflects the first sentence of article 8(2) of the Charter, which states that personal data "*must be processed fairly*".[310] The concept of 'fair' processing or 'fairness' is however not defined in the GDPR.[311] The recitals of the GDPR corresponding to the provision containing the principle of fairness also do not clarify this concept further but even seem to blend it with the principle of lawfulness and transparency.[312,313,314] The non-English language versions of the GDPR are equally vague, e.g. using the French word 'loyale' (loyal), the German 'nach Treu und Glauben' (in good faith), the Dutch 'behoorlijk' (properly), the Italian 'corretto' (correct), the Spanish 'leal' (loyal) and the Danish 'rimeligt' (reasonable).[315] The use of terms that all have slightly different meanings and connotations, plus the absence of a definition of the concept, has a result that the concept 'fairness' is a bit like a black box, meaning that the interpretation of this concept by the courts (such as the CJEU) is highly unpredictable. It is therefore argued that the concept 'fairness', for now at least, does not really add an extra layer of protection, but remains little more than a vague idea.[316]

---

[307] Article 10 GDPR.
[308] *Ibid*.
[309] *Ibid*., article 5(1)(a).
[310] Article 8 Charter. This requirement was also already provided for in Directive 95/46, see recitals 28 and 38 and article 6(1)(a) Directive 95/46.
[311] Nor was it in Directive 95/46 before.
[312] Recitals 39, 45, 60, 71 (second paragraph) GDPR. See also recital 38 Directive 95/46.
[313] See also articles 13(2), 14(2) and 40(2)(a) GDPR where the principles of 'fairness' and 'transparency' are also explained together without distinction between the two.
[314] The CJEU too seems to blend the two principles, see Judgment of 1 October 2015, *Bara and Others*, C-201/14, ECLI:EU:C:2015:638, para 34; Judgment of 16 January 2019, *Deutsche Post*, C-496/17, ECLI:EU:C:2019:26, para 59.
[315] Article 5(1)(a) GDPR.
[316] DIENST, Chapter C, 52.

§3 Transparency

92. As in the case of the two preceding principles, article 5 GDPR states in general terms that personal data must be processed 'in a transparent manner', without further explaining this in the article itself.[317] Unlike the principle of 'fairness' however, the articles and recitals of the GDPR quite extensively explain what we need to understand about 'transparency'.[318] Data subjects should e.g. know the existence, and the extent, of the processing of their personal data, the identity and contact details of the data controller and the purpose of the processing.[319] Data subjects should also be informed "*whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data*",[320] be informed of "*the existence of profiling and the consequences of such profiling*"[321] and "*be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing*".[322] Any information relating to the processing should be free of charge, "*concise*, *easily accessible and easy to understand*", and use "*clear and plain language*, *and, additionally, where appropriate, visualisation*".[323] The data subject should also be made aware of the existence of her or his rights under the GDPR.[324]

93. It is apparent from the preceding paragraph that transparency may refer to information that should be given to the data subject before the processing starts, the information that should be accessible to data subjects during the processing and to information that should be given to data subjects following a request of access to their own data.[325] In other words, transparency is required during the whole process.

---

[317] Article 5(1)(a) GDPR.
[318] *Ibid*., recitals 39, 58, 60, 71 and 78 and articles 12, 13 and 14.
[319] *Ibid*., recitals 39 and 60 and articles 13(1)(a) and (c) and 14(1)(a) and (c).
[320] *Ibid*., recital 60 and article 13(2)(e).
[321] *Ibid*., recital 60 and articles 13(2)(f) and 14(2)(g).
[322] *Ibid*., recital 39.
[323] *Ibid*., recitals 39 and 58 and article 12(1) and (5).
[324] *Ibid*., articles 13(2)(b) and 14(2)(c).
[325] C. GIAKOUMOPOULOS, G. BUTTARELLI and M. O'FLAHERTY, *Handbook on European data protection law*, European Union Agency for Fundamental Rights and Council of Europe, Luxembourg, 2018, 120 (hereinafter: 'GIAKOUMOPOULOS and others, *Handbook on European data protection law*').

94. The appearance of the transparency principle in the GDPR is new. Whereas Directive 95/46 did require a certain degree of transparency through information requirements,[326] it did not expressly articulate transparency as a general principle like the GDPR does. Furthermore, the list of information to be disclosed to the data subjects is considerably longer in the GDPR than in Directive 95/46.[327] Additionally, the Charter also does not really contain a right to transparency (even though the CJEU did, more or less, create a right to transparency, see *supra* 71). It can therefore be concluded that the GDPR truly raises the protection given under EU law regarding this aspect.

§4 Purpose limitation

95. Article 5 GDPR states that "*personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".[328] The principle of purpose limitation thus essentially means that any processing of personal data must be done for a specific, well-defined purpose and only for additional, specified, purposes that are compatible with the original one.[329] The terms 'specified', 'explicit' and 'legitimate' are not further defined in the GDPR, nor are they explained by the CJEU.[330] However, read together with the transparency principle, it can be argued that 'specified' must be strictly interpreted, meaning that purposes such as 'improving users' experience' are not specified (enough) in the sense of article 5 GDPR.[331] 'Explicit' can be interpreted as meaning that there should be no doubt or difficulty in understanding the purpose.[332] Regarding the requirement that the purpose is 'legitimate', it is argued that the fact that the processing is 'lawful' does not *ipso facto* mean that the processing is legitimate and thus constitutes a separate requirement. In order to be legitimate, the purpose must be in accordance with the law in the broadest sense (not only data

[326] Articles 10, 11 Directive 95/46. The CJEU applied these articles to enhance transparency e.g. in Judgment of 1 October 2015, *Bara and Others*, C-201/14, ECLI:EU:C:2015:638.
[327] Compare articles 10 and 11 of Directive 95/46 with articles 13 and 14 GDPR.
[328] Article 5(1)(b) GDPR; article 6(1)(b) Directive 95/46. The wording in the GDPR is almost exactly the same as the one used in Directive 95/46 before.
[329] GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 122.
[330] The CJEU merely quotes the wording of the principle in Directive 95/46, see e.g. Judgment of 30 May 2013, *Worten*, C-342/12, ECLI:EU:C:2013:355, para 34; Judgment of 16 January 2019, *Deutsche Post*, C-496/17, ECLI:EU:C:2019:26, para 58.
[331] Article 29 Working Party, Opinion 03/2013 of 2 April 2013 on purpose limitation, 00569/13/EN WP 203, 16; DIENST, Chapter C, 55.
[332] DIENST, Chapter C, 56.

protection law).[333] The purpose must also be defined before the processing started and there cannot be further processing in a way that is incompatible with the original purpose (safe for some exceptions, e.g. statistical purposes).[334] When the controller or processor wants to start processing for a new purpose, which is not compatible with the original purpose, this can only be justified on a new legal basis (*i.e.* a scenario as discussed in 87). The GDPR also explains in greater detail when a purpose is not compatible with the original purpose.[335] Note that this explanation is included in the article concerning the 'lawfulness' of processing, which indicates that both principles are in any way closely connected.

96. Like the principles of 'lawfulness' and 'fairness', the 'purpose limitation' principle is to be found in an embryonic form in the first sentence of article 8(2) of Charter, which states that personal data "*must be processed for specified purposes*".[336] The GDPR therefore again specifies the protection already given by the Charter, rather than really creating a new requirement. The GDPR is an improvement compared to Directive 95/46 in so far it has clarified some aspects of the principle.

§5 Data minimisation

97. The principle of data minimisation implies that "*personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".[337] This principle was already included in Directive 95/46, albeit in a slightly different wording, using the words 'not excessive' instead of 'necessary'.[338] It has persuasively been argued this new wording makes the principle more strict, offering a higher protection than under Directive 95/46. The principle is not included in article 8 of the Charter but it can be derived from article 52(1) of the Charter and the case law of the CJEU (see e.g. *supra* 25, 31, 42-43, 63-70).

[333] *Ibid*., 57.
[334] GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 122.
[335] See article 6(4) GDPR. This stands in contrast to Directive 95/46.
[336] Article 8 Charter.
[337] Article 5(1)(c) GDPR.
[338] Article 6(1)(c) Directive 95/46.

98. Data minimisation not only implies that as little as possible personal data should be retained and processed, but also means that the retained personal data should, as much as possible, be pseudonymised, and even anonymised.[339] In other words, if possible, measures should be taken to reduce the ability to attribute data to a data subject.[340]

§6 Accuracy

99. The principle of accuracy requires that the personal data which ought to be processed are accurate and, where necessary, kept up to date.[341] "*Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*".[342] This principle executes the second part of the second sentence of article 8(2) of the Charter. In Directive 95/46, broadly the same provision could be found.[343,344] Two changes are notably. On the one hand, the words 'or incomplete' after 'inaccurate' got deleted in the GDPR, on the other hand, the words 'without delay' were added.

100. The term 'accuracy' should be interpreted broadly, meaning that the extent and cause of the inaccuracy are irrelevant in assessing whether the data are accurate.[345] Whether personal data is accurate or not is to be viewed as a matter of fact.[346] Personal data are inaccurate if they do not correspond with reality, value judgments can, in principle, not be 'inaccurate'.[347] It is argued that, regardless of the deletion of the words 'or incomplete' in the GDPR, incomplete data can still be classified as 'inaccurate' and therefore as contravening the GDPR.[348] The same is true for data which is embedded in a wrong context.[349] However, the concept 'inaccuracy' is not limitless, accuracy must be evaluated "*having regard to the purposes for which they are processed*". This was explained in the judgment *Peter Nowak*, where the CJEU ruled that incorrect (and hence, in a

[339] For the definitions of pseudonymisation and anonymisation, see recital 26, *in fine* and article 4(5) GDPR.
[340] GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 126.
[341] Article 5(1)(d) GDPR.
[342] *Ibid.*
[343] Article 6(1)(d) Directive 95/46.
[344] For an example of an application of this principle by the CJEU, see e.g. Judgment of 16 December 2008, *Huber*, C-524/06, ECLI:EU:C:2008:724, para 60.
[345] DIENST, Chapter C, 68.
[346] *Ibid.*
[347] *Ibid.*
[348] *Ibid.*
[349] *Ibid.*

sense, 'inaccurate') answers on an examination did not represent 'inaccuracy' within the meaning of Directive 95/46.[350]

101. As said, the GDPR states data needs to be kept up to date, *where necessary*. It is not clear (yet) whether this constitutes a requirement to periodically review all processed data,[351] or only requires updating on demand of the data subject.[352] The principle of accuracy as defined in the GDPR also lays the basis for the rights to rectification, erasure and, implicitly, access, which are analysed below (*infra* 109-118).

§7 Storage limitation

102. "*Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*".[353] This is how the principle of storage limitation is defined by the GDPR. Substantially, this definition is the same as the one in Directive 95/46.[354] The GDPR is more precise regarding the exceptions (*i.a.* personal data processed for historical research purposes) applying to this principle though.[355] The principle of storage limitation can be construed as the temporal aspect of the data minimisation principle.[356] Consequently, similar to the relation between the data minimisation principle and the Charter (*supra* 97), the storage limitation principle is not included in article 8 of the Charter but can be derived from article 52(1) of the Charter and the case law of the CJEU.

103. The principle of storage limitation has as a consequence that personal data must be deleted (or anonymised) as soon as they are no longer needed for the purposes for which they were collected.[357,358] The recitals of the GDPR establish that "*in order to ensure that the personal data*

[350] Judgment of 20 December 2017, *Peter Nowak*, C-434/16, ECLI:EU:C:2017:994, para 53.
[351] Recital 39, *in fine* GDPR points in this direction since it establishes time limits in the context of the storage limitation principle (see *infra* 103).
[352] DIENST, Chapter C, 68; see also GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 127, where it is stated that "data *may* need to be checked regularly and kept up to data to secure accuracy".
[353] Article 5(1)(e) GDPR.
[354] Article 6(1)(e) Directive 95/46.
[355] Article 5(1)(e) GDPR.
[356] DIENST, Chapter C, 70.
[357] GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 129.

are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review".[359] In the original proposal of the Commission, this requirement of a periodic review was also included in the principle itself, be it limited to processing for purposes for which exceptions apply.[360] The storage limitation principle also specifies what was already said about the data minimisation principle *supra* 98: personal data should, not only as much as possible, but also as soon as possible, be pseudonymised, and even anonymised.[361]

§8 Data security ('integrity and confidentiality')

104. The last principle regarding the way personal data should be processed is the principle of integrity and confidentiality (or, hereinafter, the data security principle). Personal data should be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*".[362] The appropriateness of the security measures must be reviewed regularly and be determined on a case-by-case basis, considering *i.a.* the costs of implementation and the possible repercussions of a security breach for the rights and freedoms of natural persons.[363] Data protection must be ensured both 'by design', *i.e.* data security must already be implemented at the stage of designing systems, and 'by default', *i.e.* systems must be constructed in a way that the default option offers a high level of data protection.[364] This principle was not included as an overarching principle in Directive 95/46 but already manifested itself in a number of articles and recitals.[365] The data security principle is also not *verbatim* included in the Charter, but it is self-evident that article 8(1) of the Charter protects data subjects against e.g. unauthorised access of their personal data when this data is processed.

---

[358] For an example of an application of this principle by the CJEU, see e.g. Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197.
[359] Recital 39, *in fine* GDPR.
[360] Proposal (Commission) for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11 final of 25 January 2012.
[361] DIENST, Chapter C, 71.
[362] Article 5(1)(f) GDPR; see also articles 24, 25, 28 and 32 GDPR which specify the technical and organisational measures.
[363] *Ibid*., article 32(1); GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 131.
[364] Article 25 GDPR, see also KRZYSZTOFEK, *Post-reform Personal Data Protection*, 7-8.
[365] Recitals 25 and 46 and articles 16 and 17 Directive 95/46.

105. Closely connected with the data security principle are article 33 and 34 GDPR. Together, one could argue these articles constitute a 'right to know when one's data has been hacked'.[366] Article 33 GDPR states that data controllers must, in principle, notify personal data breaches to the supervisory authorities "*without undue delay and, where feasible, not later than 72 hours after having become aware of it*".[367] It describes in detail the minimum information that should be included in this notification.[368] Article 34 GDPR creates an obligation, subject to some exceptions, for data controllers to communicate personal data breaches to the data subjects when that personal data breach "*is likely to result in a high risk to the rights and freedoms of natural persons*".[369] The supervisory authorities are furthermore entitled to require the data controllers to communicate a personal data breach.[370] These requirements are new, demanding obligations which did not exist under Directive 95/46.[371]

§9 Accountability

106. The last principle is the principle of accountability. This is not a substantive principle but is designed to make the other, above-mentioned, principles more effective.[372] It states that "*the controller shall be responsible for, and be able to demonstrate compliance with* [the other principles]".[373] The principle requires controllers to actively implement the preceding principles in their processing activities.[374] The most innovating aspect of this principle in the GDPR in comparison with Directive 95/46 is however that controllers are now also responsible for demonstrating compliance with data protection law.[375] They must be able to demonstrate compliance at any time, to the data subjects, the general public and supervisory authorities.[376] The

[366] Communication from the Commission to the European Parliament pursuant to Article 294(6) of the Treaty on the Functioning of the European Union concerning the position of the Council on the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and repealing Directive 95/46/EC, COM(2016) 214 final, 2012/0011(COD) of 11 April 2016.
[367] Article 33(1) GDPR.
[368] *Ibid*., article 33(3).
[369] *Ibid*., article 34(1) and (3).
[370] *Ibid*., article 34(4).
[371] KRZYSZTOFEK, *Post-reform Personal Data Protection*, 6-7.
[372] DIENST, Chapter C, 73.
[373] Article 5(2) GDPR.
[374] *Ibid*., article 24(1).
[375] Article 24(1) *in fine* GDPR.
[376] GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 134.

principle of accountability thus requires controllers to actively demonstrate compliance and not merely wait for data subjects or supervisory authorities to point out shortcomings.[377] Recital 82, reinforced by article 30, further specifies that "*in order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility*".[378] It can be concluded that on the basis of this principle, the controller can be deemed to violate the GDPR when it cannot prove it complies with the GDPR, even though it does not actually breach a requirement of the GDPR.[379]

107. The principle of accountability is thus extended when compared with Directive 95/46, has no direct basis in the Charter and therefore truly raises the level of data protection in the EU.

[377] *Ibid*., 137.
[378] Recital 82 and article 30 GDPR.
[379] DIENST, Chapter C, 74.

Subsection 2: Rights of the data subject

108. In this subsection, the rights of the data subject under the GDPR will be analysed. The CJEU has explained that the principles discussed above (*supra* 86-107) are reflected in the rights conferred on individuals, the data subjects.[380] These rights are therefore more detailed than the key principles. Only the substantive rights will be analysed under this subsection, procedural rights will be examined under subsection 4 (*infra* 158-161).

§1 The right of access

109. The GDPR grants data subjects the right (1) to obtain confirmation "*as to whether or not personal data concerning him or her are being processed*" and (2) to obtain access to the respective data and additional information regarding the data processing.[381] The scope of the right of access is significantly larger under the GDPR[382] than under Directive 95/46[383], notably the requirement to grant access to the information mentioned in article 15(l)(d)-(h) GDPR was non-existent in Directive 95/46.[384] Data subject are e.g. entitled to access the categories of personal data that are processed. It is not sufficient however for the data controller to just mention the different categories of personal data, the content of the data must also be presented.[385] Therefore, it is not enough for a data controller to inform the data subject that it processes his or her address,

---

[380] Judgment of 20 December 2017, *Peter Nowak*, C-434/16, ECLI:EU:C:2017:994, para 48.
[381] Article 15(1) GDPR.
[382] Article 15(1) GDPR provides that the data subjects have a right of access concerning the following information:
"(*a) the purposes of the processing;*
(b) the categories of personal data concerned;
(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;
(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;
(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;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;
(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."
[383] Article 12(a) Directive 95/46.
[384] KRZYSZTOFEK, *Post-reform Personal Data Protection*, 113-114.
[385] *Ibid*., 114.

the controller must also provide the address which it in fact processes.[386] Data subjects ought to be able to exercise their right of access easily and at reasonable intervals.[387] The CJEU has ruled in its case law about Directive 95/46 that the right of access to personal data may not be unduly restricted by time limits and that data subjects must have a reasonable opportunity to access information about data processing operations that took place in the past.[388]

110. The GDPR provides that controllers must provide a copy of the processed personal data, (at least initially) free of charge.[389] That copy must be provided in an intelligible form, meaning that technical terms, coded language or acronyms will probably not be sufficient, unless these terms are clearly explained.[390] Controllers should also, where possible, "*provide remote access to a secure system which would provide the data subject with direct access to his or her personal data*".[391]

111. The right of access is a most fundamental right since it facilitates the other rights of the data subject. Indeed, without it, the right to rectification and erasure, amongst others, would become meaningless, as data subjects that do not know which personal data a controller processes, cannot demand the rectification or erasure of that data either.

112. As explained above, the right of access is a requirement stemming from primary law (*supra* 10). The CJEU also used in several cases the primary law provision which contains this right of access (*supra* 71 and 79). The right of access hence exists even without the GDPR. The GDPR nevertheless offers a higher level of protection than the Charter, since it is far more detailed by e.g. listing all information to which the right of access applies.

[386] *Ibid*., 114.
[387] Recital 63 GDPR.
[388] Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paras 66, 70; GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 218.
[389] Articles 12(5) and 15(3) GDPR.
[390] GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 218.
[391] Recital 63 GDPR.

§2 The right to rectification

113. Under the GDPR, data subjects have "*the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her*".[392] Moreover, data subjects also "*have the right to have incomplete personal data completed, including by means of providing a supplementary statement*".[393] The burden of proof of the inaccuracy or incompleteness of the data lies with the data subject.[394] The controller may nevertheless not preclude data subjects from exercising their right to rectification by demanding unreasonable proof of the alleged inaccuracy.[395] Data subjects should be able to exercise this right free of charge.[396] Whereas it is reasonably clear what constitutes 'inaccuracy' (see *supra* 100), it is less apparent what 'incompleteness' exactly entails.[397]

114. In various situations, the right to rectification is important to the data subject. For example, if the database of Amazon includes a wrong address of a data subject, Amazon would send ordered goods to that wrong address. It is then important for the data subject that its personal data will be rectified upon request. In that context, controllers must, after rectifying personal data, also communicate these rectifications to each recipient to whom the personal data have been disclosed (unless this proves impossible or involves disproportionate effort).[398] That way, it is ensured that inaccurate data are rectified throughout the whole 'data chain'.

115. The right to rectification already existed under Directive 95/46,[399] but is now more clearly distinguished from the right of access, the right to erasure and the right to restriction of processing, and is also better worded.[400] Like the right of access, the right to rectification also directly emanates from the Charter (*supra* 10). The added value of the GDPR hence mostly lies with the phrase "*without undue delay*" and the clarification that incomplete data also need to be 'rectified'.

---

[392] Article 16 GDPR.
[393] *Ibid*.
[394] J. SCHREY, "General conditions for data processing in companies under the GDPR, IV." in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 138 (hereinafter: 'SCHREY, Chapter D, IV.').
[395] GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 218.
[396] Recital 59 GDPR.
[397] SCHREY, Chapter D, IV., 139.
[398] *Ibid*., article 19.
[399] Article 12(b) Directive 95/46.
[400] KRZYSZTOFEK, *Post-reform Personal Data Protection*, 116-117.

§3 The right to erasure

116. According to article 17(1) GDPR, data subjects have "*the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay*".[401] However, this right only exists in one of the following cases: (1) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (2) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing; (3) the data subject objects to the processing (see *infra* 125-128); (4) the personal data have been unlawfully processed; (5) there is a legal obligation to erase the data; (6) a special situation concerning children and information society services.[402] The erasure of data here means the actual destruction of the data carriers as well as the complete anonymisation of the data.[403] The right to erasure is not absolute but, by contrast, subject to exceptions,[404] e.g. it shall not apply when processing is necessary for exercising the right of freedom of expression and information or for defence of legal claims.[405] Data subjects should be able to exercise this right free of charge.[406]

117. Besides the term 'right to erasure', the term 'right to be forgotten' is also used. This is true even in the GDPR itself, where the latter is put next to the former in the title of the relevant article, albeit between brackets and quotation marks. The academic discussion[407] about whether these two rights are one and the same thing or not (see also *supra* 80) will not be dwelled upon here. Nevertheless, from a practical point of view, it is convenient (as some authors do)[408] to use the term 'right to be forgotten' for the right contained in article 17(2) GDPR. According to that provision, controllers must, in principle, where they have made personal data public, and where they must erase that data pursuant to article 17(1), "*inform other controllers that the data subject*

[401] Article 17(1) GDPR.
[402] *Ibid*., see also recital 65 concerning the sixth situation.
[403] KRZYSZTOFEK, *Post-reform Personal Data Protection*, 121.
[404] Article 17(3) GDPR.
[405] *Ibid*., article 17(3)(a) and (e). For an example in the case law of the CJEU where the CJEU rejected a request to erase personal data, see Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197.
[406] Recital 59 GDPR.
[407] See further J. AUSLOOS, *The Right to Erasure: Safeguard for Informational Self-Determination in a Digital Society?*, Dissertation for the degree of Doctor of Laws (PhD) KU Leuven, 2018, 91-92; KRZYSZTOFEK, *Post-reform Personal Data Protection*, 119-120.
[408] SCHREY, Chapter D, IV., 141.

has requested the erasure of any links to, or copy or replication of, those personal data".[409] This is essentially the codification of the case law of the CJEU in *Google Spain*[410] (*supra* 80-81). Besides this requirement, article 19 GDPR is applicable, meaning that what has been said *supra* 114 can *mutatis mutandis* be repeated.

