Data Retention under the Proposal for an EU Entry/Exit System (EES)

Analysis of the impact on and limitations for the EES by *Opinion 1/15* on the EU/Canada PNR Agreement of the Court of Justice of the European Union

Legal Opinion by

Dr. iur. Mark D. Cole

Professor for Media and Telecommunication Law
at the University of Luxembourg and

Director for Academic Affairs at the
Institute of European Media Law in Saarbrücken

and

Teresa Quintel, LL.M.

Ph.D. Student, University of Luxembourg

(October 2017)

for

The Greens | European Free Alliance
in the European Parliament

Brussels

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This legal opinion concerns the question whether and how the recent *Opinion 1/15* of the Court of Justice of the European Union (CJEU) on the Draft EU/Canada PNR Agreement impacts the Proposal for a Regulation on an Entry/Exit System. For that purpose, it analyses in detail the main findings in *Opinion 1/15* and related earlier case law on data retention schemes before applying the identified principles to the context of data collection and retention in the planned EES.

1. With its decision in *Opinion 1/15* the Court further confirmed that the standards developed so far for data retention schemes are to be applied irrespective of the nature of the instrument when testing the admissibility of a measure in view of the right to privacy and data protection as they result from Articles 7 and 8 Charter of Fundamental Rights of the European Union respectively. Therefore, the standards can be regarded as general principles for such schemes, whether they are based on secondary EU law such as Directives or Regulations as well as in the context of International Agreements or instruments with an external effect.

2. The general principles developed by the CJEU for data retention schemes need to be respected whenever data collected and retained reveal private information. The standards are not dependent on the sector, but any relevant data retention measure is regarded to be infringing the above mentioned fundamental rights and the type of data as well as the means of collection are only of relevance for the question of justification. The fact that data collection and retention under the EES takes place in a different context than processing under the PNR Agreement, which itself had a different context than the communications data setting dealt with in the previous *Digital Rights Ireland* and *Tele2/Watson* judgments, does not influence the necessity to respect the same general principles.

3. In developing the general principles, the CJEU integrated findings of the European Court of Human Rights (ECtHR) in mass surveillance and data retention cases when the Strasbourg Court interpreted Article 8 ECHR. Together, the case law of the two Courts underlines that data retention schemes have in principle a significant impact on the right to privacy and data protection of all data subjects concerned and therefore, such measures can only be justified if they genuinely meet an objective of general interest and comply with a strict necessity-requirement. Whereas the CJEU has confirmed that fighting serious crime such as terrorism is an objective that can justify the collection and retention of certain data of specific persons for longer periods, this is much less obvious for other objectives. The EES pursues a primary objective of migration management and border control. The prevention, detection and investigation of serious crime is merely a secondary objective of the planned system. Thus, retention of data under the EES is not limited to persons who represent a risk to public security. Therefore, the retention periods as regards the primary purpose of the EES are not proportionate to the objective pursued and not strictly necessary in order to achieve it.

4. Based on the findings in *Opinion 1/15* it is clear that even justified retention of data needs to be limited in terms of duration to what is necessary in connection with the pursued objective. This led the Court to find that although the transfer by air carriers and subsequent use of air passengers data by Canadian authorities was acceptable, the continued retention after departure of the concerned individuals from Canada was no longer needed as long as they did not represent a risk to public security and therefore, in violation of EU law. The same

logic applies for the data retention periods under the EES. Where a person lawfully enters the Schengen area and exits the EU within the period of authorized stay, data may only be retained if an objective beyond facilitation of border control and management is applicable, such as objective evidence that the data may contribute to the protection of public security.

Longer retention periods concerning Third Country Nationals (TCNs) whose entry was refused or who overstayed the period of authorized stay, are possible but should be decided on a case by case basis by the competent authority verifying the conditions for entry. Thus, if the refusal of entry is based on a criminal offence, the retention of the respective data would be necessary in order to pursue a legitimate interest of public security in preventing the person from entering the EU. The same logic should be applied for individuals who exceeded the period of their authorized stay in the Schengen area. Whenever there is objective evidence that the data of a person may contribute to the prevention, detection and investigation of serious criminal offences, the prolongation of retention periods for persons falling under any of the above-mentioned categories beyond that of personal data from unsuspected persons is justified. However, it would need to be established whether that data should be stored in a system established primary for border management purposes or rather in a specific databases for LE purposes.

5. Concerning access to retained data by LEAs, the CJEU previously decided in the data retention cases mentioned as well as the *Schrems* judgment and confirmed now in *Opinion 1/15* that personal data must be effectively protected against the risk of abuse and unlawful access and use. Lawful access to personal data by competent authorities must therefore be based on objective evidence and preceded by prior review carried out by a court or by an independent authority. In cases of urgency, where early access is regarded as imperative, when the Proposal for the Regulation foresees that prior authorisation can be disregarded and the central access point shall process an access request immediately, the *ex post*-review on the legitimacy of the request is all the more important to ensure safeguards against potential fundamental rights violations. This ex post-review has to be carried out by a court or independent authority. A lack of such provisions makes the EES incompatible with the standards required by the CJEU.

6. It is important that strict necessity as condition for retention periods as well as the requirements for LE access laid down by the CJEU are applied also for the EES. The proposed EES Regulation does not fulfil these requirements at least with regard to the proportionality of retention periods that must be based on strict necessity, conditions for judicial review prior to LE access to personal data and the lack of a truly independent *ex post* review mechanism. Beyond the EES, the requirements mentioned by the CJEU should be seen as a basis to set a standard for any future database retaining data of individuals for long periods. Especially with regard to interoperable databases, concerns regarding the different purposes of databases, the conditions for LE access and varying retention periods arise. Therefore, a standard model should be established along the conditions established by the CJEU in order to prevent fundamental rights violations, particularly, by means of automated processing of personal data and profiling of the individuals concerned. When applying the standards, further requirements need to be taken into consideration with data transfer to third countries that will take place within the scope of Regulation 2016/679 and Directive 2016/680 respectively, even if data is originally stored within the territory of the European Union.

A. Background and Scope of Analysis

I. Background to the Legal Opinion

In the past decade there have been numerous measures introduced which – often responding to terrorist attacks – foresee the collection and retention of