118. Although the right to erasure is not explicitly provided for by the Charter, the CJEU has nonetheless interpreted the Charter as implicitly containing this right (*supra* 80).[411] The GDPR thus does not 'create' a new right but merely specifies the specific conditions of a right already contained in the Charter.[412] In this regard, the comments *supra* 115 about the right to rectification can be repeated concerning the right to erasure. The right to erasure is, under the current legislative framework, more clearly delineated from the right of access, the right to rectification and the right to restriction of processing. The right to erasure itself is now also considerably more elaborated. Indeed, whereas Directive 95/46 only stated that Member States 'shall guarantee' data subjects a right to erasure, the GDPR gives a quite detailed description of this right.

§4 The right to restriction of processing

119. The GDPR grants data subjects the right to obtain restriction of processing in certain situations.[413] This right to restriction of processing can be depicted as a 'freeze',[414] or a suspension[415] of the processing, subject to certain exceptions[416]. Methods to 'restrict' the processing include, *i.a.*, temporarily moving the selected data to another processing system or

[409] Article 17(2) GDPR, see also recital 66 GDPR. Note that the Parliament wanted to codify the Google Spain case law even stronger, by writing into the GDPR that "*data subjects shall have the right* […] *to obtain from third parties the erasure of any links to, or copy or replication of, those data*". See Legislative resolution of the Parliament GDPR, amendment 112.
[410] Judgment *Google Spain*.
[411] See in this regard also the Judgment of the General Court of 3 December 2015, *CN v Parliament*, T-343/13, ECLI:EU:T:2015:926. In this judgment, the General Court at least implicitly accepted that a more restricted right to erasure can be deemed compatible with article 8(1) of the Charter, see especially para 48.
[412] The right to erasure also already existed under Directive 95/46, article 12(b) Directive 95/46.
[413] Article 18(1) GDPR.
[414] Autorité de protection des données – Gegevensbeschermingsautoriteit (ADP-GBA), 'AVG/GDPR - Rechten van de burger', (Brussels, 23 November 2018) <https://www.youtube.com/watch?v=ceKry1RlQbs&feature=youtu.be> accessed 25 March 2019, 2:58-3:32.
[415] KRZYSZTOFEK, *Post-reform Personal Data Protection*, 132.
[416] Article 18(2) GDPR.

temporarily removing published data from a website.[417] The data of which the processing is restricted should be clearly marked.[418] The right to restriction exists when (1) the data subject contests the accuracy of the personal data; (2) "*the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead*"; (3) the data subject needs the personal data for exercise or defence of legal claims; (4) the data subject objects to the processing (see *infra* 125-128).[419] In the first situation, the processing is only restricted for a limited period, to enable the controller to verify the accuracy of the personal data concerned.[420] In each situation, the data subject bears the burden of proof that restriction is required.[421] Article 19 GDPR is applicable to this right too, meaning that what has been said *supra* 114 can again be repeated.

120. The term 'restriction of processing' is a new feature of the GDPR. However, the concept itself is not entirely new. Under Directive 95/46, an equivalent right existed:[422] the right to 'blocking of data'.[423] What has been said about the wording and delineation *supra* 115 and 118, respectively about the right to rectification and the right to erasure, can *mutatis mutandis* be repeated.

121. The Charter does not contain any provision relating to this right. It is conceivable however that the CJEU would, even without the existence of the GDPR, accept that the right to restriction of processing is implicitly included in article 8 of the Charter. This is based on the reasoning that the right to restriction of processing makes sure that other rights, such as the right to erasure, are enforceable in practice. Indeed, one could argue that the right to erasure is not that efficient when the erasure only occurs after a long period, due to lengthy disputes about the erasure. Nonetheless, the GDPR truly provides a higher level of protection than the Charter on this issue, by providing more detailed rules.

[417] *Ibid*., recital 67.
[418] *Ibid*., recital 67 and article 4(3).
[419] *Ibid*., article 18(1).
[420] *Ibid*., article 18(1)(a).
[421] SCHREY, Chapter D, IV., 143.
[422] Article 12(b) Directive 95/46.
[423] KRZYSZTOFEK, *Post-reform Personal Data Protection*, 132.

§5 The right to data portability

122. A completely new right in the GDPR, is the right to data portability.[424] Article 20(1) GDPR states that data subjects have the right, subject to exceptions, "*to receive the personal data concerning him or her, which he or she has provided to a controlle*r", from that controller "*in a structured, commonly used and machine-readable format*" and "*have the right to transmit these data to another controller without hindrance*".[425] This right only exists when the processing is carried out by automated means and is based on either consent or is necessary for the performance of a contract.[426] The requirement that the data be 'provided by the data subject', must be interpreted broadly and can include pseudonymised, but not anonymised data.[427] Only inferred or derived data ought to be excluded from the interpretation.[428] The phrase 'without hindrance' should be interpreted as meaning that the first controller may not impede the transmission to other controllers by any (legal or technical) restrictions.[429]

123. Whereas article 20(1) GDPR grants the data subject the right to receive his or her personal data and subsequently transmit this data without hindrance to another controller, article 20(2) GDPR goes even further, by granting the data subject a "*right to have the personal data transmitted directly from one controller to another*", where technically feasible.[430] This right however imposes no obligation on controllers to adopt or maintain technically compatible processing systems.[431] It is important to note that the exercise of the right to data portability by a data subject does not *ipso facto* trigger the erasure of the concerned personal data by the first data controller.[432] The right to data portability is hence to be clearly distinguished from the right to erasure.

---

[424] SCHREY, Chapter D, IV., 144; KRZYSZTOFEK, *Post-reform Personal Data Protection*, 9.
[425] Article 20(1), (3) and (4) GDPR. The Parliament wanted to remove the right to data portability from the Commission proposal, see Legislative resolution of the Parliament GDPR, amendment 113.
[426] *Ibid*., article 20(1).
[427] SCHREY, Chapter D, IV., 144-145.
[428] *Ibid*.
[429] *Ibid*., 145.
[430] Article 20(2) GDPR; SCHREY, Chapter D, IV., 144.
[431] Recital 68 GDPR.
[432] SCHREY, Chapter D, IV., 145; KRZYSZTOFEK, *Post-reform Personal Data Protection*, 135.

124. No equivalent right to the right to data portability can be found in Directive 95/46. The GDPR thus strengthens the rights of data subjects compared to Directive 95/46. The GDPR itself also states it intends to "*strengthen the data subject's control over his own data*".[433] The Charter equally does not provide any equivalent right. It is also not that easily conceivable that the CJEU would infer the right to data portability from article 8 of the Charter. One could therefore argue that the GDPR here genuinely 'creates' a right, thereby increasing the level of protection offered by the EU.

§6 The right to object

125. Article 21 GDPR establishes the right to object.[434] The right to object at first sight seems to resemble both the right to restriction of processing and the right to erasure. As AUSLOOS states, "*the key distinction between the right to object and the right to erasure is that the right to erasure focuses on data, whereas the right to object focuses on processing operations*".[435] As unlawfulness of one personal data processing operation does not necessarily imply unlawfulness of all processing operations concerning that data, applying the right to erasure to that data may seem disproportionate.[436] A successful exercise of the right to object has as a result that the controller may no longer process the data in question.[437] Processing operations performed prior to the objection, however, remain legal.[438] However, data subjects do not have a general right to object to the processing of their data.[439] There is only a right to object (1) on grounds related to the data subjects' particular situations, (2) to processing of data for direct marketing purposes and (3) to processing of data for scientific or historical research or statistical purposes.[440] The first two scenarios in which a right to object exists, will be examined *infra* 126-127. The last one, which is a novelty of the GDPR, will, considering its rather limited importance in the context of the PSD, not be examined.

---

[433] Recital 68 GDPR.
[434] *Ibid*., article 21.
[435] J. AUSLOOS, *The Right to Erasure: Safeguard for Informational Self-Determination in a Digital Society?*, Dissertation for the degree of Doctor of Laws (PhD) KU Leuven, 2018, 188.
[436] *Ibid*.
[437] GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 231.
[438] *Ibid*.
[439] *Ibid*., 229
[440] *Ibid*., 229-233.

126. The right to object on grounds relating to the data subject's particular situation tries to ensure that the correct balance is struck between the data subject's interests and the legitimate rights of others in processing their data.[441] The GDPR states that the controller must demonstrate "*compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject*", firmly laying the burden of proof on the data controllers.[442] Since the CJEU, in *Google Spain*,[443] has clarified that the rights of the data subjects override 'as a general rule' the economic interests of data controllers,[444] this will not be an easy task for the controllers. This right already existed under Directive 95/46 but under that Directive, the burden of proof rested on the data subject.[445] The GDPR hence provides greater protection for the data subject than Directive 95/46.

127. The right to object to processing for direct marketing purposes is an absolute right, it does not seek to find a 'balance'.[446] The data subject does not need to state reasons for the objection, and the data controller cannot provide ground which would allow him to 'override' the objection.[447] Moreover, data subjects can object to the processing "*at any time*".[448] It is important to reiterate that the controller can still process the data for other purposes, regardless of the objection to processing for direct marketing purposes.[449] This right already existed under Directive 95/46,[450] and it could even be argued that Directive 95/46 offered higher protection than the GDPR. Indeed, while the GDPR only states that the data subject must be able exercise this right 'free of charge' in the recitals, Directive 95/46 provided this in the article itself.[451]

128. The right to object is not explicitly included in the Charter. The GDPR thus strengthens the rights of data subject by providing this right. However, like what has been said *supra* 121 regarding the right to restriction of processing, it can be conceived that the CJEU would read the

[441] *Ibid*., 230.
[442] Article 21(1) GDPR.
[443] Judgment *Google Spain*.
[444] *Ibid*., para 81.
[445] Recital 45 and article 14(a) Directive 95/46.
[446] SCHREY, Chapter D, IV., 147.
[447] *Ibid*.
[448] Article 21(2) GDPR.
[449] This can be inferred from article 21(3) GDPR, which states that "*the personal data shall no longer be processed for such purposes*".
[450] Article 14(b) Directive 95/46.
[451] Recital 70 GDPR.

right to object in article 8 of the Charter. The additional protection of the GDPR hence mostly arises from the detailed rules of the GDPR, describing the exact conditions surrounding the right to object.

§7 The right not to be subject to automated individual decision-making

129. According to article 22(1) GDPR, data subjects "*have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*".[452] An example of a decision that 'significantly affects' a data subject is an automatic refusal of an online credit application.[453] Profiling means "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".[454] The Article 29 Working Party ('WP29') has interpreted article 22 GDPR, despite its wording, not really as a right, but as a general prohibition: data subjects should not be subjected to decisions solely based on automated processing (which produces legal effects concerning him or her or similarly significantly affects him or her).[455] This means that article 22 GDPR is applicable in any circumstances and does not require the data subject to proactively exercise this 'right'. Since the European Data Protection Board is the successor of the WP29,[456] and the Board has explicitly obtained the competence to issue guidelines concerning profiling,[457] this interpretation is still valid.

130. The prohibition of article 22(1) GDPR is subject to several exceptions listed in article 22(2) GDPR. The prohibition does not apply when Union or Member State law authorises the decision (e.g. for the purposes of tax-evasion purposes) and lays down suitable safeguards for the

[452] Article 22(1) GDPR.
[453] *Ibid*., recital 71.
[454] *Ibid*., article 4(4).
[455] Article 29 Working Party, Guidelines of 3 October 2017 on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679, 17/EN WP 251, 15.
[456] Recital 139 GDPR.
[457] *Ibid*., recital 72 and article 70(1)(f).

data subject.[458] The prohibition is equally not applicable if the data subject has explicitly consented to a decision as described in 22(1) GDPR or the decision is necessary "*for entering into, or performance of, a contract between the data subject and a data controller*".[459] In the latter two cases, the controller must provide to the data subject "*a right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*" [460] and also explain the decision.[461] In effect, this means that there is always at least a 'right to review'.[462]

131. Lastly, automated individual decision-making based on sensitive data is, in line with what has been said *supra* 89, in principle, prohibited. The exceptions under which automated individual decision-making based on sensitive data is nonetheless permitted are far more limited than the ones applicable to 'regular' processing of sensitive data. Only explicit consent of the data subject and the situation in which the "*processing is necessary for reasons of substantial public interest*" can legitimise the automated individual decision-making based on sensitive data.[463] Automated individual decision-making based on sensitive data, manifestly made public by the data subject, is hence not allowed under article 22 GDPR.

132. The right not to be subject to automated individual decision-making is not entirely new. It already existed under Directive 95/46.[464] On the one hand, under Directive 95/46, there was no exception which allowed automated individual decision-making on the basis of explicit consent of the data subject. On the other hand, there was no 'right to review' at all as under the GDPR. Neither was there a separate provision about automated individual decision-making based on sensitive data. Put together, one could argue that this 'right' is indeed strengthened by the GDPR.

133. The Charter not explicitly provides for the right under article 22 GDPR, although the provision regarding sensitive data reflects the principle of non-discrimination enshrined in article 22 of the Charter (see also *supra* 73, 89). Taken as a whole, the general prohibition on automated individual decision-making in article 22 GDPR increases the level of data protection in the EU.

---

[458] *Ibid*., recital 71 and article 22(2)(b).
[459] *Ibid*., article 22(2)(a) and (c).
[460] *Ibid*., article 22(3).
[461] *Ibid*., recital 71.
[462] SCHREY, Chapter D, IV., 151.
[463] Article 22(4) j° article 9(1)(a) and (g) GDPR.
[464] Article 15 Directive 95/46.

Subsection 3: Specific processing situations

134. The GDPR has several "*provisions relating to specific processing situations*".[465] These provisions try to reconcile fundamental rights and important public interests with the principles and rights explained above (*supra* 86-133).

135. The GDPR states that Member States must reconcile the right to the protection of personal data as developed by the GDPR with right to freedom of expression and information, including processing for journalistic purposes and purposes of academic, artistic or literary expression.[466] The GDPR hence provides for a sort of 'general escape clause' for processing which is necessary to exercise the right freedom of expression and information.[467] *De facto*, this codifies the case law of the CJEU in *Google Spain*, regarding the right to be forgotten, which states that "*a fair balance should be sought*" between the right to be forgotten (interpreted as being an aspect of the right to protection of personal data) and the right to information.[468] It also extends this case law to all rights and principles of the GDPR.

136. The GDPR also foresees that issues may arise from the tension between the right to protection of personal data and the right to access to official documents,[469] a right also recognised by the Charter (and also the TFEU).[470,471] The GDPR states that official documents held by a

[465] Articles 85-91 GDPR.
[466] *Ibid*., article 85(1).
[467] *Ibid*., article 85(2).
[468] Judgment *Google Spain*, paras 81, 97, 99.
[469] Article 86 GDPR.
[470] Article 42 Charter; article 15(3) TFEU.
[471] The case law of the CJEU concerning article 42 of the Charter, in relation to the protection of personal data, is quite scarce. When article 42 is invoked, it is mostly only mentioned and not really interpreted: see e.g. Judgment of 28 June 2012, *Commission v Éditions Odile Jacob*, C-404/10P, ECLI:EU:C:2012:393, para 84; Judgment of 18 July 2017, *Commission v Breyer*, C-213/15P, ECLI:EU:C:2017:563, para 52. When article 42 is interpreted, then it is almost never balanced against article 8 of the Charter: see e.g. Judgment of 13 March 2019, *AlzChem v Commission*, C-666/17P, ECLI:EU:C:2019:196, paras 62-67; Judgment of the General Court of 28 March 2017, *Deutsche Telekom v Commission*, T-210/15, ECLI:EU:T:2017:224, paras 110-121; Judgment of the General Court of 5 February 2018, *Edeka-Handelsgesellschaft Hessenring v Commission*, T-611/15, ECLI:EU:T:2018:63, paras 107-112; Judgment of the General Court of 27 February 2018, *CEE Bankwatch Network v Commission*, T-307/16, ECLI:EU:T:2018:97, paras 139-143. The case law of the CJEU concerning the balance between articles 8 and 42 of the Charter is even scarcer. The only case in which there was a real balancing by the CJEU between data protection on the one hand, and the right to access to official documents on the other hand, and in which article 42 of the Charter was invoked, is the Judgment of the Court of First Instance of 8 November 2007, *Bavarian Lager v Commission*, T-194/04, ECLI:EU:T:2007:334. In this case, the Court of First Instance decided that the right to access to official documents

authority containing personal data, "*may be disclosed by the authority in accordance with Union or Member State law to which the public authority* […] *is subject*".[472] Hence, the GDPR does not really offers detailed rules about how to solve clashes between the two rights. Instead, it leaves the EU institutions and the member states the opportunity to create such detailed rules.

137. Specific rules are also provided for processing in the context of employment[473] and for the processing of 'national identification numbers', which may be processed under appropriate safeguards for the rights and freedoms of the data subject flowing from the GDPR, determined by the Member states.[474] Processing in the context of employment should "*include suitable and specific measures*" laid down by the member states, "*to safeguard the data subject's human dignity, legitimate interests and fundamental rights*".[475] Lastly, certain derogations from data subjects' rights are allowed for processing "*for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*".[476]

---

prevailed, in the circumstances of the case, over the right to the protection of personal data. This judgment was later set aside on appeal, albeit without invoking article 42 of the Charter, rather relying on Directive 95/46, see Judgment of 29 June 2010, *Commission v Bavarian Lager*, C-28/08P, ECLI:EU:C:2010:378.

[472] Article 86 GDPR.

[473] *Ibid*., article 88.

[474] *Ibid*., article 87.

[475] *Ibid*., article 88.

[476] *Ibid*., article 89.

Subsection 4: Oversight, control mechanisms and enforcement

138. The GDPR provides for several accountability schemes which all seek to improve compliance with the GDPR. This includes to some extent self-controlling mechanisms such as data protection impact assessments ('DPIA's')[477] and the installation of Data Protection Officers ('DPO's') inside the organisational structure of data controllers and processors,[478] but also more traditional oversight by a supervisory body[479] and the accompanying enforcement by fines[480]. This subsection will discuss all these elements. Of the requirements examined under this subsection, only the requirement of the existence of a supervisory body can be inferred from the Charter. Therefore, there will only be a comparison of that requirement with the Charter.

§1 Data protection impact assessments and prior consultation

139. DPIA's are instruments designed to identify, address and mitigate the risks following from a certain processing of personal data, essentially with the goal to enable the data controller (or processor) to limit the likelihood of a negative impact on individuals as a result of that processing.[481] DPIA's contain e.g. "*a systematic description of the envisaged processing operations and the purposes of the processing*" and "*an assessment of the necessity and proportionality*".[482] They are only required when the processing operation "*is likely to result in a high risk to the rights and freedoms of natural person*".[483] Some processing operations are explicitly considered to result in such a high risk, e.g. the processing on a large scale of sensitive data.[484]

[477] *Ibid*., article 35.
[478] *Ibid*., articles 37-39.
[479] *Ibid*., articles 51-59.
[480] *Ibid*., articles 77-83.
[481] GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 179.
[482] Article 35(7)(a) and (b) GDPR.
[483] *Ibid*., article 35(1).
[484] *Ibid*., article 35(3)(c).

140. Where a DPIA indicates "*that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk*", the controller shall consult the supervisory authority (about this authority, *infra* 146-157) prior to that processing (this is the so-called 'prior consultation').[485] Where the authority considers that the intended processing would infringe the GDPR, e.g. because the controller has insufficiently mitigated the risk, the authority can take measures such as banning the processing.[486]

141. The DPIA is a new instrument under the GDPR, it did not occur in Directive 95/46.[487] The GDPR thus adds another layer of data protection by creating this instrument on the European level.

§2 Data protection officers

142. DPO's are persons who inform and advise on compliance with data protection rules.[488] Moreover, they act as an internal or external control mechanism since they also monitor this compliance.[489] In addition, they act as intermediaries between the supervisory authorities, data subjects and the data controllers or processors by which they have been appointed.[490] In other words, they are the 'contact point' for the supervisory authorities.[491]

143. The GDPR provides for specific safeguards regarding the position of the DPO within the organisation they are appointed in. DPO's e.g. must be "*involved properly and in a timely manner, in all issues which relate to the protection of personal data*"[492], must be provided resources necessary to carry out their tasks and cannot fulfil tasks and duties which result in conflicts of interests.[493] Furthermore, DPO's must be bound by secrecy or confidentiality concerning the performance of his or her tasks.[494] Lastly, DPO's ought not to receive any instructions regarding

[485] *Ibid*., article 36(1).
[486] *Ibid*., article 36(2) j° article 58(2)(f).
[487] KRZYSZTOFEK, *Post-reform Personal Data Protection*, 7.
[488] Article 39(1)(a) GDPR; GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 175.
[489] Article 39(1)(b) GDPR.
[490] Article 39(1)(e) GDPR; GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 175.
[491] Article 39(1)(e) GDPR.
[492] *Ibid*., article 38(1).
[493] *Ibid*., article 38(2) and (6).
[494] *Ibid*., article 38(5).

the exercise of their tasks.[495] To this end, they cannot be dismissed or penalised by the controller or the processor for performing their task and they should directly report to the highest management level of the controller or the processor.[496]

144. While in general, a data controller (or processor) may, but is not required to, designate a DPO, in certain scenarios there is an obligation to do so.[497] For example, where the "*processing is carried out by a public authority or body, except for courts acting in their judicial capacity*" or where "*the core activities of the controller or the processor consist of processing on a large scale*" of sensitive data.[498]

145. Directive 95/46 already mentioned the concept of a DPO but did not contain an obligation to appoint one and left it largely to the discretion of the member states.[499] Therefore, one can conclude that the GDPR has added an extra requirement here in comparison with Directive 95/46.

§3 An independent supervisory body

146. The existence of an independent supervisory authority overseeing data protection law is already discussed as a requirement of primary law of the EU (*supra* 10, 13, 52 and 72). The existence and functioning of such a body however needs to be made operational by secondary law, *in casu* the GDPR. The GDPR provides that each member state of the EU must establish "*one or more independent public authorities to be responsible for monitoring the application of this Regulation*"[500] (a national data protection authority, hereinafter: 'DPA') and establishes the European Data Protection Board ('Board') itself.[501] The Board is composed of the head of one DPA of each Member State and of the European Data Protection Supervisor (EDPS).[502] To say it

[495] *Ibid*., article 38(3).
[496] *Ibid*., article 38(3).
[497] *Ibid*., article 37(4).
[498] *Ibid*., article 37(1)(a) and (c).
[499] Recitals 49 and 54 and articles 18(2), second indent and 20(2) Directive 95/46; SCHREY, "General conditions for data processing in companies under the GDPR, VI." in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 175.
[500] Article 51(1) GDPR.
[501] *Ibid*., article 68(1).
[502] *Ibid*., article 68(3); the EDPS is not established by the GDPR but by Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of

shortly, the GDPR creates independent supervision on two levels: on the European level by the EDPS and the Board, and on the national level by the DPA's.[503] The GDPR also enacts rules about so-called 'lead authorities' and 'cooperation and consistency mechanisms' to coordinate all the involved authorities.[504] Those mechanisms will not be discussed, since they do not really result in a higher level of protection of personal data, but rather delineate the competences of the involved authorities. Most focus will be placed on the DPA's, since the characteristics of those authorities largely mirror the characteristics of the Board and there is no need to repeat all of this.[505]

a) Independence

147. Both the Board and the DPA's ought to be completely independent.[506] This means that all members of the DPA's must "*remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody*".[507] Additionally, members cannot "*engage in any incompatible occupation, whether gainful or not*", they must, in general, "*refrain from any action incompatible with their duties*".[508] Member states on the other hand must ensure that each DPA "*is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers*" and that the DPA's are able to choose their own staff.[509] The DPA's must have separate, public annual budgets, must be subject to financial control, but this control may not affect its independence.[510] The independence of the DPA's is also reflected in the rules concerning the appointment and dismissal of its members. Members must be appointed by either the parliament, government, head of state or "*an independent body entrusted with the appointment*" of a member state and can only be

---

personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, *OJ* L295/39 of 21 November 2018 (hereinafter: 'Regulation 2018/1725').

[503] See also Judgment *Commission v Germany*, para 27.

[504] Articles 56 and 60-67 GDPR.

[505] For example, in Judgment *Commission v Germany*, para 28, the CJEU stated that the provisions concerning the EDPS and the DPA's "*should be interpreted homogeneously*".

[506] Articles 52(1) and 69(1) GDPR. However, one author persuasively argues that the involvement of the Commission in the Board undermines the independence of the Board. Since the Board can issue binding decisions to the DPA's, the same author further argues that this in turn affects the independence of the DPA's. See M. SZYDLO, "The independence of data protection authorities in EU law: between the safeguarding of fundamental rights and ensuring the integrity of the internal market", *ELR* 2017, (369) 384-386.

[507] *Ibid*., article 52(2); regarding the Board, see article 69(2).

[508] *Ibid*., article 52(3).

[509] *Ibid*., article 52(4) and (5).

[510] *Ibid*., article 52(6).

dismissed "*in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties*".[511] To summarise, the DPA's must have a seven layered independence: functional independence (no external influence), freedom from conflicts of interest, ability to independently select their own staff, organisational independence (have their own non-financial resources), financial independence (a separate budget), rules concerning appointments and lastly, all the preceding layers must be provided for by law.[512]

148. Some of the requirements set out *supra* 147 are codifications of the case law of the CJEU concerning Directive 95/46. Directive 95/46 provided that the DPA's "*shall act with complete independence*" but did not specify this any further.[513] This gave much leeway to the CJEU to interpret this requirement, which it did in three important cases: *Commission v Germany*[514], *Commission v Austria*[515] and *Commission v Hungary*[516]. In *Commission v Germany*, the CJEU interpreted 'independence' as meaning "*a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure*"[517], and the adjective 'complete' implies "*a decision-making power independent of any direct or indirect external influence*".[518] These requirements were repeated in *Commission v Austria*[519] and *Commission v Hungary*[520] and are now included in the GDPR.

149. In *Commission v Germany*, these statements led the CJEU to conclude that Germany failed to transpose Directive 95/46 correctly.[521] Germany (and its Länder) provided that its DPA's were subject to state scrutiny, meaning that the government of a Land, or an administrative body subject to that government, could check that acts of the supervisory authorities comply with the data protection law.[522] The CJEU found this to constitute 'direct or indirect influence', since these

[511] *Ibid*., article 53(1) and (4).
[512] M. SZYDLO, "The independence of data protection authorities in EU law: between the safeguarding of fundamental rights and ensuring the integrity of the internal market", *ELR* 2017, (369) 375.
[513] Article 28(1) second subparagraph Directive 95/46.
[514] Judgment *Commission v Germany*.
[515] Judgment *Commission v Austria*.
[516] Judgment *Commission v Hungary*.
[517] Judgment *Commission v Germany*, para 18.
[518] *Ibid*., para 19.
[519] Judgment *Commission v Austria*, paras 41-42.
[520] Judgment *Commission v Hungary*, paras 51-52.
[521] Judgment *Commission v Germany*, para 56.
[522] *Ibid*., para 33.

scrutinising authorities might "*not be able to act objectively when they interpret and apply*"[523] the data protection law, essentially opening the door to the "*risk that the scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities*".[524] The CJEU further stated that "*for the purposes of the role adopted by those authorities as guardians of the right to private life, it is necessary that their decisions, and therefore the authorities themselves, remain above any suspicion of partiality*",[525] thereby setting a high bar, almost resembling the adage "*not only must justice be done; it must also be seen to be done*",[526] for the independence of the DPA's.

150. In *Commission v Austria*, the CJEU found three problematic aspects which, in its view, imperilled the independence of the Austrian DPA.[527] The CJEU first examined the position of the 'managing member' of the Austrian DPA (the member responsible for the management of the day-to-day business of the DPA).[528] This member was a federal official, and therefore subject to supervision by his hierarchical superior (an official part of the 'normal' Austrian administration).[529] Even though the Austrian legislation was designed to prevent this hierarchical superior to issue instructions to the managing member,[530] the CJEU nonetheless stated that "*the hierarchical superior* [has the ability] *not only to ensure that his staff carry out their tasks in accordance with the law, efficiently and economically* [… but also to] *encourage the promotion of his staff in accordance with their performance and direct them to those tasks which correspond best to their capacities*".[531] This could lead to 'prior compliance' on the part of the managing member, since the hierarchical superior was responsible for the evaluation, and consequently the career path, of the managing member.[532] This in turn affected the independence of the Austrian

[523] *Ibid*., para 34.
[524] *Ibid*., para 36.
[525] *Ibid*., para 36.
[526] This adage originates from the case *R v Sussex Justices*, which states that "*it is not merely of some importance but is of fundamental importance that justice should not only be done, but should manifestly and undoubtedly be seen to be done*" in the context of the independence and impartiality of the judiciary. See High Court of Justice (UK) 9 November 1923, *R v Sussex Justices, ex parte McCarthy*, 1 KB 256. Indeed, there are indications that the independence of the DPA's is somewhat similar to that of the judiciary, see e.g. Opinion of Advocate General Tanchev of 11 April 2019, *Commission v Poland*, C-619/18, ECLI:EU:C:2019:325, para 81.
[527] Judgment *Commission v Austria*, para 66.
[528] *Ibid*., paras 12, 45-55.
[529] *Ibid*., paras 46, 48.
[530] *Ibid*., para 50.
[531] *Ibid*., para 49.
[532] *Ibid*., para 51.

DPA.[533] Next, the CJEU ruled that the integration of the Austrian DPA with the departments of the Federal Chancellery jeopardised its independence (the DPA was composed of officials of the Federal Chancellery), since this implies supervision by the Federal Chancellery (which is, as explained above, not acceptable to the CJEU).[534] Lastly, the CJEU ruled that the fact that the Austrian Federal Chancellor had an unconditional right to information covering all aspects of the work of the Austrian DPA is incompatible with the required independence of the DPA.[535] Notably, the CJEU did not consider the fact that the Austrian DPA did not have a separate budget, compromised the independence of the DPA.[536]

151. Lastly, in *Commission v Hungary*,[537] the CJEU ruled that Hungary compromised the independence of its DPA by prematurely bringing to an end the term served by the supervisor of that DPA.[538] Hungary had compelled the supervisor of the Hungarian DPA to vacate office in the context of an institutional reform, thereby disregarding national rules concerning the 'end of office' of that supervisor.[539] The CJEU stated that "*the threat of such premature termination to which that authority would be exposed throughout its term of office could lead it to enter into a form of prior compliance with the political authority, which is incompatible with the requirement of independence*".[540] It further considered that independence necessarily requires the DPA's "*to serve their full term of office and to have them vacate office before expiry of the full term only in accordance with the rules and safeguards established by the applicable legislation*", regardless of the fact that institutional changes were the reason for the premature termination.[541]

152. In conclusion, it can be argued that since the GDPR, in contrast to Directive 95/46, spells out a whole list of requirements concerning the independence of the supervisory authorities (*supra* 147), and since the CJEU already required high standards when interpreting Directive 95/46 (*supra* 148-151), it is likely that the CJEU will now be even more strict when assessing the independence of these authorities.

---

[533] *Ibid*., para 55.
[534] *Ibid*., para 66 j° 56 and 59.
[535] *Ibid*., paras 62, 63, 66.
[536] *Ibid*., para 58.
[537] Judgment *Commission v Hungary*.
[538] *Ibid*., para 62.
[539] *Ibid*., para 19.
[540] *Ibid*., para 54.
[541] *Ibid*., paras 55, 59.

b) Tasks and powers

153. The GDPR grants a whole array of tasks to the DPA's. The main task of the DPA's is to monitor and enforce the GDPR.[542] Other tasks the DPA's have under the GDPR are, *i.a.*, to advise their "*national parliament, government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing*" and to handle complaints lodged by data subjects, which will be, in principle, free of charge for the data subject.[543]

154. Likewise, the GDPR grants a whole array of powers to all DPA's. The GDPR stipulates that the DPA's have authorisation and advisory powers, e.g. they can issue "*on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data*"[544], but also various investigative powers, e.g. they can order data controllers "*to provide any information it requires for the performance of its tasks*" and obtain access to the premises of data controllers[545] and, maybe most importantly, corrective powers.[546] Each DPA can issue warnings to data controllers that intended processing operations are likely to infringe the GDPR and issue reprimands saying that processing operations have infringed the GDPR.[547] They can order data controllers to comply with data subject's requests to exercise their rights (*supra* 108-133), order the rectification or erasure of personal data or restriction of processing and order data controllers to communicate data breaches to the data subjects (see also *supra* 105).[548] Even more far-reaching, the DPA's also have the powers to simply ban processing or suspend data flows to recipients in third countries.[549] Lastly, the DPA's have the power to impose administrative fines (*infra* 163-164).[550] In connection to this, the DPA's have the power to bring infringements of the GDPR to the attention of the judicial authorities and

[542] Articles 57(1)(a) GDPR.
[543] *Ibid*., article 57(1)(c) and (f) and 57(3).
[544] *Ibid*., article 58(3)(b).
[545] *Ibid*., article 58(1)(a) and (f).
[546] *Ibid*., article 58(2).
[547] *Ibid*., article 58(2)(a) and (b).
[548] *Ibid*., article 58(2)(c), (e) and (g).
[549] *Ibid*., article 58(2)(f) and (j).
[550] *Ibid*., article 58(2)(i).

to initiate legal proceedings to enforce the GDPR.[551] The exercise of all mentioned powers ought to be subject to judicial review.[552]

155. Data controllers and processors have a duty to cooperate with the supervisory authorities.[553] Although this duty is not directed to the supervisory authorities, but to the data controllers and processers, it enhances the powers of those authorities. For example, the data controllers must at least tolerate access to their premises.[554]

156. Much more than under Directive 95/46, the supervisory authorities now have, under the GDPR, clearly defined and summed up tasks and powers.[555] These tasks and powers help to ensure that data controllers and processors actually comply with the GDPR, and therefore contribute to the level of protection offered to personal data throughout the EU.

c) Professional secrecy

157. Like under Directive 95/46,[556] the members and the staff of the DPA's are subject to a duty of professional secrecy both during and after their term of office, "*with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers*".[557]

[551] *Ibid*., article 58(5).
[552] *Ibid*., article 58(4).
[553] *Ibid*., article 31.
[554] J. SCHREY, "General conditions for data processing in companies under the GDPR, V." in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 164.
[555] Compare article 28(3) Directive 95/46 with article 58 GDPR.
[556] Article 28(7) Directive 95/46.
[557] Article 54(2) GDPR.

§4 Remedies, liability, compensation and sanctions

a) The right to lodge a complaint with the supervisory authorities and the right to initiate judicial proceedings

158. As already mentioned *supra* 108, data subjects not only have substantive rights but also procedural rights. The GDPR states that data subjects have the right to lodge a complaint with a supervisory authority if they consider that the processing of personal data concerning them infringes the GDPR.[558] In practice, the data subject will lodge the complaint almost always with a DPA, except where it is alleged that an EU institution or body infringes the GDPR, then the data subject needs to lodge his or her complaint with the EDPS.[559] Data subjects can choose to lodge the complaint either with the supervisory authority "*in the Member State of his or her habitual residence, place of work or place of the alleged infringement*"[560], ensuring this right is not a hypothetical right but, to the contrary, a right that can easily be exercised by the data subjects. After handling the complaint, the engaged supervisory authority needs to inform the data subject on the progress and the outcome of the complaint and the possibility to challenge in court the decision taken about the complaint as taken by that DPA.[561] These rights more or less already existed under Directive 95/46, albeit that they are now much more clearly described. For example, under Directive 95/46, it was not specified with which authority exactly data subjects could lodge their complaints.

159. As under Directive 95/46,[562] data subjects, but also other natural or legal persons such as data controllers, can challenge any legally binding decision of a supervisory authority (including the exercise of any of the powers *supra* 154) concerning them.[563] In addition, data subjects now have the express right to initiate legal proceedings where supervisory authorities do not handle a complaint or do not inform the data subject within three months on the progress or outcome of the

[558] *Ibid*., article 77(1).
[559] Articles 2(1) j° 63(1) of Regulation 2018/1725; GIAKOUMOPOULOS and others, *Handbook on European data protection law*, 238.
[560] Article 77(1) GDPR.
[561] *Ibid*., article 77(2) GDPR and article 63(2) of Regulation 2018/1725.
[562] Article 28(3) *in fine* Directive 95/46.
[563] Article 78(1) GDPR; article 64(2) of Regulation 2018/1725.

complaint lodged.[564,565] This way, the GDPR ensures that the right to an effective judicial remedy, enshrined in the Charter,[566] is respected.

160. Besides the right to challenge legally binding decisions of the supervisory authorities, data subjects now also have the right to initiate proceedings against data controllers and processors when the data subjects consider that their rights under the GDPR are infringed upon.[567] It is important to note that data subjects have the right to choose where to initiate these proceedings, either before the courts of the member state where the controller (or processor) has an establishment or where the data subject has his or her habitual residence.[568,569] The latter option makes sure that the data subjects have indeed an *effective* judicial remedy, since they are not obliged to initiate proceedings before a court in a member state which they have no affinity with whatsoever.

161. In connection to this, the GDPR also grants data subjects the right to mandate not-for-profit organisations which are "*active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data*", to exercise the rights analysed *supra* 158-160,[570] making a form of class action lawsuits available to data subjects. This is a completely new right, not existing under Directive 95/46.

b) Liability and compensation

162. The GDPR states that controllers and processors should, in principle, "*compensate any damage which a person may suffer as a result of processing that infringes*" the GDPR.[571] In other words, controllers are liable for the damage caused as a result of processing by them which infringes the GDPR. The concept of damage ought to be broadly interpreted, comprising both

[564] Article 78(2) GDPR and article 64(2) of Regulation 2018/1725.
[565] Directive 95/46 did not provide for such a right.
[566] Article 47 Charter.
[567] Article 79(1) GDPR.
[568] *Ibid*., article 79(2).
[569] The latter option is only available when the controller or processor is not a public authority of a Member State acting in the exercise of its public powers.
[570] Article 80(1) GDPR.
[571] *Ibid*., recital 146 and article 82(2).

material and non-material damage.[572] Where more than one controller or processor is involved in the same processing, each controller or processor is to be held liable for the entire damage, ensuring that data subjects are fully and effectively compensated for the damage they have suffered.[573] Directive 95/46 also stated that persons should receive compensation for damage as a result of an unlawful processing[574] but the GDPR reinforces this right to compensation, providing for a higher protection than Directive 95/46.

c) Fines

163. As a last, and ultimate, element of enforcement, the GDPR provides for administrative fines. The DPA's should ensure that those fines are effective, proportionate and dissuasive.[575] The GDPR describes in great detail which elements shall be given regard to when imposing fines,[576] e.g. whether the infringement was intentional or negligent and which categories of personal data were affected by the infringement.[577] For the gravest infringements, the DPA's can impose administrative fines up to € 20 000 000, or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[578] The GDPR nevertheless leaves it up to the member states to decide whether and to what extent these fines "*may be imposed on public authorities and bodies established in that Member State*".[579]

164. Unlike the GDPR, Directive 95/46 did not provide for any fines, it only stated that member states should "*adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement*".[580] Whereas this provision should in theory ensure that the protection offered by the legislation is implemented in reality, it is self-evident that harder, more precise rules about fines, such as in the GDPR, are more likely to stimulate compliance with the protection offered.

---

[572] *Ibid*., recital 146 and article 82(1).
[573] *Ibid*., recital 146 and article 82(4).
[574] Article 23 Directive 95/46.
[575] Article 83(1) GDPR.
[576] *Ibid*., article 83(2).
[577] *Ibid*., article 83(2)(b) and (g).
[578] *Ibid*., article 83(5).
[579] *Ibid*., article 83(7).
[580] Article 24 Directive 95/46.

CHAPTER III: THE REQUIRED LEVEL OF PROTECTION IN THIRD COUNTRIES FOR TRANSFERS OF DATA TO THOSE COUNTRIES

Section 1: Introduction

165. There are several legal grounds on which personal data transfers to third countries can be based. Directive 95/46 already provided for transfers on the basis of 'adequacy decisions' and transfers subject to 'appropriate safeguards.'[581] The latter included both transfers on the basis of the SCC Decisions (see also *supra* 7), since standard contractual clauses were explicitly mentioned in the Directive,[582] and, as a legal practice, transfers on the basis of binding corporate rules.[583] Directive 95/46 also already established that in specific situations data transfers could still take place even though there is no adequacy decision nor are there 'appropriate safeguards', e.g. where the data subject has given his or her unambiguous consent.[584]

166. The GDPR still provides for adequacy decisions, 'appropriate safeguards' (including standard contractual clauses) and 'derogations for specific situations.'[585] In addition, the GDPR now explicitly provides for transfers on the basis of binding corporate rules[586] and introduces codes of conduct[587] and certification mechanisms[588].

167. Since the PSD is an adequacy decision, only the requirements regarding these adequacy decisions will be highlighted. The requirements for other means for transferring personal data to third countries (such as the SCC decisions) will not be discussed.

---

[581] Articles 25(6) and 26(2) Directive 95/46.
[582] *Ibid*., article 26(4).
[583] T. KUGLER, "Practical Examples" in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 202-204. The WP29 has developed rules concerning these binding corporate rules.
[584] Article 26(1)(a) Directive 95/46. See also recital 112 GDPR.
[585] Respectively articles 45, 46 and 49 GDPR. See also recital 108 GDPR.
[586] Article 47 GDPR.
[587] *Ibid*., article 40 j° article 46(2)(e).
[588] *Ibid*., article 42 j° article 46(2)(f).

Section 2: An 'adequate' level of protection

Subsection 1: The GDPR and Directive 95/46

168. The GDPR, essentially in the same way as Directive 95/46 before,[589] states that "*a transfer of personal data to a third country* […] *may take place where the Commission has decided that the third country* […] *in question ensures an adequate level of protection*".[590] In contrast to Directive 95/46 however, the GDPR lists several elements the Commission needs to take account of when assessing this 'adequate level of protection'.[591] The Commission must 'in particular', indicating a non-exhaustive list of elements, take account of, *i.a.*, "*the rule of law, respect for human rights and fundamental freedoms, relevant legislation*", "*the implementation of such legislation*", "*rules for the onward transfer of personal data to another third country*", "*case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress*" and "*the existence and effective functioning of one or more independent supervisory authorities, including adequate enforcement powers*".[592] The GDPR is therefore far more specific than the older Directive, demanding a more rigorous assessment of adequacy by the Commission.

169. Besides this more stringent initial assessment of adequacy, the GDPR states that, once adopted, these adequacy decisions are subject to monitoring schemes.[593] Indeed, the GDPR states that the adequacy decisions "*shall provide for a mechanism for a periodic review, at least every four years*".[594] Moreover, the GDPR requires the Commission to monitor "*on an ongoing basis* […] *developments in third countries* […] *that could affect the functioning of* [the] *decisions adopted*"[595] and to "*repeal, amend or suspend the decision*" when it finds that the third country no longer ensures the required 'adequate level of protection'.

[589] Article 25(6) Directive 95/46.
[590] Article 45(1) GDPR.
[591] *Ibid*., article 45(2).
[592] *Ibid*., article 45(2)(a) and (b).
[593] *Ibid*., recital 106 and article 45(3), (4), (5).
[594] *Ibid*., article 45(3).
[595] *Ibid*., article 45(4).

170. On top of this, the GDPR determines that the foregoing provisions "*shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined*",[596] indicating the required level of protection should meet that offered by the GDPR itself.

Subsection 2: Case law of the CJEU

171. Firstly, it is important to note that there has been a legal dispute concerning the legal basis of an adequacy decision, namely the case *Parliament v Council and Commission*.[597] In this case, the Commission based its adequacy decision[598] concerning transfers of PNR data to the USA on Directive 95/46. The CJEU however subsequently annulled this adequacy decision.[599] It stated that the adequacy decision concerned processing operations for purposes of "*public security and activities of the State in areas of criminal law*".[600] Since these matters fall outside the scope of Directive 95/46, the adequacy decision could not lawfully be based on that Directive.[601] Although the PSD by no means exclusively deals with transfers of personal data for purposes of "*public security and activities of the State in areas of criminal law*", it does cover, to a certain extent, the adequacy of data protection by U.S. public authorities (including agencies ensuring public security (*infra* 224-265) and investigating criminal offences).[602] It is therefore not inconceivable that questions concerning the legal basis of the PSD could arise before the CJEU. These questions will nevertheless not be discussed.[603]

---

[596] *Ibid*., article 44.
[597] Judgment of 30 May 2006, *Parliament v Council and Commission*, C-317/04 and C-318/04, ECLI:EU:C:2006:346.
[598] Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, *OJ* L235/11 of 6 July 2004.
[599] Judgment of 30 May 2006, *Parliament* v *Council and Commission*, C-317/04 and C-318/04, ECLI:EU:C:2006:346, para 61.
[600] *Ibid*., para 56.
[601] *Ibid*., para 59.
[602] See recitals 64-135, Annex III, Annex VI and Annex VII PSD.
[603] For more information concerning legal challenges to the legal basis of the various PNR schemes, see e.g. C. CHEVALLIER-GOVERS, "Personal Data Protection: Confrontation between the European Union and the United States of America" in Y. ECHINARD and others (eds), *L'Union européenne et les Etats-Unis : processus, politiques et projets*, Bruxelles, Larcier, 151-159.

172. The previous subsection already made clear that the concept 'adequate level of protection' is a key element. Whether a third country ensures an adequate level of protection is a real make-or-break requirement. When it is not fulfilled, personal data can only be transferred when the involved controllers and processors adhere to additional standards such as binding corporate rules. It is therefore imperative to determine what this 'adequate level of protection' exactly entails.

173. The CJEU has interpreted the concept 'adequate level of protection', mainly in *Schrems*[604]. This subsection will therefore first discuss *Schrems* itself and will next discuss some issues arising from this case law.

§1 *Schrems* and essentially equivalent protection

174. The factual circumstances of *Schrems* are already explained *supra* 2-4. In this judgment, the CJEU gave much-needed clarification on how the concept 'adequate level of protection' should be interpreted. It started by admitting that this concept is not defined anywhere in Directive 95/46.[605] However, the CJEU did state that this concept "*implements the express obligation laid down in Article 8(1) of the Charter to protect personal data*" and is thus "*intended to ensure that the high level of that protection continues where personal data is transferred to a third country*", echoing the remark by AG Bot that the objective of the concept is "*to ensure the continuity of the protection afforded by* [Directive 95/46] *where personal data is transferred to a third country*".[606]

175. After these observations, the CJEU proceeded to make its, one could argue, most significant statements of the whole judgment. "*The word 'adequate'* […] *admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However* […] *the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter*".[607] The CJEU unequivocally establishes here that 'adequate' should be

[604] Judgment *Schrems*.
[605] *Ibid*., para 70.
[606] *Ibid*., para 72; Opinion of AG Bot *Schrems*, para 139.
[607] Judgment *Schrems*, para 73.

interpreted as meaning 'essentially equivalent'.[608] The CJEU motivates this interpretation on the basis that in case of any other interpretation, the protection of personal data could easily be bypassed through transfers to third countries.[609] This interpretation did obviously not appear out of thin air. AG Bot already considered that 'adequate' cannot merely be understood as 'satisfactory' or 'sufficient'[610] and that an adequate level of protection could only exist where it is established that a third country "*offers a level of protection that is essentially equivalent to that afforded by* [Directive 95/46]*, even though the manner in which that protection is implemented may differ from that generally encountered within the European Union*".[611] In other words, "*transfers of personal data to third countries should not be given a lower level of protection than processing within the European Union*".[612]

176. This case law that equates 'adequate' with 'essentially equivalent' was reiterated in *PNR Canada*[613] by both AG Mengozzi and the CJEU itself.[614] In that case, the CJEU conceded that "*the means intended to ensure such a level of protection may differ from those employed within the European Union*" (reflecting the statement that the protection offered is not required to be identical, *supra* 175) but that third countries, *in casu* Canada, should still ensure protection essentially equivalent to that guaranteed within the European Union.[615]

177. Besides the clarification what 'adequate' means, the CJEU, in *Schrems*, also established a few other things concerning adequacy decisions taken by the Commission, most of which are now incorporated in the GDPR (see *supra* 169). The CJEU stated that the Commission must, in its assessment of adequacy, "*take account of all the circumstances surrounding a transfer of personal*

[608] One author compares this requirement of essentially equivalent protection with the *Solange* judgment of the German Bundesverfassungsgericht, see L. AZOULAI and M. VAN DER SLUIS, "Institutionalizing personal data protection in times of global institutional distrust: Schrems", *CMLRev* 2016, (1343) 1363. Note that in some language versions, 'essentially equivalent' is translated into a softer requirement, e.g. in the Dutch version, the words 'in grote lijnen overeenkomen' (broadly match) are used. However, in the French, Italian and German versions, the words 'substantiellement équivalent' (substantially equivalent) and, respectively, 'sostanzialmente equivalente' (substantially equivalent) and 'ein Schutzniveau […] der Sache nach gleichwertig ist' (a level of protection that is in substance equivalent) are used, resembling the English phrasing. In any case, as English is the language of the case, the English language version is the only authentic one and has therefore precedence over the other versions.
[609] Judgment *Schrems*, para 73.
[610] Opinion of AG Bot *Schrems*, para 142.
[611] *Ibid*., para 141.
[612] *Ibid*., para 141.
[613] Opinion *PNR Canada*.
[614] See Opinion *PNR Canada*, paras 93, 134, 214; Opinion of AG Mengozzi *PNR Canada*, para 204.
[615] Opinion *PNR Canada*, para 134.

data to a third country",[616] proving that the protection is essentially equivalent as in the EU, both in law and in practice.[617] The Commission must duly state reasons that the third country assessed does in fact ensure an essentially equivalent level of protection.[618] Establishing empty findings such as 'country x ensures an adequate level of protection since it provides for satisfactory and essentially equivalent protection', without actually scrutinising the protection offered is not sufficient. Moreover, the assessment should be strict as the Commission's discretion is reduced due to the potential, grave impact on a large number of persons should a transfer of personal data to a country which does not ensure an adequate level of protection happen.[619] The CJEU also established that the Commission, after adopting an adequacy decision, must check periodically whether the finding that the third country offers adequate protection is still factually and legally justified.[620]

178. As explained above (*supra* 168), the GDPR has taken over the concept of an 'adequate level of protection', meaning that the interpretation of this concept by the CJEU under Directive 95/46 is still relevant under the GDPR. Since the GDPR makes the rules concerning adequacy decisions stricter than they were under Directive 95/46 (*supra* 168-170), it is conceivable that the case law of the CJEU will also get stricter.

§2 Problems arising from the interpretation in *Schrems*

179. While the case law in *Schrems* concerning the 'essentially equivalent' protection required by the CJEU in third countries can be applauded for closing the door to circumvention of EU data protection rules through transfers to third countries, one could argue that this 'essentially equivalent' case law, at the same time, opens Pandora's box. Surely, the requirement that the level of protection should be 'essentially equivalent' to the level of protection in the EU is a good thing when the level of protection in the EU is high, which is the case for the protection offered to

[616] Judgment *Schrems*, para 75.
[617] *Ibid*., paras 74-75.
[618] *Ibid*., para 96.
[619] *Ibid*., para 78.
[620] *Ibid*., para 76. AG Bot also stressed the importance of periodic review, stating that "*the obligation for the third country to ensure an adequate level of protection is thus an ongoing obligation*" and that the word 'ensures' in the Directive, conjugated in the present tense, "*implies that, in order to be able to be maintained,* [adequacy decisions] *must relate to a third country which, after the adoption of the decision, continues to guarantee such an adequate level of protection*". See Opinion of AG Bot *Schrems*, paras 137, 146-147, 230.

personal data falling within the scope of the GDPR and the Charter. However, not all processing of personal data falls under the GDPR and the Charter. Indeed, the GDPR itself states that it does not apply to several categories of processing (*supra* 84).[621]

180. For example, the GDPR does not apply to processing of personal data by police services "*for the purposes of prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security*".[622] This has as a result that, still according to the case law of the CJEU, when the police services of a third country process personal data for these purposes, they should, for that third country to be considered providing 'essentially equivalent' protection, not adhere to the requirements set by the GDPR, since the GDPR is in the EU itself also not applicable to this processing. In the context of processing of personal data by police services, the fact that the requirements set by the GDPR are not to be adhered to is not that dramatic, since there is a distinct regulatory framework for this kind of processing, namely Directive 2016/680 (the so-called Law Enforcement Directive, hereinafter: 'LED').[623] The LED also offers significant protection of personal data, similar to the protection offered by the GDPR.[624] Consequently, third countries processing personal data in that context must ensure 'essentially equivalent' protection as offered by the LED. Moreover, the Charter also applies to this processing of personal data, also offering protection which needs to be

[621] Article 2(2) GDPR.
[622] *Ibid*., recital 19 and article 2(2)(d).
[623] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ* L119/89 of 4 May 2016 (hereinafter: 'LED').
[624] All 'key principles' of the GDPR can also be found in the LED. The principles of fairness, purpose limitation, data minimisation, accuracy, storage limitation and accountability can be found in respectively article 4(1)(a), 4(1)(b), 4(1)(c), 4(1)(d), 4(1)(e) and 4(4) LED. The principle of lawfulness can be found in article 4(1)(a) LED and is further specified in article 8 LED and, like in the GDPR, there is also a separate article concerning the lawfulness of processing of sensitive data (article 10 LED). The principle of data security can be found in article 4(1)(f) LED and is further specified in articles 29-31 LED. The LED does not provide for the principle of transparency *as a principle*, but it is mentioned in recital 26 and *de facto* provided for in articles 12 and 13 LED. The LED also provides for most rights of the data subject, only the right to object and the right to data portability lack. The absence of the latter is rather obvious and can hardly be deemed to deprive the data subjects of a right considering the nature of the processing we are dealing with here. The rights to access, rectification, erasure, restriction and the right not to be subject to automated individual decision making are provided for by respectively articles 14-15, article 16(1) and (5), article 16(2), article 16(3) and article 11 LED. Additionally, the LED provides for DPIA's and prior consultation (articles 27-28), DPO's (articles 32-24) and independent supervisory bodies (articles 41-49). Lastly, the LED, again like the GDPR, provides for the right to lodge a complaint with the supervisory body (article 52), rights concerning judicial remedies (articles 53-55), the right to compensation (article 56) and penalties (article 57).

'matched' by the third country if it wants to be considered to offer 'essentially equivalent' protection. In this context, one could still argue that the third countries offering 'essentially equivalent' protection as the LED indeed provide an 'adequate' level of protection.

181. However, the GDPR also states that it does not apply to the processing of personal data "*in the course of an activity which falls outside the scope of Union law*",[625] meaning that activities of security services[626] are not covered by the GDPR (see, again, *supra* 84).[627] However, since these activities by definition fall outside the scope of Union law, it is impossible for the EU to legislate on this matter. Indeed, the Treaty on European Union ('TEU') states that "*national security remains the sole responsibility of each Member State*", prohibiting the EU to enact legislation on this subject-matter.[628] The Charter is likewise not applicable to processing of personal data by security services since it states that "*the provisions of this Charter are addressed* […] *to the Member States only when they are implementing Union law*".[629] Thus, when strictly following the interpretation of adequacy by the CJEU, since there is, in this context, no level of protection 'guaranteed within the EU',[630] it is no problem for third countries to have no protection at all since such a level of protection would still be 'essentially equivalent'. Nonetheless, it is hard to grasp how this 'level of protection' (*i.e.* no protection) could still be considered to be 'adequate'.

182. The CJEU handily sidesteps these issues by implicitly assuming that the processing of personal data in the dispute before it (i.e. between Mr. Schrems and Facebook) was purely commercial by nature.[631] As a result, the CJEU never considers whether the U.S. practices it denounces would be lawful on this side of the Atlantic.[632] Indeed, the Snowden revelations not only uncovered mass surveillance by the American NSA, but also by the UK GCHQ.[633]

---

[625] Article 2(2)(a) GDPR.
[626] Article 4(2) TEU.
[627] This reasoning was also (albeit regarding Directive 95/46), unsuccessfully, brought forward by Facebook in Judgment High Court (IRL), paras 50-58, 92. For the reasoning as to why this argument failed, see *ibid*., paras 61 97.
[628] *Contra* S. CRESPI, "The applicability of Schrems principles to the Member States: national security and data protection within the EU context", *ELR* 2018, (669) 677-683, where it is argued that the EU law is, to some extent, applicable to the activities of security and intelligence services.
[629] Article 51(1) of the Charter.
[630] Cf. the words of the CJEU in Judgment *Schrems*, paras 74, 96.
[631] L. AZOULAI and M. VAN DER SLUIS, "Institutionalizing personal data protection in times of global institutional distrust: Schrems", *CMLRev* 2016, (1343) 1364.
[632] *Ibid*.
[633] *Ibid*., 1365.

Subsection 3: Practical problems with the adequacy requirement

183. Besides the legal issues surrounding the adequacy requirement, some authors also question the utility and workability of this requirement.[634] It is a fact that data protection regulation, like all regulation, is subject to change. This implies that, even if the level of protection of personal data is considered to be adequate at one point in time, legislative amendments or other changes (both in law or in practice) to data protection rules can also potentially upend the assessment of adequacy.[635] The GDPR provides for periodic reviews, and to a certain extent, even constant monitoring, of adopted adequacy decisions as a solution to this problem (*supra* 169).[636] However, one could question the feasibility of constant monitoring of all adequacy decisions.[637]

184. An even more pressing question is whether adequacy assessments by the Commission can be relied on to depict the actual level of protection of personal data by third countries.[638] Indeed, revelations concerning secret data processing programmes such as PRISM[639] and the program concerning SWIFT[640] have made clear that even though a third country might seem to provide an adequate level of protection on the outside, in practice, it clearly does not.

[634] E. DE BUSSER, "Flagrant Denial of Data Protection: Redefining the Adequacy Requirement" in D. J. B. SVANTESSON and D. KLOZA (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, Cambridge, Intersentia, 2017, 430 (hereinafter: DE BUSSER, "Flagrant Denial of Data Protection").
[635] *Ibid*.
[636] Recital 106 and article 45(3), (4) and (5) GDPR.
[637] DE BUSSER, "Flagrant Denial of Data Protection", 430-431.
[638] L. AZOULAI and M. VAN DER SLUIS, "Institutionalizing personal data protection in times of global institutional distrust: Schrems", *CMLRev* 2016, (1343) 1366.
[639] DE BUSSER, "Flagrant Denial of Data Protection", 430.
[640] *Ibid*., 441.

CHAPTER IV: DOES THE PRIVACY SHIELD ADHERE TO THE REQUIRED LEVEL OF PROTECTION?

185. In this last chapter, an analysis will be made on whether the PSD provides an 'adequate level of protection' (as discussed in Chapter III), *i.e.* whether the PSD ensures an equivalent level of protection as provided by EU law, here limited to EU primary law (discussed in chapter I) and the GDPR (discussed in chapter II). However, before delving into this analysis, the PSD itself will be briefly discussed.

Section 1: What is the Privacy Shield?

186. The PSD is, again like the SHD before, and unlike the majority of adequacy decisions, not an unconditional adequacy decision which establishes in a generalised manner that "[country name] *is considered as providing an adequate level of protection for personal data transferred from the European Union*".[641] The PSD however only states that "*the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield*".[642] This 'EU-U.S. Privacy Shield' is based on a

[641] For example, the adequacy decision concerning the Principality of Andorra states that "*For the purposes of Article 25(2) of Directive 95/46/EC, Andorra is considered as providing an adequate level of protection for personal data transferred from the European Union.*", see article 1 Commission Decision 2010/625/EU of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra, *OJ* L277/27 of 21 October 2010. The same phrasing (or at least a similar phrasing) can be found in the adequacy decisions concerning Argentina, the Bailiwick of Guernsey, the Isle of Man, the Bailiwick of Jersey, New Zealand and the Eastern Republic of Uruguay, see respectively article 1 Commission Decision 2003/490/EC of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, *OJ* L168/19 of 5 July 2003; article 1 Commission Decision 2003/821/EC of 21 November 2003 on the adequate protection of personal data in Guernsey, *OJ* L308/27 of 25 November 2003; article 1 Commission Decision 2004/411/EC of 28 April 2004 on the adequate protection of personal data in the Isle of Man, *OJ* L151/48 of 30 April 2004; article 1 Commission Decision 2008/393/EC of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey, *OJ* L138/21 of 28 May 2008; article 1 Commission Implementing Decision 2013/65/EU of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, *OJ* L28/12 of 30 January 2013; article 1 Commission Implementing Decision 2012/484/EU of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data, *OJ* L227/11 of 28 August 2012.

[642] Article 1(1) PSD. The PSD therefore takes essentially the same approach to adequacy in the USA as the SHD. The SHD equally stated that only personal data under the Safe Harbour was considered to be adequately protected, see article 1(1) SHD. The adequacy decisions concerning Canada, the Faeroese Islands, the State of Israel and Japan also

system of self-certification by which U.S. organisations commit to a set of privacy principles (the Privacy Shield Principles, hereinafter: 'the PSP's').[643] The PSD also contains in its annexes a series of unilateral statements of the U.S. government,[644] replicating the approach taken in the SHD.[645] Once a U.S. organisation has committed to the PSP's, transfers of personal data from the EU to this organisation are allowed under the PSD. This technique has as a consequence that, initially, an assessment needs to be made of the level of protection of personal data offered by the PSP's, rather than the protection offered by the legal system of the USA itself. However, since the PSD, yet again like the SHD,[646] contains for national security, law enforcement and public interests purposes several possible derogations to the PSP's,[647] the adequacy of the U.S. legislative framework surrounding these derogations also need to be assessed by the Commission.

---

have, to a certain extent, 'strings attached', see respectively article 1 Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, *OJ* L2/13 of 4 January 2002; article 1 Commission Decision 2010/146/EU of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data, *OJ* 58/17 of 9 March 2010; article 1(1) Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, *OJ* L27/39 of 1 February 2011; article 1(1) and (2) Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, *OJ* L76/1 of 19 March 2019.

[643] Recital 14 PSD.

[644] S. SALUZZO, "Looking for safe harbours outside the European Union: The issue of onward transfers in EU data protection law and its external dimension" in G. VERMEULEN and E. LIEVENS (eds), *Data Protection and Privacy under Pressure*, Antwerp, Maklu, 2017, 139.

[645] L. AZOULAI and M. VAN DER SLUIS, "Institutionalizing personal data protection in times of global institutional distrust: Schrems", *CMLRev* 2016, (1343) 1368.

[646] Annex I, fourth paragraph SHD.

[647] Annex II, I.5. PSD.

Section 2: Does the Privacy Shield Decision comply with EU law?

Subsection 1: The Privacy Shield Principles

187. In this subsection, the substance and the enforcement of the PSP's will be analysed in the light of the primary law of the EU as interpreted by the CJEU in *Digital Right Ireland, Tele2 Sverige*, *Schrems* and *PNR Canada*, and from the perspective of whether they provide essentially equivalent protection as the GDPR. For that purpose, the problematic aspects of the PSP's will be analysed one by one. The rules concerning onward transfers will not be discussed.

§1 Concerns about proportionality: storage limitation and data minimisation in peril?

188. The first big problem with the PSP's seems to be the rather dubious wording of the data minimisation principle (*supra* 97-98) and, connected to it, the absence of a clearly formulated storage limitation principle[648] (*supra* 102-103). This in turn imperils the proportionality requirement of article 52(1) of the Charter as interpreted by the CJEU.

189. Although one of the PSP's, the 'Data Integrity and Purpose Limitation' principle ('Principle 5'), states in annex II, II.5.a. of the PSD that "*personal information must be limited to the information that is relevant for the purposes of processing*",[649] echoing the data minimisation principle, problems arise when this requirement is examined in greater detail. Like the WP29 argues, "*the mere fact that the data shall be relevant to the processing is not sufficient to make the processing proportionate*".[650] Certainly, it is highly doubtful that the CJEU would consider it 'strictly necessary' to process personal data in relation to the purposes for which they are processed, whenever this processing is 'relevant' for these purposes. The GDPR equally states that personal data should not only be relevant but on top should be 'limited to what is necessary in relation to the purposes for which they are processed'.[651] 'Necessary' and 'relevant' obviously do not have the same meaning, and, even if they would, the Commission should have insisted on using the term 'necessary' for the sake of consistency. Annex II, II.5.a of the PSD thus at least

[648] Article 29 Working Party, Opinion 01/2016 of 13 April 2016 on the EU – U.S. Privacy Shield draft adequacy decision, 16/EN WP 238, 3 (hereinafter: 'WP29 on the PSD').
[649] Annex II, II.5.a. PSD.
[650] WP29 on the PSD, 23.
[651] Article 5(1)(c) GDPR.

pushes the limits of the data minimisation principle, and, at the same time, stretches the storage limitation principle over its maximum. This is so since Principle 5 states that "*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*".[652] Indeed, when one accepts that the initial processing of personal data is already not proportional (or, 'strictly necessary'), the continued retention of that personal data is *a fortiori* not proportional.

190. To add insult to injury, Principle 5 adds that "*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*".[653] This is not an essentially equivalent protection to the protection of the GDPR, since the latter provides that personal data may be stored for longer periods than necessary for the purposes for which the personal data are processed if the personal data will be processed *solely* for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[654] Again, 'solely' is not equivalent to 'reasonably serving the purposes of', and it even if it would, the PSD should use the terminology of the GDPR for the sake of consistency. Furthermore, principle 5 does not require any specific safeguards concerning this further processing of the personal data. It only states that this processing will still be subject to the other PSP's, which in itself does not provide any additional protection (since these principles would apply anyway). Indeed, Principle 5 does not, like the GDPR,[655] require technical and organisational measures, such as pseudonymisation and, if possible, anonymisation, to ensure respect for the data minimisation principle. Lastly, Principle 5 states that organisations "*should take reasonable and appropriate measures in complying with this provision*".[656] This wording is quite weak, considering the word 'should' instead of 'shall' and the use of 'reasonable'.

---

[652] Annex II, II.5.b. PSD. Note that the Commission, in recital 23 of the PSD, does not use the word 'relevant' but instead states that "*personal data* [may] *only* [be retained] *for as long as it serves the purpose(s) for which it was initially collected or subsequently authorized*", without referring back to e.g. recital 21. This wording resembles more the true meaning of the storage limitation principle but veils the actual situation under the PSP's.
[653] Annex II, II.5.b. PSD.
[654] Article 5(1)(e) GDPR.
[655] Recital 156 and article 89(1) GDPR.
[656] Annex II, II.5.b. *in fine* PSD.

§2 A crippled purpose limitation principle

191. The way the purpose limitation principle is constructed in the PSD is extremely complex. The scope of the principle is different under various PSP's.[657] While the Choice Principle, one of the PSP's, uses the term 'materially different purpose', Principle 5 uses the term 'incompatible purpose'. Neither term is defined, leading the WP29 to voice serious concern about possible inconsistencies.[658] Especially the lack of a definition of what is to be regarded as a 'materially different' purpose is criticised by the WP29, since it leads to legal uncertainty.[659]

192. Besides the issue concerning the different scopes, other problems arise. While the purpose limitation principle as established by Principle 5 is a proper transposition of the purpose limitation principle under the GDPR, the purpose limitation principle as established by the Choice Principle is not. The Choice Principle provides for a right to opt-out to disclosure of personal information to a third party or to the use of personal information for a purpose 'materially different'.[660] In addition, Supplemental Principle 12[661] provides that individuals should have the choice to opt-out for the processing of personal information for direct marketing purposes.[662] If the latter two principles are interpreted as meaning that further processing for incompatible ('materially different') purposes is allowed where an 'opt-out' is provided, thereby creating a loophole to circumvent Principle 5,[663] the PSP's do not provide essentially equivalent protection. While the recitals of the PSD assert that the Choice Principle "*does not supersede the express prohibition on incompatible processing*",[664] this is not applicable to the U.S. organisations self-certifying to the PSP's, since they only commit to the PSP's themselves and not to the entire PSD.[665] The WP29 therefore rightly advised to change the wording in the Choice principle from 'materially different' to 'materially different but nevertheless compatible'.[666]

---

[657] WP29 on the PSD, 24.
[658] *Ibid*.
[659] *Ibid*., 20.
[660] Annex II, II.2.a. PSD.
[661] Annex II, III.12.a. PSD.
[662] See WP29 on the PSD, 19.
[663] *Ibid.*, 20, 25.
[664] Recital 22 PSD.
[665] Annex II, I.1 and annex II, I.2. PSD.
[666] WP29 on the PSD, 20.

§3 Problems regarding sensitive data, automated decision-making and non-discrimination

a) The Sensitive Data Principle

193. Under the Choice Principle, data subjects have to give 'affirmative express consent' for further processing of sensitive data "*for a purpose that is materially different from the purpose(s) for which it was originally collected*" or for onward transfers (which is a form of processing) of that data.[667] So far so good (however, see also *supra* 191-192), *i.e.* all seems in accordance with the specific protection offered by the GDPR to sensitive data.[668] However, the supplemental principle about Sensitive Data (Sensitive Data Principle) in the PSD asserts that 'affirmative express consent' is not required to process sensitive data in certain processing scenarios.[669] Not only do not all processing scenarios enumerated in this Sensitive Data Principle correspond with (and provide for essentially equivalent protection as, *infra* 194-198) the other legitimate grounds on which processing can be based provided for by the GDPR, the very principle itself is very confusing. Indeed, whereas the Choice Principle establishes that consent is required for the *enumerated processing operations*, the Sensitive Data Principle in contrast establishes that consent is *not* required, concerning all sensitive data processing operations, for the *enumerated scenarios*. The latter is problematic, since it gives the wrong impression that it is applicable to processing for the enumerated scenarios, even when this processing entirely takes place in the EU, without any relation with a transfer to the U.S. The PSD could then seemingly provide additional lawful scenarios for processing, which cannot be found in the GDPR, thereby contravening the lawfulness principle (*supra* 87-90). In other words, even if the Sensitive Data Principle would provide essentially equivalent protection, the principle would be problematic since only the GDPR can apply to the said processing.[670] The Commission cannot alter the scope GDPR by way of an Implementing Decision such as the PSD, of which the Sensitive Data Principle is part of. The WP29 therefore rightly argued that the Sensitive Data Principle may only be applied to sensitive data already transferred to the U.S., with the initial collection of the data being based on a legitimate ground listed in the GDPR.[671]

---

[667] Recital 22 and annex II, II.2.c. PSD.
[668] See article 9(2)(a) GDPR.
[669] Annex II, III.1.a. PSD.
[670] See in this context also the assessment of the WP29, WP29 on the PSD, 14.
[671] WP29 on the PSD, 14.

194. Even if the Sensitive Data Principle is interpreted as being only applicable to sensitive data already transferred to the U.S.,[672] aspects of the principle stay problematic since they do not offer essentially equivalent protection as the GDPR.

195. Firstly, the Sensitive Data Principle states that consent is not required where the processing is "*in the vital interests of the data subject or another person*".[673] The corresponding legitimate ground for processing in the GDPR by contrast asserts that processing is legitimate when "*processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent*".[674] Immediately, it is clear that the GPDR is considerably stricter than the PSD. The GDPR mentions two conditions which are absent in the PSD. Firstly, only where the data subject is physically or legally incapable of giving consent, the processing of sensitive data can be based on 'vital interests'. Secondly, only vital interests of *natural* persons count under the GDPR.

196. Secondly, the Sensitive Data Principle allows processing without consent required to provide medical care or diagnosis.[675] While this provision at first sight seems to be essentially equivalent to, or even more restricted than, the corresponding legitimate ground for processing in the GDPR,[676] it is not entirely. Indeed, the GDPR provides in another provision that sensitive data may only be processed on this basis when the data are processed "*by or under the responsibility of a professional subject to the obligation of professional secrecy*".[677] While it may well be that the same requirement applies in the U.S., no finding of that kind is made in the PSD. The Commission can therefore not lawfully conclude that the PSP's ensure essentially equivalent protection on this point.

[672] Which is a reasonable interpretation given that the PSD provides that the PSP's "*are intended for use solely by organizations in the United States receiving personal data from the European Union*", see Annex II, I.1. PSD.
[673] Annex II, III.1.a.i. PSD.
[674] Article 9(2)(c) GDPR.
[675] Annex II, III.1.a.iii PSD.
[676] Article 9(2)(h) GDPR.
[677] Article 9(3) GDPR.

197. Thirdly, processing of sensitive data "*carried out in the course of legitimate activities by a foundation*" is allowed by the Sensitive Data Principle without consent under certain conditions.[678] The corresponding legitimate ground in the GDPR is almost identically worded.[679] However one condition found in the GDPR is missing in the Sensitive Data Principle. The GDPR provides that the processing must be carried out 'with appropriate safeguards'. Whether or not this is 'essentially equivalent' is not clear at all.

198. Fourthly, and lastly, the Sensitive Data Principle states that processing without consent is allowed where the processing is "*necessary to carry out the organisation's obligations in the field of employment law*". The corresponding legitimate ground in the GDPR is similarly worded, but like *supra* 195, the GDPR states that 'appropriate safeguards' should be included, which is not repeated in the Sensitive Data Principle. While one could further argue that the protection is not essentially equivalent offered by the Sensitive Data Principle to that of the GDPR, since obligations ensuing from employment law in the U.S. might not be essentially equivalent to those in the EU, that argument is not really convincing. Indeed, these obligations are not even harmonised within the EU. Therefore, it is even unclear to which rules the concerned obligations in the U.S. should be essentially equivalent to.

b) Data in the context of pharmaceutical and medical products

199. The WP29 also assessed some aspects of Supplemental Principle 14,[680] concerning pharmaceutical and medical products. The WP29 considered that due to the medical context, this principle will mostly be applicable to sensitive data.[681] The WP29 considered it problematic that personal data falling under this supplemental principle, could be transferred to U.S. regulators,[682] while it is not clear whether those regulators are eligible to self-certify under the Privacy Shield.[683] As a consequence, the concerned personal data could end up without any adequate protection in the U.S., since the Commission did not even establish that U.S. regulators will provide any

[678] Annex II, III.1.a.iv PSD.
[679] Article 9(2)(d) GDPR.
[680] Annex II, III.14 PSD.
[681] WP29 on the PSD, 32.
[682] Annex II, III.14.d. PSD.
[683] WP29 on the PSD, 32.

protection at all in its findings.[684] Still concerning Supplemental Principle 14, the WP29 voiced concerns regarding the listing of 'marketing' as an example of processing for future scientific research,[685] which, under the PSP's, consequently does not need a new legal basis for processing.[686] Indeed, this provision makes a mockery of the purpose limitation principle since it is all too obvious that 'marketing' is no scientific research and thus needs to be justified on a new legal basis (*supra* 95).[687]

c) Automated decision-making

200. The PSP's do not provide anything resembling the right not to be subject to automated individual decision-making (*supra* 129-133).[688] The recitals of the PSD do include some findings on U.S. law on this point. It is stated that "*in areas where companies most likely resort to the automated processing of personal data to take decisions affecting the individual (e.g. credit lending, mortgage offers, employment), U.S. law offers specific protections against adverse decisions*".[689] It is further stated that these acts *typically* provide that "*individuals have the right to be informed of the specific reasons underlying the decision*".[690]

201. It is clear from the outset that this does not amount to essentially equivalent protection. First of all, the offered protection is not essentially equivalent, since U.S. law, according to this finding, in principle, allows automated individual decision-making and only provides *a posteriori* protection. The GDPR on the other hand in principle prohibits automated individual decision-making, only allowing it in a restricted number of scenarios.[691] Secondly, the offered protection *a posteriori* is still not sufficient, since it does not include the right to obtain a human intervention. Thirdly, even the allegedly provided protection is not ensured. Indeed, the use of the phrases 'in areas where companies most likely resort to' and 'typically' by the Commission is not really reassuring.

---

[684] *Ibid*.
[685] *Ibid*.
[686] Annex II, III.14.b.ii. PSD.
[687] The WP29 also voiced concerns about so-called 'key-coded data', but this will not be discussed, see Annex II, III. 14.g. PSD; WP29 on the PSD, 31-32.
[688] WP29 on the PSD, 3, 17-18.
[689] Recital 25 PSD.
[690] *Ibid*.
[691] Article 22 GDPR.

202. Furthermore, nothing at all is said, not even in the recitals, about automated individual decision-making of sensitive data. Given the CJEU's reservations in *PNR Canada* concerning automated processing based on sensitive data in the light of the principle of non-discrimination (*supra* 73), it is highly likely that this omission in the PSD will not be received well in Luxembourg.[692]

§4 Essentially equivalent rights of the data subject?

a) The right of access

203. The rules concerning the right to access are contained in three principles: in the Access Principle, in the supplemental principle concerning access ('Supplemental Principle 8') and in the supplemental principle concerning Public Record and Publicly Available Information ('Supplemental Principle 15').[693] The Access Principle states that "*individuals must have access to personal information about them that an organisation holds* […] *except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated*".[694] As long as 'holds' is interpreted as meaning 'processes', the Access Principle seems to provide more or less essentially equivalent protection. While the *caveat* concerning disproportionality cannot be found in the same fashion in the GDPR,[695] one can reasonably argue that the Access Principle nonetheless provides essentially equivalent protection since it provides for a balancing of rights and interests.[696] Indeed, the CJEU in *Schrems* did not require identical protection, merely essentially equivalent protection (*supra* 175).

---

[692] See also M. ZALNIERIUTE, "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement", *Mod. Law Rev.* 2018, (1046) 1059-60. This author also doubts whether the PSD will "*survive the increased scrutiny elaborated by the CJEU*" in *PNR Canada*.
[693] Annex II, II.6. PSD and annex II, III.8. PSD.
[694] Annex II, II.6.a. PSD.
[695] Recital 62 and article 14(5) GDPR resemble this *caveat* the most. However, recital 63 is only a recital and specifies that disproportionality will 'in particular' occur where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, thereby not explicitly excluding disproportionality on the basis of a high expense for the data controller but not mentioning it either. Article 14(5) GDPR in its turn is only applicable to processing of personal data which have not been obtained from the data subject.
[696] Moreover, Annex II, III.8.b.ii PSD provides extra safeguards for sensitive data and data used for 'decisions that will significantly affect the individual', e.g. by saying that access to such data must be granted, even if it is 'relatively difficult or expensive to provide' this information.

204. Problems arise however when examining the Supplemental Principles 8 and 15. First of all, a similar criticism on Supplemental Principle 8 as on the Access Principle itself can be made. Supplemental Principle 8 states that "*an organization may charge a fee that is not excessive*".[697] The GDPR on the other hand provides that the exercise of the right of access will be free of charge, safe for manifestly unfounded or excessive requests.[698] Supplemental Principle 8 further states that "*access needs to be provided only to the extent that an organisation stores the personal information*".[699] It should be made clear that 'stores' cannot be interpreted restrictively but should be regarded here as a synonym for 'processes'.[700] On a more serious point, both principles provide for absolute exceptions to the right of access, *i.e.* no balance of rights and interests between those of the data subject and those of the organisation will occur.[701] No such exceptions exist under the GDPR. For these reasons, the PSP's do not provide an essentially equivalent level of protection. Moreover, the exceptions on the right of access also infringe article 8(2) of the Charter, since that provision establishes a right to access (*supra* 10). It is highly doubtful that the CJEU would accept that this infringement can be justified under article 52(1) as there is no balancing, and therefore the infringement is likely to be considered disproportionate.

[697] Annex II, III.8.f.i. PSD. Annex II, III.8.f.ii. PSD states that charging a fee may be justified, *for example*, where requests are manifestly excessive. See also recital 25 PSD.
[698] Article 12(5) GDPR.
[699] Annex II, III.8.d.ii. PSD.
[700] WP29 on the PSD, 25.
[701] *Ibid.*, 26, 33. For example, reasons for denying (or limiting) access are: "*breaching a professional privilege or obligation*", "*prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organisations*", "*prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization*", see annex II, III.8.e.i.3., annex II, III.8.e.i.4. and annex II, III.8.e.i.5. PSD. Organisations may also deny or limit access "*to the extent that granting full access would reveal its own confidential commercial information, such as marketing inferences*", see annex II, III.8.c.i. PSD. The PSD also states that "*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*", see annex II, III.8.e.i. PSD. However, under the GDPR, these restrictions must "*respect the essence of the fundamental rights and freedoms and [be] a necessary and proportionate measure in a democratic society*", article 23(1) GDPR. Lastly, the Access principle does not apply to 'public record information' and 'information that is already publicly available to the public at large', giving organisations all the means to deny access to this personal data, see annex II, III.15.d. and annex II, III.15.e. PSD. Again, such an exception does not exist under EU law.

b) The right to rectification and the accuracy principle

205. The exceptions to the right of access provided for by Supplemental Principle 8 and 15 also have an impact on the right to rectification. Indeed, when a data subject cannot access its personal data, it cannot control the accuracy of that data and it is therefore impossible for the data subject to demand rectification of that data.[702] The PSD thus does not provide essentially equivalent protection.

206. This absence of a genuine right to rectification in certain circumstances imperils the accuracy principle (*supra* 99-101). However, this is not the only problem regarding that principle. Principle 5 equally imperils the accuracy principle by stating that "*to the extent necessary for those purposes, an organisation must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current*".[703] The WP29 correctly doubted whether the words 'to the extent necessary to these purposes' should be included.[704] Indeed, the GDPR requires personal data to be accurate and establishes that "*every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified*".[705] 'Having regard to' is not essentially equivalent to 'to the extent necessary'. The latter seems to indicate that if accuracy is not 'necessary' for the processing purposes, the personal data does not need to be accurate, while the former only establishes that the processing purposes ought to be considered when contemplating erasure or rectification. Again, the PSD does not provide essentially equivalent protection.

c) The right to erasure, the right to be forgotten and freedom of the press

207. First of all, what has been said *supra* 205 about the right to rectification can be repeated *mutatis mutandis* concerning the right to erasure.

[702] WP29 on the PSD, 33.
[703] Annex II, II.5.a. PSD.
[704] WP29 on the PSD, 24.
[705] Article 5(1)(d) GDPR; WP29 on the PSD, 24.

208. Furthermore, the WP29 voiced concerns regarding the supplemental principle concerning journalistic exceptions ('Supplemental Principle 2').[706] The WP29 argued that Supplemental Principle 2 is broader than the exceptions concerning processing for journalistic purposes in the EU and is also not completely in line with the case-law of the CJEU in *Google Spain*.[707] Supplemental Principle 2 seems indeed to place press freedom above data protection in any case, without any balancing,[708] by disapplying the PSP's completely to "*personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives*".[709] Firstly, this is contrary to the case law of the CJEU, which requires a balancing between the right to a free press and the right to the protection of personal data.[710] Moreover, as the WP29 has argued,[711] Supplemental Principle 2 seems to include not only processing for journalistic purposes, but also any further processing of the covered personal data by any data controller or processor. If so, Supplemental Principle 2 leaves no room at all for the right to be forgotten as established by the CJEU in *Google Spain*. Therefore, the PSD does not ensure essentially equivalent protection on this point.

d) The right to object

209. The PSD does not provide for a general right to object such as provided for by the GDPR (*supra* 125-128) and can therefore not be considered to provide essentially equivalent protection. Moreover, as it has been argued *supra* 128, this absence could potentially also lead to an unjustified infringement of the Charter. The PSD does establish an 'opt-out' for the processing for 'materially different purposes', which is in itself already problematic (*supra* 192) and for

[706] Annex II, III.2. PSD.
[707] WP29 on the PSD, 25.
[708] Even though the PSD itself uses the word 'balancing' in Annex II, II.2.a. PSD, it does not actually state that a balance must be sought. It merely states that the First Amendment of the U.S. Constitution must govern the balancing between the freedom of the press and 'privacy protection interests'. Nowhere is it established by the Commission that any balancing actually happens in the U.S., let alone that such balancing would result in essentially equivalent protection.
[709] Annex II, III.2.b. PSD.
[710] Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, para 56; Judgment *Google Spain*, para 81; Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, para 64.
[711] WP29 on the PSD, 25.

processing in the context of direct marketing purposes.[712] The opt-out provided for processing in the context of direct marketing purposes can be considered to be essentially equivalent to a right to object in that context.[713] However, this provision cannot compensate the lack of a right to object in other contexts. The WP29 therefore rightly recommended that the Commission should make clear that the right to object should exist at any given moment, in any situation.[714]

e) The absence of the right to data portability

210. The PSD does not include anything resembling the right to data portability.[715] While this was not problematic at the time of the adoption of the PSD, since Directive 95 did not include the right to data portability either (*supra* 122), it is now. The GDPR was adopted more than three years ago,[716] and is now for more than a year in force, meaning that the Commission had enough time to update the PSD to ensure essentially equivalent protection. The fact that this has not happened means that no essentially equivalent protection can exist on this point.

f) The absence of the right to restriction of processing

211. Nothing at all resembling the right restriction of processing can be found in the PSD. This is all the more damning since a similar right already existed under Directive 95/46 (*supra* 120). The PSD therefore does not provide essentially equivalent protection. What has been said *supra* 209 concerning the Charter can *mutatis mutandis* be repeated.

[712] Annex II, II.2.a. and annex II, III.12.a PSD.
[713] Something that is also implicitly alleged by the Commission in recital 22 PSD.
[714] WP29 on the PSD, 19-20.
[715] *Ibid*., 15.
[716] As of 15/5/2019.

§5 A curtailed data security principle

212. While the PSD has a Security Principle,[717] and while this principle seems to be more or less[718] essentially equivalent to the 'integrity and confidentiality' principle under the GDPR[719], it never mentions the concepts of 'privacy by design' and 'privacy by default' (*supra* 104),[720] nor does it provide for a 'right to know when one's data has been hacked' (*supra* 105). What has been said *supra* 210 can therefore be repeated *mutatis mutandis*.

§6 Accountability issues

213. No overarching accountability principle such as in the GDPR (*supra* 106)[721] can be found in the PSP's. The Verification Principle states that "*organizations must provide follow up procedures for verifying that the attestations and assertions they make about their Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principle*",[722] and asserts that, in the case that the organisation has chosen outside compliance review, "*such a review must demonstrate that* [it] *conforms to the Privacy Shield Principles, that it is being complied with*".[723] Nevertheless, nowhere is the word 'responsible', used in the GDPR, to be found. It is therefore not entirely clear where the burden of proof concerning the compliance of the organisations with the PSP's lies.

§7 The absence of DPIA's and DPO's

214. The PSD makes no reference at all to DPIA's[724] and only to something more or less comparable to DPO's in the context of data processing not falling under the PSP's. What has been said *supra* 210 can, again, be repeated *mutatis mutandis*.

---

[717] Annex II, II.4.a PSD.
[718] Some minor criticisms can be articulated concerning this principle. The principle states that "*Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data*." The use of the word 'reasonable' and the phrase 'taking into due account the risks involved in the processing and the nature of the personal data' is questionable.
[719] Article 5(1)(f) GDPR.
[720] WP29 on the PSD, 15.
[721] Article 5(2) GDPR.
[722] Annex II, III.7.a PSD.
[723] *Ibid*., Annex II, III.7.d.
[724] *Ibid*., Annex II, III.7.d.

§8 Independent oversight and enforcement, Privacy Shield style

215. The GDPR requires the existence of an independent supervisory body with the task of overseeing data protection law. This body must moreover have effective powers to enforce data protection law.[725] Moreover, the existence of such a body is also required by the Charter, leading the CJEU to state that "*the establishment of independent supervisory authorities is thus an essential component of the protection of individuals with regard to the processing of personal data*" (*supra* 72). It is therefore highly likely that the CJEU will closely scrutinise the existence of the such bodies/authorities.

216. As explained above (*supra* 147), these supervisory bodies must have a seven layered independence. It seems that, in the constellation established by the PSP's, the role of the supervisory body will be 'played' mainly by the FTC,[726] and, to a lesser extent, the Department of Commerce ('DoC')[727] and the Department of Transportation ('DoT').[728]

217. From the outset, it is clear that both the DoC and the DoT are not independent, as they are integral parts of the executive branch of government. Consequently, no *independent* supervisory body exists in the context of data protection by airlines and ticket agents, since the body responsible for oversight on these organisations is the DoT.[729] Thus, no independent supervision exists concerning PNR data, a situation already declared unacceptable by the CJEU in *PNR Canada*.[730]

[725] See in this context *supra* 153-156.
[726] Recitals 18, 26, 30, 35-36, 40-41, 54-55, annex II, III,11.f. and annex IV PSD.
[727] Recitals 18, 30-37, 46, 49, 52-53, 62, 138, article 1(3), annex I, 1 and annex II, I. PSD. Concerning the DoC, the WP29 noted, that "*the Privacy Shield role of the DoC in the certification process appears to be reduced to a mere checking of completeness of documents. Although the WP29 acknowledges that self-certification does not imply a systematic a priori check of the implementation of the privacy policies, the DoC should at the very least commit to systematically check that privacy policies include all Privacy Shield principles. Such commitment is mentioned in the draft adequacy decision but cannot not be clearly identified in the representation letter of the DoC*", see WP29 on the PSD, 15.
[728] Recitals 18, 26, 30, 35-36, 40 and annex V PSD.
[729] Annex V, I.A., first paragraph j° annex IV, I.A., second paragraph PSD.
[730] *Supra* 72.

218. Whether the FTC can be regarded as 'independent' is less clear-cut. At least in the U.S. itself, the FTC is considered to be an independent agency.[731] On this side of the Atlantic, the opposite is contended.[732] In any case, no finding of the Commission concerning the independence of the FTC can be found in the PSD. A quick look at the Federal Trade Commission Act already indicates that the FTC will probably not pass the test of independence by the CJEU, since the FTC lacks financial (a separate budget), and organisational independence.[733] Moreover, the FTC is subject to oversight by several congressional committees, meaning those committees can exercise influence over the FTC.[734] Besides the problems regarding the independence of the FTC, the WP29 voiced concern about the enforcement powers of that body. The WP29 doubted whether these powers are "*sufficient to meet the CJEU's requirement of effective detection and supervision mechanisms of infringement*", thereby explicitly questioning whether the FTC has the power "*to conduct on-site inspections on the premises of self-certified organisations to investigate Privacy Shield violations*" and whether "*the sanctions under the Privacy Shield are deterrent in practice*".[735] Indeed, the PSD does not include any findings concerning the power of the FTC to fine organisations for violating the PSP's, let alone that it includes findings on whether the fines are sufficiently deterrent, or essentially equivalent to the fines in the GDPR (*supra* 163). Similar concerns about the FTC were voiced by AG Bot in *Schrems* (*supra* 46).[736]

219. To conclude, no independent supervisory body as required by the Charter and the GDPR exists in the U.S. (or at least this is not established by the PSD) to monitor the PSP's. Therefore, the essence of article 8(3) of the Charter is not respected and no essentially equivalent protection as required by the GDPR exists on this point.

---

[731] C. J. HOOFNAGLE, *Federal Trade Commission: Privacy Law and Policy*, New York, Cambridge University Press, 2016, 83; see also <https://www.usa.gov/independent-agencies>.
[732] C. CHEVALLIER-GOVERS, "Personal Data Protection: Confrontation between the European Union and the United States of America" in Y. ECHINARD and others (eds), *L'Union européenne et les Etats-Unis : processus, politiques et projets*, Bruxelles, Larcier, 150.
[733] 15 U.S.C. §42 *in fine*. This section provides that "*The commission* […] *shall have authority to employ and fix the compensation of such attorneys, special experts, examiners, clerks, and other employees as it may from time to time find necessary for the proper performance of its duties and as may be from time to time appropriated for by Congress*." The phrase 'may be from time to time appropriated for by Congress' is problematic in the light of the requirement of organisational and financial independence.
[734] C. J. HOOFNAGLE, *Federal Trade Commission: Privacy Law and Policy*, New York, Cambridge University Press, 2016, 96.
[735] WP29 on the PSD, 30.
[736] Opinion of AG Bot *Schrems*.

§9 Problems regarding redress and the right to effective judicial protection

220. The PSD provides for all sorts of redress. However, as the WP29 has argued, there is a lack of clarity about the overall architecture of the framework, making it very complex. For example, according to the recitals, the data subject may pursue cases of non-compliance with the PSP's through direct contacts with the involved organisation, which is then obliged to provide a response.[737] To this purpose, the organisations must put in place 'an effective redress mechanism'. Nowhere in the PSP's is such 'redress mechanism' to be found. What can be found is that organisations must provide for 'independent recourse mechanisms'.[738] However, this seems more to correspond with the second form of redress, the 'independent resolution body'.[739]

221. The other forms of redress include one which involves the DPA's, however this form of redress is only applicable to human resources data and when the organisations have voluntarily signed up to this[740]. According to the Commission, there are also 'redresses' which involve the DoC and the FTC.[741] Additionally, there is a 'Privacy Shield Panel', which is a form of binding arbitration.[742] This panel has no authority to provide monetary relief,[743] will be located in the USA[744], the language of the arbitration will be English[745] and no EU (or Member State) authority may participate in the arbitrations.[746] Lastly, "*additional venues for judicial redress may be available under the law of the U.S. States*".[747]

---

[737] Recitals 43-44 PSD.
[738] Annex II, II.7.a. PSD. Complaints are investigated by this body at no cost for the data subject and must be able to impose 'sufficiently rigorous sanctions'.
[739] Recitals 45-47 PSD.
[740] Recitals 48-51, annex II, III.5., annex II, III.9.d. PSD.
[741] Recitals 52-53 and 54-55 PSD respectively. The WP29 in this context states "*Alternatively, complaints could be directly made with the Federal Trade Commission, even if there is no duty for the FTC to deal with them. A DPA could also refer a complaint and the DoC has committed to review and undertake best efforts to facilitate resolution of complaints (Annex I) which will be given 'priority consideration' by the Federal Trade Commission (Annex II, III.7.e). However, the prioritisation of complaints by the FTC does not give any certainty to the data subject that its complaints will be dealt with*." The WP29 is thus quite sceptical, to say the least. See WP29 on the PSD, 29.
[742] Recitals 56-58, Annex I, 2, I. PSD.
[743] Annex I, 2, I.B. PSD.
[744] Annex I, 2, I.G.5. PSD. Video or telephone participation will be provided at no cost and in-person participation is not required.
[745] Annex I, 2, I.G.6. PSD. Interpretation and translation will be provided at no cost.
[746] Annex I, 2, I.G.4. PSD. DPA's may assist only in the preparation of the notice to initiate the binding arbitration.
[747] Recital 59 PSD. It is self-evident that the word 'may' is not very reassuring in this context.

222. Two general remarks can be made concerning these forms of redress. Firstly, the complexity is such that it risks impairing the effective use of the several forms of redress by EU data subjects.[748] Secondly, as eloquently stated by the WP29, "*the quality of redress mechanism* [sic] *should prevail over the quantity of mechanisms available to the EU individuals*".[749] More seriously, not one of the forms of redress grants a true 'essentially equivalent' right to an effective judicial remedy (or 'effective judicial protection'). Indeed, under the GDPR, data subjects have the right to initiate proceedings before a *court* (*supra* 160). All forms of redress, safe for the Privacy Shield Panel, cannot even remotely be considered to include a court. The Privacy Shield Panel is still no court, and access to that panel is limited, as are its powers. Furthermore, there is no guarantee whatsoever that data subjects can bring claims for damages before the U.S. courts. And even if it were, as the GDPR grants data subjects the right to initiate proceedings where the data subject has his or her habitual residence, it is still not clear this would constitute essentially equivalent protection. Indeed, the WP29 has also already recommended that EU data subjects "*should be "able to bring claims for damages in the European Union" as well as be "granted the right to lodge a claim before a competent EU national court'*"".[750] Therefore, the essence of article 47 of the Charter is not respected and no essentially equivalent protection exists on this point.

§10 Intermediary conclusion

223. Not a single 'right of the data subject' as established by the GDPR can be detected in an 'essentially equivalent' form in the PSP's. The same can be said about several key principles. No essentially equivalent oversight by an independent supervisory authority of the PSP's can be found in the PSD. Several other layers of protection such as DPIA's are lacking. The remedies provided by the PSD concerning non-compliance with the PSP's are not essentially equivalent to those in the GDPR either. On top of this, this can also lead to possible, non-justifiable, infringements of article 8(1), (2) and (3), 21, 47 of the Charter. The PSP's therefore do not ensure an essentially equivalent, and therefore adequate, level protection.

[748] WP29 on the PSD, 3.
[749] WP29 on the PSD, 26.
[750] WP29 on the PSD, 27.

Subsection 2: The national security derogation to the Privacy Shield Principles

224. The PSD contains several exemptions from the PSP's.[751] It states that adherence to the PSP's may be limited for reasons of national security, public interest, law enforcement, or by statute, government regulation or case law which creates conflicting obligations or explicit authorisations.[752] Where these derogations apply, U.S. law itself should offer the level of protection required under EU law. In this subsection, the derogation concerning national security will be analysed. Other derogations will not be discussed.

225. As a preliminary note, it must be acknowledged that the PSD now at least discusses the possible access by security services for purposes of national security to personal data processed under the Privacy Shield, limitations on that access and possible legal redress against that access.[753] Indeed, the complete lack of findings by the Commission concerning these issues was a major point of criticism in *Schrems* (*supra* 40).[754] However, whilst the PSD indeed includes a *description* of the protections offered under U.S. law, it never assesses whether the protection is essentially equivalent with that offered by the EU.[755,756]

§1 Interferences with the right to a private life and the right to protection of personal data

226. As the derogation for national security allows deviations from the PSP's, and therefore of data protection law, it is self-evident that that derogation constitutes an interference with the right to protection of personal data. Additionally, when one keeps the case law of the CJEU in mind (*supra* 21, 28, 39 and 57), there is an interference with the right to a private life. Hereafter, it will be assessed whether these interferences can be justified, *i.e.* whether they are 'provided by law', respect the essence of the rights concerned, are proportionate and strictly necessary. Since it is clear that 'national security' is an objective of general interest, that condition will not be discussed.

---

[751] Annex II, I.5. PSD.
[752] *Ibid*. See also WP29 on the PSD, 17.
[753] Recitals 67-124 PSD; WP29 on the PSD, 4.
[754] Judgment *Schrems*, paras 88-99.
[755] Concerning the question to what exactly U.S. law should be essentially equivalent to, *supra* 179-182.
[756] The only time the words 'essentially equivalent' are used in this context, they are used to point out that the protection offered by the U.S. should not be identical. See recital 124, footnote 178.

(a) Vague concepts and inconsistent terminology, is the derogation for national security 'provided by law' as interpreted by the CJEU?

227. According to the Charter, all processing of personal should be based on a legal basis, *i.e.* the processing should be 'provided for by law'.[757] In *PNR Canada*, the CJEU clarified that legislation must define in a clear and precise manner which personal data is to be processed, for which purposes the data is processed and lay down the substantive and procedural conditions governing the use of collected personal data (*supra* 60).[758] Moreover, the CJEU is quite strict in its assessment whether provisions are 'clear and precise'.[759]

228. Several legal bases for processing of personal data for national security purposes (hereinafter called 'surveillance') exist in the USA. All bases can potentially be used for processing of both metadata and content of communications. Only the following ones will be analysed: Section 104, Section 501 and Section 702 of the Foreign Intelligence Surveillance Act ('FISA')[760] and Executive Order 12333 ('EO12333').[761] Another legal instrument, the Presidential Policy Directive 28 ('PPD-28'),[762] prescribes the limits of 'signals intelligence' ('sigint') (*infra* 233), no matter which legal basis is used and where data was obtained, but is in itself not a legal basis for surveillance.[763] PPD-28 will also be examined.

229. Section 104 FISA is probably the least problematic legal basis. It requires security services to obtain a court order from the FISC[764] on an individualised basis[765] to be able to conduct (electronic) surveillance. The section describes in quite great detail which elements the application for such a court order must contain.[766] However, some terms used are defined in a very broad

[757] As any processing of personal data is considered to interfere with the right to protection of personal data, article 52(1) Charter is applicable.
[758] Opinion *PNR Canada*, para 155, 192.
[759] See *supra* 60 for several terms which were deemed too broad.
[760] 50 U.S.C. §1804, 50 U.S.C. §1861 and 50 U.S.C. §1881a.
[761] Executive Order 12333 of 8 December 1981 on the United States Intelligence Activities, *Federal Register* Vol. 40, No 235 (hereinafter: 'EO12333').
[762] Presidential Policy Directive 28 of 17 January 2014 regarding Signals Intelligence Activities (hereinafter: 'PPD-28').
[763] WP29 on the PSD, 35.
[764] 50 U.S.C. §1804(a).
[765] 50 U.S.C. §1804(a)(2).
[766] 50 U.S.C. §1804(a).

way.[767] For example, "*a significant purpose of the surveillance* [must be] *to obtain foreign intelligence information*".[768] 'Foreign intelligence information' is defined as containing five specific categories of information, one of which is 'information with respect to a foreign power or foreign territory that relates to the conduct of the foreign affairs of the United States'.[769] It is doubtful whether the CJEU would accept such a definition in the light of its case law in *PNR Canada*, since it is not very 'clear and precise' which data will be processed. As this definition is also applicable to the other sections of the FISA (*infra* 230-231), those sections are also affected.

230. Section 501 FISA permits the Federal Bureau of Investigation ('FBI') to make an application to the FISC for a court order requiring "*the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information*" from a business or other entity.[770] As the definition of 'tangible things' includes 'other items', resembling the term 'etc', which was not considered acceptable by the CJEU in *PNR Canada* (*supra* 60), it unlikely that this definition will be accepted by the CJEU.[771]

231. Section 702 FISA permits surveillance, after annual approval by the FISC, by targeting non-US persons reasonably believed to be located outside the United States, without specifying to the FISC the particular non-US persons who will be targeted, in order to acquire foreign intelligence information.[772] Moreover, it is sufficient that a 'significant purpose' of the acquisition is to obtain foreign intelligence information.[773] Section 702 was used in the past for two important surveillance programs: PRISM and UPSTREAM.[774] Section 702 is considerably less detailed than Sections 104 and 501, except for the procedural conditions to get the approval by the FISC. In particular, it is not clear what kind of intelligence operations will exactly happen when the surveillance is approved. Indeed, the most we learn is that there will be 'targeting'.[775] This section of the FISA is therefore the least likely to pass the 'provided by law' test of the CJEU.

---

[767] Judgment High Court (IRL), para 169.
[768] 50 U.S.C. §1804(a)(6)(B). See also *infra* 231 and footnote 773 in regard to problems with 'a significant purpose'.
[769] 50 U.S.C. §1801(e)(2)(B); see also WP29 on the PSD, 36.
[770] 50 U.S.C. §1861(a)(1).
[771] See also WP29 on the PSD, 36.
[772] 50 U.S.C. §1881a(a), (h)(1)(A) j° 50 U.S.C. §1881a(j)(3)(A); see also recital 109 PSD.
[773] 50 U.S.C. §1881a(h)(2)(A)(v). See WP29 on the PSD, 39. This wording leaves doubt whether the purpose is specific enough to pass the test of proportionality.
[774] Recital 81 PSD. To get an insight in these programs, see the said Judgment High Court (IRL), paras 181-186.
[775] 50 U.S.C. §1881a(a)

232. EO12333 is a legal basis for surveillance outside the USA, so, at first sight, one could question its relevancy to assess adequacy of data protection *in* the USA. However, EO12333 can be relied upon for the collection of data in transit *to* the United States.[776] The EO12333 states that "*All means* […] *shall be used to obtain reliable intelligence information to protect the United States and its interests*"[777] and moreover, to quote the words used by the Irish High Court, uses an "*extremely broad definition*"[778] of 'foreign intelligence'.[779] Indeed, these provisions do not define in a clear and precise manner which personal data is to be processed, nor for which purposes they will be processed. This is also reflected in the comments of the WP29 on the EO12333. Notwithstanding the problems with the FISA, the WP29 indeed reserved its most severe criticism for the EO12333. "*The WP29 notes that EO12333 does not provide a lot of detail regarding its geographical scope, the extent to which data can be collected, retained or further disseminated, nor on the nature of offences that may give rise to surveillance or the kind of information that may be collected or used*".[780]

233. As said, PPD-28 places limits on sigint-activities.[781] However, the concept of sigint is not defined in PPD-28, nor in any other applicable text.[782] Therefore, it is not even clear whether the limits of PPD-28 apply to all surveillance. This is again highly problematic in the light of *PNR Canada*. Furthermore, some of the limits imposed on sigint-activities in PPD-28 are in themselves also not very clear and precise. For example, the six purposes for which 'bulk collection' is allowed under PPD-28 are detecting and countering certain activities of foreign powers, counterterrorism, counter-proliferation of weapons of mass destruction, cybersecurity, detecting and countering threats to U.S. or allied armed forces, and combating transnational criminal threats.[783] As the term

---

[776] This means that it is a legal basis "*to collect data from the deep underwater cables on the floor of the Atlantic by means of which data are transferred from the EU to the US for processing within the US before the data arrives within the US*". See Judgment High Court (IRL), para 179.
[777] Article 1.1(a) of the EO12333.
[778] Judgment High Court (IRL), para 178.
[779] See article 3.5(e) of the EO12333, "*Foreign intelligence means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.*"
[780] See also WP29 on the PSD, 35.
[781] Recital 69 PSD.
[782] WP29 on the PSD, 36.
[783] Annex VI, I.b., fifth paragraph PSD; see also G. VERMEULEN, "The Paper Shield: On the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement service" in D. J. B. SVANTESSON and D. KLOZA (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, Cambridge, Intersentia, 2017, 142 (hereinafter: 'VERMEULEN, "The Paper Shield"').

'serious transnational crime' was barely accepted by the CJEU (and not by the AG) in *PNR Canada*, even when this term was defined by reference to domestic Canadian law (*supra* 60), it is doubtful whether 'transnational criminal threats' will be accepted here.

(b) Respecting the essence, proportionality and strict necessity

(1) Individualised surveillance

234. When one applies the case law of the CJEU in *Tele2 Sverige* (*supra* 30) to Section 104 FISA, that section can probably not be considered proportionate. Even though surveillance is limited in respect to the persons concerned[784] and the categories of data and types of communication affected,[785] it is not limited with respect to the retention period. The duration of the surveillance itself is more or less limited,[786] but there is no limit on the retention period of already collected data.

235. Section 501 FISA will probably not pass the proportionality test either. Although there are 'minimization procedures', *i.e.* procedures "*to minimize the retention, and prohibit the dissemination, of nonpublicly available information*", these procedures are not applicable to EU data subjects.[787] The fact that U.S. government officials have stated that the minimisation procedures have *in practice* been extended to all persons[788] should be regarded as irrelevant. Moreover, the minimisation procedures as described in Section 501 FISA, do not include provisions concerning retention periods (safe for one provision which states that in certain circumstances the FISC may require destruction of personal data).[789] Note that in any case, EU law also requires proportionality for the processing of publicly available personal data, and not only to 'nonpublicly available information'.

---

[784] 50 U.S.C. §1804(a)(2).
[785] 50 U.S.C. §1804(a)(5) states that each application shall include "*a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance*".
[786] 50 U.S.C. §1804(a)(9).
[787] 50 U.S.C. §1861(g). These procedures only concern 'unconsenting United States persons'; see also WP29 on the PSD, 38.
[788] See also WP29 on the PSD, 38.
[789] 50 U.S.C. §1861(c)(2)(f)(vii). Footnote 94 of the PSD however states that the retention period is 5 years according to the NSA itself, subject to exceptions, see https://fas.org/irp/nsa/ufa-2016.pdf. Nonetheless, it is not clear whether this retention period is really binding, nor that a retention period of 5 years is proportionate.

(2) 'Bulk' collection of data

236. Whilst Section 104 and Section 501 FISA can be considered to at least respect the essence of the right to the protection of personal data and the right to a private life, the same cannot confidently be said about Section 702 FISA and EO12333, even when read in conjunction with PPD-28. Section 104 and Section 501 FISA are legal bases for individualised surveillance and require a connection between the processed personal data and the objective pursued, as required by the CJEU in *Tele2 Sverige* and *PNR Canada* (*supra* 30, 67-69). Section 702 FISA and EO12333 are legal bases for the bulk collection of data which necessarily implies that this requirement for a connection between the processed personal data on a non-aggregate basis and the objective pursued is absent.

237. First of all, concerning Section 702 FISA, we need to keep in mind that this section is used for non-individualised surveillance of both metadata and content. According to the letter in annex VI of the PSD however, the surveillance allowed under Section 702 FISA is nevertheless "*not 'mass and indiscriminate' but is narrowly focused on the collection of foreign intelligence from individually identified legitimate targets*".[790] The writer of the letter[791] describes certain minimisation procedures, but these procedures principally do not apply to EU data subjects[792] although, according to the letter, some provisions of these minimisation procedures also provide "*substantial protection to information about non-U.S. persons as well*".[793] Two examples are provided: 1) "*communications acquired under Section 702, whether of U.S. persons or non-U.S. persons, are stored in databases with strict access controls*" and 2) "*use of the data is limited to identification of foreign intelligence information or evidence of a crime*".[794] However, neither of these provisions actually ensures that the processing is proportionate and strictly necessary. The first merely ensures data security, the second provision only deals with proportionality concerning the use of the personal data, not the initial collection, which is also a processing operation.[795] In other words, no proportionality in the sense of data minimisation is to be found here.

---

[790] Annex VI, II., first paragraph PSD.
[791] General Counsil Robert Litt from the Office of the Director of National Intelligence ('ODNI').
[792] 50 U.S.C. §1881a(e)(1) j° 50 U.S.C. §1801(h).
[793] Annex VI, II., fourth paragraph PSD.
[794] *Ibid*., annex VI, II., sixth paragraph.
[795] See in this context also VERMEULEN, "The Paper Shield", 138, 141-142.

238. Concerning retention periods in the context of surveillance programs based on Section 702 FISA, the PSD states that "*metadata and unevaluated content for PRISM is retained for no more than five years, whereas UPSTREAM data is retained for no more than two years*".[796] This is again highly problematic in the light of the case law of the CJEU, especially in *Digital Rights Ireland* (a judgment about the retention of metadata, *supra* 27). In that case, the CJEU criticised the DRD for failing to make a distinction between the categories of data on the basis of their possible usefulness for the purposes of the objective, instead retaining the data indiscriminately. As the PSD states that "*the NSA complies with these storage limits through an automated process that deletes collected data at the end of the respective retention period*", it is unlikely that this will satisfy the CJEU. Indeed, *automated* processes that delete collected data *at the end* of the respective retention period (be it five or two years) are likely to be considered indiscriminate.

239. In confirmation of the above, the Irish High Court comes to the following conclusion concerning Section 702 FISA: "*on the basis of* [the definition in Directive 95/46] *and the evidence in relation to the operation of the PRISM and Upstream programmes authorised under s. 702 of FISA, it is clear that there is mass indiscriminate processing of data by the Unites States government agencies, whether this is described as mass or targeted surveillance*".[797]

239. The PSD barely mentions any provisions contained in EO12333 which could potentially create some proportionality at initial collection stage. It only states that 'the least intrusive collection techniques' shall be used[798] and that the collected information must respond to 'intelligence priorities set by the President'.[799]

[796] Footnote 94 PSD.
[797] Judgment High Court (IRL), para 193.
[798] Footnote 69 PSD. However, even this provision only addresses subsidiarity and not proportionality or strict necessity. See in this context VERMEULEN, "The Paper Shield", 146.
[799] Footnote 76 PSD. These 'intelligence priorities set by the President' are also problematic when assessed in the light of the 'provided by law' condition.

240. PPD-28 however is designed to compensate for the lack of proportionality on the part of EO12333. It states that sigint-activities shall be 'as tailored as feasible'.[800] Nevertheless, 'as tailored as feasible' is not the same as 'proportional' and certainly not the same as 'strictly necessary'.[801] The WP29 rightly considered that processing that is 'as tailored as feasible', can still be considered to be massive.[802] In addition, as said *supra* 233, PPD-28 permits bulk collection[803] for six purposes. In annex VI of the PSD, it is alleged that the "*intelligence community must collect bulk signals intelligence in certain circumstances in order to identify new or emerging threats and other vital national security information that is often hidden within the large and complex system of modern global communications*",[804] which seems to imply that, at least to the mind of the USA and the Commission, this bulk collection is necessary. Still according to Annex VI, bulk collection does not amount to 'indiscriminate' surveillance,[805] as policies "*should require that wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants*".[806] As stated by VERMEULEN, "*there is a little too much of 'should' in this sentence for it to be genuinely convincing*".[807] The use of the words 'wherever practicable' is likewise not really reassuring.[808] It is implied that this bulk collection is not 'mass' surveillance either, since "*any bulk collection activities regarding internet communications* […] *operate on a small proportion* [sic] *of the internet*".[809] This is in turn contested by the WP29, which basically argues that, even if true,[810] this statement is meaningless, since "'*"communications data make up a very small part of global internet traffic", given that the "vast majority of global internet traffic consists of high-volume streaming and downloads such as television series, films and sports"*'".[811]

---

[800] PPD-28, section 1(d).
[801] WP29 on the PSD, 38.
[802] *Ibid*., 40.
[803] "*References to signals intelligence collected in "bulk" mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)*", see PPD-28, footnote 5.
[804] Annex VI, I.b., third paragraph PSD.
[805] *Ibid*., annex VI, I.b., fourteenth (last) paragraph.
[806] *Ibid*., annex VI, I.b., second paragraph. See also recital 70 PSD.
[807] VERMEULEN, "The Paper Shield", 138, 141.
[808] *Ibid*.
[809] Annex VI, I.b., seventh paragraph PSD.
[810] The WP29 indeed states in this regard that it "would appreciate further evidence".
[811] WP29 on the PSD, 38, footnote 47. See in this context also L. MOEREL, "De betekenis van de Safe Harbor uitspraak van het Europese Hof voor datadoorgiftes naar de VS", *Nederlands juristenblad* 2016, (1174) 1176.

240. The PSD also claims that PPD-28 provides for limitations on the retention of collected data concerning EU data subjects (*i.a.* on the basis of EO12333).[812] PPD-28 indeed states that the protection concerning retention periods offered to U.S. persons by EO12333 is extended to non-U.S. persons.[813] However, the protection offered by EO12333 to U.S. persons is in itself very meagre. Under EO12333, the retention of certain data is allowed for an unlimited period of time as long as it can be qualified as a certain type of information.[814] All of the types of information on the list of types of information for which there is no retention limit are very broadly construed, e.g. "*incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws*".[815] PPD-28 states that if *no* determination is made that the data qualify as such a type of information, that data may not be retained for more than five years, *unless* it is determined that continued retention is "*in the national security interests of the United States*".[816] In other words, all collected data may be retained for up to five years, data belonging to some (vague) categories may be retained forever and data, even when it cannot be considered as belonging to these categories, may still be retained forever on the basis of an even more vague purpose. No need to despair according to the Commission though, "*information about a person may not be disseminated solely because an individual is a non-U.S. person*" and "*signals intelligence about the routine activities of a foreign person would not be considered foreign intelligence that could be disseminated or retained permanently by virtue of that fact alone*".[817,818] Yet again, this is almost impossible to reconcile with the case law of the CJEU. The limitless retention of some data on vague criteria is certainly disproportionate, and almost *ipso facto* compromising the essence of the right to protection of personal data, no matter how insignificant the retained data are. Considering the case law of the CJEU in *Digital Rights Ireland* (*supra* 22), it is likely that this in addition unjustifiably infringes the right to freedom of expression.

---

[812] Annex VI, I.a., second paragraph, fifth indent and Annex VI, I.c. PSD.
[813] Section 4(a)(i), second indent PPD-28.
[814] Section 2.3. EO12333.
[815] *Ibid*., Section 2.3.(i).
[816] Recital 86, annex VI, I.c. first and second paragraph PSD and Section 4(a)(i), second indent PPD-28.
[817] Recital 87, annex VI, I.c. third paragraph PSD.
[818] The opposite would be especially grave. To paraphrase one author, who used the words 'Whoopty doo' concerning the prohibition on industrial espionage in the PSD, one could here use the words 'yippie ya yay'. See G. VERMEULEN, "The Paper Shield: On the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement service", 2016, 8, accessed on 1 May 2019 via https://biblio.ugent.be/publication/8110845/file/8110875.

241. When one combines the fact that Section 702 FISA and EO12333 are not only used for the processing of metadata, but also for processing of content of communications, with the lack of proportionality of both legal instruments, both at the initial collection stage as in the further retention period, and with the case law of the CJEU in *Digital Rights Ireland* and *Schrems*, it is hard to escape the conclusion that Section 702 compromises the essence of the right to protection of personal data and the right to a private life, regardless of the 'limitations' placed on both instruments by PPD-28. Even if the CJEU would consider that the essence of both rights is respected, it is almost certain that it will be of the opinion that proportionality and strict necessity are not. The WP29 likewise states that "*massive and indiscriminate surveillance of individuals can never be considered as proportionate and strictly necessary in a democratic society*".[819] It is therefore likely that the CJEU will annul the PSD on this ground, essentially coming to the same conclusion as in *Schrems* about the SHD (*supra* 42).

§2 Right of access and right to rectification

242. In *Schrems*, AG Bot criticised the SHD for failing to make findings regarding opportunities for EU data subjects to obtain access to or rectification or erasure of data in the context U.S. surveillance programmes (*supra* 47). The PSD does make some findings concerning this issue, at least ensuring that the essence the right of access, enshrined in article 8(2) of the Charter, is probably not compromised. The PSD indeed includes findings concerning the Freedom of Information Act ('FOIA'),[820] on the basis of which EU data subjects can ask access to any agency record including personal data relating to that data subject.[821] It must be noted however that when a FOIA request concerns information classified for national security reasons, it is unlikely that it will be successful.[822] In any case, nowhere in the PSD is anything to be found regarding the right to rectification, equally enshrined in article 8(2) of the Charter, in the context of surveillance. To the extent that judicial remedies can remedy these shortcomings, they will be examined *infra* 254-264.

---

[819] WP29 on the PSD, 4.
[820] Recitals 111, 114, 130, 133, Annex III, Annex A, 5. and Annex VI, V., third paragraph PSD. See also recitals 124 and 139 PSD, where the Commission seems satisfied with these findings.
[821] Recital 133 PSD; WP29 on the PSD, 44.
[822] WP29 on the PSD, 44. See also footnote 196 of the PSD, which includes several grounds to reject FOIA requests, some of which are extremely broadly construed.

§3 Problems with sensitive data and non-discrimination

243. The PSD contains no findings of the Commission, and only one statement of a U.S. agency, concerning the processing of sensitive data in the context of surveillance. However, sensitive data of EU data subjects *are* processed under surveillance programs such as PRISM and UPSTREAM. Indeed, when one keeps in mind that the CJEU considered that even PNR data may provide sensitive information about air passengers (*supra* 57), then one cannot reasonably argue that surveillance of the kind allowed under Section 702 FISA and EO12333 will not process sensitive data.

244. The CJEU further considered in *PNR Canada* that measures based on the premise that sensitive data may in itself be relevant to security purposes, regardless of the conduct of the individuals involved, would infringe article 7 and 8, read in conjunction with article 21 of the Charter (*supra* 73).[823] On that basis alone, it already concluded that transfer of PNR data to Canada is not allowed under the Charter.[824] Nonetheless, nowhere it is stated that such measures are not allowed in the USA. As said, only one statement of a U.S. agency is provided in this regard: "*The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion*".[825] The opposite would be truly shocking. As no safeguards at all are provided, one could argue the PSD compromises the essence of the principle of non-discrimination enshrined in article 21 of the Charter.

§4 Independent oversight on surveillance activities à l'américaine

245. An independent supervisory authority should exist in the context of surveillance, as the existence of such a body is not only required by the GDPR, but also by article 8(3) of the Charter. It must be recognised that the PSD offers more protection on this point than the SHD. Indeed, whereas the SHD did not contain any findings concerning this issue, the PSD does.[826]

---

[823] Opinion *PNR Canada*, para 165.
[824] *Ibid*., paras 167, 172.
[825] Section 1(b) PPD-28. See Annex VI, I.a, second paragraph, third indent PSD.
[826] Recitals 65, 91-110, 116-122, Annex III, Annex VI, I.d., Annex VI, letter to Mr Antonipillai and Mr Dean, sixth paragraph PSD.

(a) Internal oversight

246. The USA does not have one single supervisory body tasked to surveillance programmes.[827] Rather, there is multi-layered oversight, both internal and external.[828] While the presence of internal oversight bodies, such as 'Inspectors-Generals' and 'Privacy and Civil Liberty Officers',[829] is by no means a negative point, it is not sufficient either. Indeed, no matter how many times the PSD repeats that these bodies are independent,[830] as no evidence is presented that they actually meet all requirements to be considered independent, they cannot be considered as such. For example, nowhere is anything to be found about freedom from conflicts of interest of the Inspectors-Generals (*supra* 147). Moreover, the PSD itself states that the Inspector-Generals "*can only be removed by the President*" and that "*while the U.S. Constitution requires that the President have IG removal authority, it has rarely been exercised*".[831] It is questionable whether these statements will persuade the CJEU that the Inspectors-Generals enjoy functional independence, given its case law concerning 'prior compliance' (*supra* 150-151). Therefore, the WP29 rightly considered that these bodies cannot "*meet the required level of independence to act as independent supervisor*".[832] In any case, the Inspectors-General do not have any obligation to look at every complaint they receive, they rather have a discretionary power to assess complaints.[833] One could therefore also question whether their supervision tasks are defined broadly enough.

(b) External oversight

247. External oversight consists of oversight by Congressional Committees, judicial oversight by the FISC, and oversight by the Privacy and Civil Liberties Oversight Board ('PCLOB').[834]

248. The oversight by Congressional Committees cannot be equated with the existence of an independent supervisory authority. To compare the two is to compare apples with oranges. In any

[827] WP29 on the PSD, 40.
[828] *Ibid.*
[829] See recitals 93-101 PSD for an exhaustive list.
[830] Concerning e.g. the Inspectors-General, see recitals 97, 120, Annex III, Annex A, 6.a., Annex VI, I.d., first paragraph, second indent, Annex VI, II., seventh paragraph, Annex VI, letter to Mr Antonipillai and Mr Dean, twelfth, thirteenth and fourteenth paragraph PSD.
[831] Annex VI, letter to Mr Antonipillai and Mr Dean, thirteenth paragraph PSD.
[832] WP29 on the PSD, 41.
[833] *Ibid.*, 44.
[834] *Ibid.*, 44.

way, the WP29 questions the ability of these committees to even discuss the processing of personal data of individuals, especially of non-U.S. persons.[835]

249. The FISC is a judicial body, therefore it can be considered to be independent. However, it is harder to qualify it as a supervisory authority that can ensure effective oversight.[836] For example, surveillance on the basis of Section 702 FISA is subject to oversight *ex ante*, but not *ex post*.[837] In other words, the FISC does not truly enforces data protection law like its counterparts, the DPA's, do in the EU. They merely allow surveillance programs to go through (*supra* 231), without monitoring these programs afterwards.

250. The PCLOB probably comes closest to an actual independent supervisory authority. The tasks and powers of the PCLOB seem to be comparable to those of independent supervisory authorities in the EU.[838] The WP29 has in this context stated that the "*PCLOB has demonstrated its independent powers by disagreeing with the President of the United States on legal issues*".[839] However, the PSD does not present any evidence concerning all aspects of independence as required by the CJEU. For example, no findings are made concerning its financial independence or its ability to independently select its own staff (*supra* 147). It is again questionable whether the CJEU will accept that the PCLOB is independent simply because it is stated that it is, without any further findings.[840]

251. Regardless of anything said *supra* 245-250, one substantial gap in oversight remains. That is, there is no oversight whatsoever of surveillance on the basis of EO12333.[841] This is obviously highly problematic and will almost certainly not be accepted by the CJEU, as this imperils the essence of article 8(3) of the Charter.

---

[835] *Ibid*., 42.
[836] *Ibid*., 43.
[837] 50 U.S.C. §1861(h)(6) j° 50 U.S.C. §1861(j)(1)(A). See also WP29 on the PSD, 41.
[838] Recital 98, Annex VI, I.d., first paragraph, fourth indent and Annex VI, letter to Mr Antonipillai and Mr Dean, seventh to eleventh paragraph PSD. See also WP29 on the PSD, 42.
[839] WP29 on the PSD, 42.
[840] The WP29 nevertheless seems to accept that the PCLOB is independent, given its statement that "*The WP29, however, is concerned that there is insufficient oversight of the surveillance programmes undertaken on the basis of EO12333*". This seems to imply that, *a contrario*, oversight by PCLOB of surveillance on the basis of FISA is sufficient, see WP29 on the PSD, 43.
[841] WP29 on the PSD, 42-43.

§5 The right to effective judicial protection

252. In *Schrems*, the CJEU ruled that the SHD did not respect the essence of the right to effective judicial protection in article 47 of the Charter (*supra* 48). The SHD did not contain any findings regarding the judicial review of surveillance. The PSD does contain findings of the Commission and statements of the U.S. government concerning this issue[842] and establishes a new redress mechanism: the Privacy Shield Ombudsperson ('Ombudsperson').[843]

(a) Judicial protection by 'normal' courts

253. The PSD mentions several legal bases that EU data subjects could use to seek legal recourse before ordinary courts against government officials for unlawful surveillance.[844] However, as admitted by the PSD itself, all these legal bases concern particular factual situations and are available under certain conditions such as intentional violation of data protection law.[845] Useful as they may be in those particular situations, they can thus not provide for effective judicial protection in every situation in which there has been an unjustifiable interference with the right to protection of personal data of an EU data subject.[846]

254. EU data subjects could also initiate legal proceedings before ordinary courts on a more general basis: the Privacy Act, read in conjunction with the Judicial Redress Act. The Privacy Act allows US citizens to access personal data held by governmental agencies and to review those records.[847] The Judicial Redress Act in its turn extends the protections of the Privacy Act concerning certain agencies in respect of covered countries.[848] All EU member states, safe for the United Kingdom and Denmark, are covered countries.[849] However, both the Privacy Act and the

[842] Recitals 111-124, Annex VI, V. PSD.
[843] *Ibid*., recitals 65, 116-122, 124, Annex III and Annex III, Annex A.
[844] For example, the Computer Fraud and Abuse Act or the Right to Financial Privacy Act. Recital 113 PSD.
[845] Recital 113 PSD. See also Judgment High Court (IRL), paras 38, 170-186. Paragraphs 170-197 are used twice in this judgment, to the extent references are made to any paragraph between 170 and 197 under the title 'The right to effective judicial protection', the second time this paragraph is used in the judgment is meant, except otherwise indicated.
[846] Judgment High Court (IRL), para 38.
[847] *Ibid*., para 187. See 5 U.S.C. §552a(d)(1).
[848] Judgment High Court (IRL), para 190.
[849] As of May 2019, see Attorney General Order No. 3824–2017 of 23 January 2017 on the Judicial Redress Act of 2015: Attorney General Designations, *Federal Register*, Vol. 82, No. 13.

Judicial Redress Act contain stumbling blocks.[850] There are regulations prohibiting the disclosure of records relating to the functions and activities of the NSA in the context of the Privacy Act[851] and the NSA is not a designated agency in the context of the Judicial Redress Act.[852] Therefore, EU data subjects cannot initiate legal proceedings against the NSA on this basis.[853] As the NSA is the operator of surveillance programs such as PRISM and UPSTREAM, these limitations for all practical purposes have as a result that there is a wide gap concerning effective judicial protection against surveillance on this basis.[854]

255. The PSD also mentions the Administrative Procedure Act.[855] Besides questions relating to the scope of this act, it is sufficient to say that no damages can be awarded under it.[856] It is therefore doubtful whether this act can offer *effective* judicial *remedies*.

256. The Fourth Amendment to the U.S. Constitution, considered to offer protection against unlawful government surveillance, cannot be relied upon by most EU data subjects either.[857] Indeed, non-US citizens[858] "*lacking substantial voluntary connection with the USA*" may not bring a Fourth Amendment case.[859] The PSD states that EU data subjects may nevertheless 'benefit indirectly' from the protections guaranteed by the Fourth Amendment.[860] Be that as it may, that is not sufficient to constitute an effective judicial remedy.

257. Furthermore, to be able to initiate judicial proceedings on any of these legal bases, all individuals, including the EU data subjects, need to demonstrate 'standing'.[861] In practice, this means that 'concrete, particularised, and actual or imminent or injury' must be demonstrated.[862] It is extremely hard to conceive how someone could demonstrate this kind of injury, since the very

[850] WP29 on the PSD, 43.
[851] Judgment High Court (IRL), para 187.
[852] *Ibid*., para 190.
[853] *Ibid*., para 190.
[854] *Ibid*., para 187.
[855] Recital 113 PSD. See 5 U.S.C. §702.
[856] Judgment High Court (IRL), para 196.
[857] *Ibid*., first para 197.
[858] *Ibid*., first para 197 refers to 'non-*EU* citizens', this is a lapsus.
[859] *Ibid*., first para 197.
[860] Recital 127 PSD.
[861] WP29 on the PSD, 43, 48; Judgment High Court (IRL), para 197.
[862] WP29 on the PSD, 48. See for a more extensive analysis, Judgment High Court (IRL), para 198 and concerning case law about standing in the context of surveillance, Judgment High Court (IRL), paras 199-213.

purpose of the proceedings might even be to discover whether there is (or has been) any processing of personal data concerning the data subject.[863]

(b) Judicial protection by the FISC

258. The involvement of the FISC in procedures to authorise surveillance is already discussed *supra* 230-231, 235. In the PSD, it is argued that this involvement amounts to oversight by an independent supervisory authority (*supra* 249).[864] However, at the same time, the FISC should play a role in providing an effective judicial remedy. It is hard to predict whether the CJEU will accept such a merger of functions. As there exists an appellate court (the Foreign Intelligence Surveillance Court of Review, or 'FISCR'),[865] and an appeal to the Supreme Court is possible against decisions of the FISCR,[866] it might be argued that the FISC is the independent supervisory authority and the FISCR the body that offers effective judicial protection. Indeed, if the FISC is to be identified as the independent supervisory authority, there need to be possibilities for judicial review of decisions of the FISC.

259. In any case, additional problems exist concerning the FISC (and the FISCR). Already in *Schrems*, AG Bot considered that the nature of proceedings before the FISC is problematic (*supra* 48). The fact that proceedings are secret ('*in camera*') and *ex parte*[867] has as a consequence that it cannot be deemed to offer effective judicial protection. These concerns have not been remedied but only mitigated to a certain extent.[868] The USA Freedom Act has amended FISA and created so-called *amici curiae*.[869] The task of these *amici curiae* is to give optional[870], unbiased advice to the FISC in significant cases or when new legal questions arise.[871] The *amici curiae* argue on the

[863] See in this context WP29 on the PSD, 43-44. The WP29 there states that "*Such requirement* [i.e. the requirement of standing] *appears to be nullified by the lack of notification to individuals subjected to surveillance even after these measures have ended*" and "*nevertheless, as already stated, the plaintiff will have to demonstrate he has standing which will not be possible in practice*".
[864] Recital 105-110 PSD.
[865] 50 U.S.C. §1803(b).
[866] *Ibid.*
[867] 50 U.S.C. §1881a(l)(2).
[868] WP29 on the PSD, 43.
[869] 50 U.S.C. §1803(i)(1).
[870] 50 U.S.C. §1803(i)(4). This section states that amici curiae shall provide legal arguments 'as appropriate'.
[871] 50 U.S.C. §1803(i)(2)(a); WP29 on the PSD, 41, 44.

merits of a case from a privacy and civil rights perspective[872] but do not defend the interest of a specific individual upon request.[873] Therefore one could conclude that the shortcomings to the procedure before the FISC are not fully addressed, as the procedure is still *ex parte* and *in camera* and that the FISC thus cannot ensure effective judicial protection. Furthermore, is not mentioned whether an *amicus curiae* can lodge an appeal against any decision of the FISC to the FISCR. As explained above, the CJEU might conclude that in the current constellation of bodies, the FISCR is to be identified as the body ensuring effective judicial protection and the FISC as the independent supervisory authority. If the CJEU concludes exactly that, one could question whether there is actually any possibility for effective judicial review, regardless of the problems concerning the procedure, since only the U.S. government could appeal against the decisions of the FISC.

(c) 'Judicial' protection by the Ombudsperson?

260. As said, the PSD also introduced a completely new redress mechanism, the Ombudsperson.[874] This mechanism will work as follows. EU individuals first submit a request to a DPA, or another member state or EU body.[875] Next, that body will forward the request to the Ombudsperson after certain checks.[876] The Ombudsperson will then provide a response "*confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executive orders, presidential directives, and agency policies,* […] *have been complied with, or, in the event of non-compliance, such non- compliance has been remedied*".[877] The response will "*neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied*".[878] In practice, the Ombudsperson is an undersecretary, an executive government position, and is thus part of the U.S. administration. As of May 2019, the position is filled by Under Secretary for Economic Growth, Energy, and the Environment, Manisha Singh.[879]

---

[872] 50 U.S.C. §1803(i)(4)(a); WP29 on the PSD, 41.
[873] WP29 on the PSD, 44.
[874] Recitals 65, 116-122, 124, Annex III and Annex III, Annex A PSD.
[875] *Ibid*., Annex III, Annex A, 3.a.
[876] *Ibid*., Annex III, Annex A, 3.a. and b.
[877] *Ibid*., Annex III, Annex A, 4.e.
[878] *Ibid*.
[879] See <https://www.state.gov/r/pa/ei/biog/276185.htm>, accessed on 5 May 2019.

261. As the Ombudsperson is manifestly not a court (or tribunal, to use the terminology of article 47 of the Charter),[880] one could question whether the Ombudsperson can ever be considered to offer 'judicial' protection and be in compliance with article 47 of the Charter.[881] As the WP29 rightly notes, the CJEU has given no indication that the requirements of article 47 of the Charter are to be lowered when an individual seeks judicial protection against surveillance.[882] To the contrary, the CJEU already applied article 47 of the Charter to measures of surveillance.[883] The Ombudsperson is moreover not established by law, as required by the Charter, but by a mere Memorandum.[884] The CJEU might still accept that a body which is not formally a tribunal, nor established by law can still offer effective judicial protection, even though this is highly unlikely. However, in that case, that body would likely still be required to have the core attributes of a tribunal: it should have an adversarial (*inter partes*) procedure which permits individuals to initiate legal proceedings, be fully independent and be able to provide effective remedies.[885]

262. The requirement that the Ombudsperson should have an *inter partes* procedure seems to be met. EU data subjects[886] also do not need to demonstrate that their personal data has in fact been accessed by U.S. government agencies through its sigint activities, eliminating the problems concerning standing.[887]

[880] See e.g. Judgment 31 May 2005, *SYFAIT*, C-53/03, ECLI:EU:C:2005:333, para 29 and Judgment of 31 January 2013, *Belov*, C-394/11, ECLI:EU:C:2013:48, para 38 for criteria whether a body can be considered to be a tribunal or not, according to the CJEU.
[881] WP29 on the PSD, 46.
[882] *Ibid*.
[883] Judgment of 3 September 2008, *Kadi and Al Barakaat*, C-402/05P, ECLI:EU:C:2008:461, para 326; Judgment of 3 December 2009, *Hassan and Ayadi*, C-399/06P, ECLI:EU:C:2009:748, para 73; Judgment of 16 November 2011, *Bank Melli Iran*, C-548/09P, ECLI:EU:C:2011:735, para 105; Judgment of 18 July 2013, *Kadi II*, C-584/10P, ECLI:EU:C:2013:518, para 97. See also WP29 on the PSD, 46.
[884] WP29 on the PSD, 47.
[885] These are the not-*pro-forma*-requirements set by the CJEU to determine whether a body is a tribunal in Judgment 31 May 2005, *SYFAIT*, C-53/03, ECLI:EU:C:2005:333, para 29 and Judgment of 31 January 2013, *Belov*, C-394/11, ECLI:EU:C:2013:48, para 38.
[886] Note that the PSD uses the concept 'EU individual' instead of EU data subject, leading the WP29 to voice concerns regarding the scope of the Ombudsperson mechanism. See Annex III, Annex A, 3.b. PSD and WP29 on the PSD, 46-47.
[887] See Annex III, Annex A, 3. PSD; Judgment High Court (IRL), para 293.

263. Big problems arise however when assessing the independence of the Ombudsperson. Although the PSD states that the Ombudsperson is "*independent from the U.S. Intelligence community*",[888] this is not sufficient. The Ombudsperson should be *independent*, full stop. Indeed, the full statement by then acting U.S. Secretary of State John Kerry is: "*Under Secretary Novelli is independent from the U.S. intelligence community, and reports directly to me*".[889] The last words immediately make clear that the Ombudsperson can never be considered to be truly independent.[890] It is especially troublesome that the PSD does not contain any criteria for the dismissal of the Ombudsperson, which seems to imply that the Ombudsperson can be dismissed at will, as is true for all undersecretaries.[891]

264. Lastly, the Ombudsperson cannot be considered to be able to provide effective remedies. For example, no details are provided whether the Ombudsperson can even access all necessary information to be able to assess whether the data are lawfully processed.[892] In such a situation, it is hard to imagine how the Ombudsperson would be able to provide an effective remedy. Neither can it be concluded that the Ombudsperson can order unlawful obtained data to be erased.[893] Finally, the Ombudsperson must not reveal if there has been any unlawfulness surveillance concerning the complaining data subject.[894] Not even declaratory relief is thus on offer. Because of the stated reasons, the Ombudsperson cannot be considered to offer effective judicial protection.

[888] See Annex III PSD.
[889] See Annex III PSD.
[890] The Irish DPA is also of the opinion that the Ombudsperson is not independent, see Judgment High Court (IRL), para 299. See in this context also VERMEULEN, "The Paper Shield", 145.
[891] WP29 on the PSD, 49.
[892] *Ibid.*, 51.
[893] *Ibid.*, 50-51.
[894] *Ibid.*, 51.

§6 Intermediary conclusion

265. All key problems concerning the derogation for national security existing under the SHD still exist under the PSD. There is still mass, indiscriminate surveillance, notwithstanding the fact that the issue is at least recognised by the PSD. The right of access and the right to rectification are in practice still virtually impossible to enforce. No mention is made of measures to comply with the principle of non-discrimination. There is still no fully-fledged independent supervisory authority. The newly created Ombudsperson cannot be considered to offer effective judicial protection. No other general avenues for judicial redress concerning surveillance truly providing effective judicial protection exist either. It is therefore highly likely that the CJEU will conclude that the PSD, much like the SHD, and regardless to any improvements made to the PSD in comparison with the SHD, does not respect the essence of article 7, 8(1), (2) and (3), 21 and 47 of the Charter. If not, it is almost certain that the CJEU will nevertheless rule that the PSD non-justifiably infringes on these articles, e.g. by not respecting the proportionality and strict necessity principles.

CONCLUSION

266. The PSD is a big improvement in comparison to the SHD on one point: the PSD argues why the U.S. legal framework, as complemented by the PSP's, provides, in the Commission's view, adequate protection. It also gives an, albeit at times chaotic, insight in the U.S. practices concerning surveillance. In that respect, the Commission now at least formally adheres to the requirement set by the CJEU in *Schrems* that it should find, duly stating reasons, that the USA in fact ensures an adequate level of protection. Nonetheless, one could still question whether the assessment is rigorous enough in the light of the new, extensive list of elements the Commission must take account of when taking an adequacy decision under the GDPR.

267. More importantly, the assessment of the Commission itself is highly questionable. The protection offered by the PSP's is not essentially equivalent to the protection offered within the EU, and therefore not adequate in the view of the CJEU. Moreover, the PSP's also seem to non-justifiably infringe several articles of the Charter. Several problems thus exist concerning the compatibility of the PSD with the Charter as well as with the GDPR. Moreover, all substantial problems identified by the CJEU in *Schrems* concerning the SHD, in particular concerning surveillance, still exist with regard to the PSD. Yes, some problems are mitigated to some, albeit limited, extent, but these mitigations cannot be considered to be sufficient. Arguably, the only thing the Commission learned from the *Schrems* judgment is that it should make an assessment concerning the protection in the USA,[895] after which it can declare that the USA ensures an adequate protection, no matter what it finds during the assessment.

268. The most flagrant incompatibilities are mainly situated in the field of the national security derogation. The CJEU will almost certainly qualify the 'bulk collection' of personal data allowed under the PSD as mass, indiscriminate surveillance, which the CJEU has made clear it will not tolerate in the light of the right to protection of personal data, the right to a private life and freedom of expression. The lack of a truly independent supervisory authority, both in the context of the PSP's as in the context of the national security derogation is likely to be a thorn in the flesh

[895] VERMEULEN, "The Paper Shield", 144-145.

of the CJEU as well. Problems also persist in the field of the right to an effective judicial remedy. It is true that the phrase used by the CJEU in *Schrems* that "*legislation not providing for any possibility for an individual to pursue legal remedies does not respect the essence of the fundamental right to effective judicial protection*" is no longer applicable. Still, the possibilities provided constitute a true labyrinth, do not allow effective judicial protection in *all* cases and are hard to exercise in practice, given the requirement of standing. More minor, yet equally problematic, issues exist concerning the rights of the data subject and aspects of several key principles enshrined in the GDPR. Lastly, problems arise concerning the compatibility of the PSD with the principle of non-discrimination. When all these problems are put together, one can indeed state, like Mr. Schrems, that Privacy Shield is Safe Harbour with (a whole bouquet of) flowers on it.

269. Therefore, the likely outcome of the pending cases against the PSD is that the latter will be annulled. To decide otherwise is for the CJEU to make itself vulnerable to harsh criticism from the doctrine and national constitutional courts. The doctrine was already critical to certain aspects of the case law of the CJEU in other data protection cases such as *PNR Canada*, even though in that case, the CJEU did prevent the coming into force of the PNR Agreement with Canada. If the CJEU would give a pass to the PSD, the criticism will inevitably be relentless. However, as one author argues, the EU is economically too interdependent with the US to seriously consider suspending all data transfers.[896] The saga will therefore likely continue with more adequacy decisions, more legal challenges and more preliminary questions to the CJEU.

[896] M. ZALNIERIUTE, "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement", *Mod. Law Rev.* 2018, (1046) 1061.

BIBLIOGRAPHY

Regulation

Primary law of the EU

Treaty on the Functioning of the European Union 2012/C 326/01, *OJ* C326 of 26 October 2012.

Treaty on European Union 2012/C 326/01, *OJ* C326 of 26 October 2012.

Charter of Fundamental Rights of the European Union 2012/C 326/02, *OJ* C 326/391 of 26 October 2012.

International Treaties

Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950.

Acts of the institutions

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* L281/31 of 23 November 1995.

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, *OJ* L215/7 of 25 August 2000.

Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, *OJ* L2/13 of 4 January 2002.

Commission Decision 2003/490/EC of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, *OJ* L168/19 of 5 July 2003.

Commission Decision 2003/821/EC of 21 November 2003 on the adequate protection of personal data in Guernsey, *OJ* L308/27 of 25 November 2003.

Commission Decision 2004/411/EC of 28 April 2004 on the adequate protection of personal data in the Isle of Man, *OJ* L151/48 of 30 April 2004.

Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, *OJ* L235/11 of 6 July 2004.

Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, as amended by Council Regulation (EC) No 1437/2007 of 26 November 2007, and Commission Regulation (EC) No 259/2008 of 18 March 2008 laying down detailed rules for the application of Regulation No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD), *OJ* L209/01 of 11 August 2005.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* L105/54 of 13 April 2006.

Commission Decision 2008/393/EC of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey, *OJ* L138/21 of 28 May 2008.

Commission Decision 2010/146/EU of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data, *OJ* L58/17 of 9 March 2010.

Commission Decision 2010/625/EU of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra, *OJ* L277/27 of 21 October 2010.

Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, *OJ* L27/39 of 1 February 2011.

Commission Implementing Decision 2012/484/EU of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data, *OJ* L227/11 of 28 August 2012.

Commission Implementing Decision 2013/65/EU of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, *OJ* L28/12 of 30 January 2013

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ* L119/1 of 4 May 2016.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ* L119/89 of 4 May 2016.

Commission Implementing Decision 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, *OJ* L207/1 of 1 August 2016.

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, *OJ* L295/39 of 21 November 2018.

Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, *OJ* L76/1 of 19 March 2019.

Proposed acts of the institutions and preparatory documents concerning acts of the institutions

Proposal (Commission) for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11 final of 25 January 2012.

Proposal (Commission) for a Council Decision on the conclusion of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, COM(2013) 0528 final of 18 July 2013.

European Parliament legislative resolution P7_TA(2014)0212 of 12 March 2014 on the proposal for the GDPR and the position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of the GDPR, *OJ* C378/399 of 9 November 2017.

Voting result 2012/0011 (COD) of 8 April 2016 concerning the adoption of the Council's position at first reading and the statement of the Council's reasons concerning the GDPR, ST 7920 2016 INIT, 2012/011 (OLP), 7920/16 of 14 April 2016.

Regulatory Opinions, Guidelines and Communications

Article 29 Working Party, Opinion 03/2013 of 2 April 2013 on purpose limitation, 00569/13/EN WP 203.

Communication from the Commission to the European Parliament pursuant to Article 294(6) of the Treaty on the Functioning of the European Union concerning the position of the Council on the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and repealing Directive 95/46/EC, COM(2016) 214 final, 2012/0011(COD) of 11 April 2016.

Article 29 Working Party, Opinion 01/2016 of 13 April 2016 on the EU – U.S. Privacy Shield draft adequacy decision, 16/EN WP 238.

Article 29 Working Party, Guidelines of 3 October 2017 on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679, 17/EN WP 251.

U.S. law

Title 5, 15 and 50 of the Code of Laws of the United States of America.

Executive Order 12333 of 8 December 1981 on the United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)), *Federal Register* Vol. 40, No 235.

Presidential Policy Directive 28 of 17 January 2014 regarding Signals Intelligence Activities.

Attorney General Order No. 3824–2017 of 23 January 2017 on the Judicial Redress Act of 2015: Attorney General Designations, *Federal Register* Vol. 82, No. 13.

Case law

Judgments and Opinions by the CJEU

Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294.

Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

Judgment 31 May 2005, *SYFAIT*, C-53/03, ECLI:EU:C:2005:333.

Judgment of 30 May 2006, *Parliament v Council and Commission*, C-317/04 and C-318/04, ECLI:EU:C:2006:346.

Judgment of the Court of First Instance of 8 November 2007, *Bavarian Lager v Commission*, T-194/04, ECLI:EU:T:2007:334.

Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54.

Judgment of 3 September 2008, *Kadi and Al Barakaat*, C-402/05P, ECLI:EU:C:2008:461.

Judgment of 16 December 2008, *Huber*, C-524/06, ECLI:EU:C:2008:724.

Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727.

Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293.

Judgment of 3 December 2009, *Hassan and Ayadi*, C-399/06P, ECLI:EU:C:2009:748.

Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125.

Judgment of 29 June 2010, *Commission v Bavarian Lager*, C-28/08P, ECLI:EU:C:2010:378.

Judgment of 9 November 2010, *Volker und Markus*, C-92/09, ECLI:EU:C:2010:662.

Judgment of 16 November 2011, *Bank Melli Iran*, C-548/09P, ECLI:EU:C:2011:735.

Judgment of 24 November 2011, *ASNEF*, C-468/10 and C-469/10, ECLI:EU:C:2011:777.

Judgment of 28 June 2012, *Commission v Éditions Odile Jacob*, C-404/10P, ECLI:EU:C:2012:393.

Judgment of 16 October 2012, *Commission v Austria*, C-614/10, ECLI:EU:C:2012:631.

Judgment of 31 January 2013, *Belov*, C-394/11, ECLI:EU:C:2013:48

Judgment of 30 May 2013, *Worten*, C-342/12, ECLI:EU:C:2013:355.

Judgment of 18 July 2013, *Kadi II*, C-584/10P, ECLI:EU:C:2013:518.

Judgment of 7 November 2013, *IPI*, C-473/12, ECLI:EU:C:2013:715.

Judgment of 12 December 2013, *X*, C-486/12, ECLI:EU:C:2013:836.

Judgment of 8 April 2014, *Commission v Hungary*, C-288/12, ECLI:EU:C:2014:237.

Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger*, C-293/12, ECLI:EU:C:2014:238.

Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317.

Judgment of 17 July 2014, *YS and Others*, C-141/12, ECLI:EU:C:2014:2081.

Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428.

Judgment of 1 October 2015, *Bara and Others*, C-201/14, ECLI:EU:C:2015:638

Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650.

Judgment of the General Court of 3 December 2015, *CN v Parliament*, T-343/13, ECLI:EU:T:2015:926.

Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970.

Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197.

Judgment of the General Court of 28 March 2017, *Deutsche Telekom v Commission*, T-210/15, ECLI:EU:T:2017:224.

Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:336.

Judgment of 18 July 2017, *Commission v Breyer*, C-213/15P, ECLI:EU:C:2017:563.

Opinion of 26 July 2017, *Accord PNR UE-Canada*, Opinion 1/15, ECLI:EU:C:2017:592.

Judgment of 27 September 2017, *Peter Puškár*, C-73/16, ECLI:EU:C:2017:725.

Judgment of 20 December 2017, *Peter Nowak*, C-434/16, ECLI:EU:C:2017:994.

Judgment of the General Court of 5 February 2018, *Edeka-Handelsgesellschaft Hessenring v Commission*, T-611/15, ECLI:EU:T:2018:63.

Judgment of the General Court of 27 February 2018, *CEE Bankwatch Network v Commission*, T-307/16, ECLI:EU:T:2018:97.

Judgment of 5 June 2018, *ULD Schleswig-Holstein v Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388.

Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788.

Judgment of 16 January 2019, *Deutsche Post*, C-496/17, ECLI:EU:C:2019:26.

Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122.

Judgment of 13 March 2019, *AlzChem v Commission*, C-666/17P, ECLI:EU:C:2019:196.

Pending cases before the CJEU

Action brought on 25 October 2016, *La Quadrature du Net and Others* v *Commission*, T-738/16.

Reference for a preliminary ruling from the High Court (Ireland) of 9 May 2018, *Facebook Ireland and Schrems*, C-311/18.

Opinions of the Advocate General

Opinion of Advocate General Kokott of 18 July 2007, *Promusicae*, C-275/06, ECLI:EU:C:2007:454.

Opinion of Advocate General Cruz Villalón of 12 December 2013, *Digital Rights Ireland and Seitlinger,* C-293/12, ECLI:EU:C:2013:845.

Opinion of Advocate General Bot of 23 September 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:627.

Opinion of Advocate General Mengozzi of 8 September 2016, *Accord PNR UE-Canada*, Opinion 1/15, ECLI:EU:C:2016:656.

Opinion of Advocate General Tanchev of 11 April 2019, *Commission v Poland*, C-619/18, ECLI:EU:C:2019:325.

Other case law

High Court of Justice (UK) 9 November 1923, *R v Sussex Justices, ex parte McCarthy*, 1 KB 256.

ECtHR 4 December 2008, *S. and Marper v. the United Kingdom*, nos. 30562/04 and 30566/04.

High Court (IRL) 3 October 2017, *The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems*, No. 4809 P.

Secondary sources

Books

AUSLOOS J., *The Right to Erasure: Safeguard for Informational Self-Determination in a Digital Society?*, Dissertation for the degree of Doctor of Laws (PhD) KU Leuven, 2018, 468.

GIAKOUMOPOULOS C., BUTTARELLI G. and O'FLAHERTY M., *Handbook on European data protection law*, European Union Agency for Fundamental Rights and Council of Europe, Luxembourg, 2018, 397.

GONZÁLEZ FUSTER, G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham, Springer, 2014, 274.

HOOFNAGLE, C. J., *Federal Trade Commission: Privacy Law and Policy*, New York, Cambridge University Press, 2016, 402.

KRZYSZTOFEK M., *Post-reform Personal Data Protection In the European Union : General Data Protection Regulation (eu) 2016/679***,** Alphen aan den Rijn, Kluwer Law International B.V., 2017, 255.

LYNSKEY, O., *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press, 2015, 307.

Contributions to edited books

BRKAN M., "The Court of Justice of the EU, Privacy and Data Protection: Judge-made law as a leitmotif in fundamental rights protection" in BRKAN, M. and PSYCHOGIOPOULOU, E., *Courts, privacy and data protection in the digital environment*, Cheltenham, Edward Elgar Publishing, 2017, 241.

CHEVALLIER-GOVERS C., “Personal Data Protection: Confrontation between the European Union and the United States of America” in Y. ECHINARD and others (eds), *L'Union européenne et les Etats-Unis : processus, politiques et projets*, Bruxelles, Larcier, 2012, 287.

DE BUSSER E., “Flagrant Denial of Data Protection: Redefining the Adequacy Requirement” in SVANTESSON D. J. B. and KLOZA D. (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, Cambridge, Intersentia, 2017, 430.

DIENST S., “Lawful processing of personal data in companies under the GDPR” in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 291.

KUGLER T., “Practical Examples, I.” in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 291.

RÜCKER D., “Scope of application of the GDPR, I.” in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 291.

SALUZZO S., “Looking for safe harbours outside the European Union: The issue of onward transfers in EU data protection law and its external dimension” in VERMEULEN G. and LIEVENS E. (eds), *Data Protection and Privacy under Pressure*, Antwerp, Maklu, 2017, 341.

SCHREY J., “General conditions for data processing in companies under the GDPR, IV.” in D. RÜCKER and T. KUGLER (eds), *New European General Data Protection Regulation*, München, Beck, 2018, 291.

VERMEULEN G., “The Paper Shield: On the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement service” in SVANTESSON D. J. B. and KLOZA D. (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, Cambridge, Intersentia, 2017, 430.

Scholarly Articles

ANDOULSI, I., "L'arrêt de la Cour du 9 novembre 2010 dans les affaires jointes Volker und Markus Schecke GBR et Hartmut Eifert contre Land d'Hessen (C-92/09 et C-93/09): une reconnaissance jurisprudentielle du droit fondamental à la protection des données personnelles?", *Cah. dr. eur.* 2011, 471-522.

AZOULAI, L., VAN DER SLUIS M., "Institutionalizing personal data protection in times of global institutional distrust: Schrems", *Common Market Law Review* 2016, 1343-1371.

BOBEK, M., "Joined Cases C-92 & 93/09, *Volker und Markus Schecke GbR and Hartmut Eifert*, Judgment of the Court of Justice (Grand Chamber) of 9 November 2010", *CMLRev* 2011, 2005-2022.

BRÉCHOT, F.-X., "Clap de fin pour la conservation généralisée des données de connexion en Europe?", *RUE* 2017, 178-187.

CAROTTI, B., "Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa", *Giornale di diritto amministrativo* 2016, 333-344.

CRESPI, S., "The applicability of Schrems principles to the Member States: national security and data protection within the EU context", *ELR* 2018, 669-686.

DOCKSEY, C., "Opinion 1/15 Privacy and security, finding the balance", *MJECL* 2017, 768-773.

EPSTEIN, R. A., "The ECJ's Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices", *European Constitutional Law Review* 2016, 330-340.

EYNARD, J., "D'une ingérence généralisée à une autre : deux poids, deux mesures ?", *R.T.D.H.* 2018, 761-783.

FALOT N. and HIJMANS, H., “Tele2: de afweging tussen privacy en veiligheid nader omlijnd”, *NtER* 2017, 44-52.

FORGET, C., “L'avis de la C.J.U.E. sur l'accord PNR Union européenne-Canada : une occasion ratée de réaffirmer le principe de finalité?”, *JDE* 2018, 87-89.

GRANGER M.-P. and IRION K., “The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection”, *ELR* 2014, 835-850.

HIJMANS H., “PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators”, *EDPL* 2017, 406-412.

KUNER, C., “International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR”, *CMLRev* 2018, 857-882.

LE BONNIEC, N., “L'avis 1/15 de la CJUE relatif à l'accord PNR entre le Canada et l'Union européenne : une délicate conciliation entre sécurité nationale et sécurité numérique”, *RTD Eur* 2018, 617-628.

LYNSKEY, O., “Control over Personal Data in a Digital Age: *Google Spain* v *AEPD and Mario Costeja Gonzalez*”, *Mod. Law Rev.* 2015, 522-548.

LYNSKEY, O., “The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*”, *CMLRev* 2014, 1789-1812.

MOEREL, L., “De betekenis van de Safe Harbor uitspraak van het Europese Hof voor datadoorgiftes naar de VS”, *Nederlands juristenblad* 2016, 1174-1183.

OJANEN, T., “Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter”, *European Constitutional Law Review* 2016, 318-329.

PEYROU, S., “Arrêt «Tele2 Sverige» : l’interdiction du stockage de masse de données à caractère personnel réaffirmée par la Cour de justice de l’Union européenne”, *JDE* 2017, 107-109.

PEYROU, S., “La Cour de justice de l'Union européenne, à l'avant-garde de la défense des droits numériques”, JTDE 2015, 395-398.

ROBERTS, A., “Privacy, Data Retention and Domination: *Digital Rights Ireland Ltd* v *Minister for Communications*”, *Mod. Law Rev.* 2015, 535-548.

SCHEININ, M., “Towards evidence-based discussion on surveillance: A Rejoinder to Richard A. Epstein”, *European Constitutional Law Review* 2016, 341-348.

SZYDLO, M., “The independence of data protection authorities in EU law: between the safeguarding of fundamental rights and ensuring the integrity of the internal market”, *ELR* 2017, 369-387.

STEENBRUGGEN, W. and VAN HARTEN, S., “Safe Harbour is dood. Lang leve Safe Harbour 2.0?", *Mediaforum* 2015, 281-285.

TRACOL, X., ““Invalidator” strikes back: The harbour has never been safe”, *CLSR* 2016, 345-362.

ZALNIERIUTE, M., “Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement”, *Mod. Law Rev.* 2018, 1046-1063.

Videographic sources

Autorité de protection des données – Gegevensbeschermingsautoriteit (ADP-GBA), 'AVG/GDPR - Rechten van de burger', (Brussels, 23 November 2018) <https://www.youtube.com/watch?v=ceKry1RlQbs&feature=youtu.be> accessed 25 March 2019.

CONFIDENTIALITY CLAUSE

I, the undersigned, declare that the contents of this master's thesis may be consulted and/or reproduced for personal use. The use of this master's thesis is subject to the provisions of copyright law and the source must always be acknowledged.

Ondergetekende verklaart dat de inhoud van deze masterproef mag worden geraadpleegd en/of gereproduceerd voor persoonlijk gebruik. Het gebruik van deze masterproef valt onder de bepalingen van het auteursrecht en bronvermelding is steeds noodzakelijk.

Simon Gunst
Gent, 15 mei 2019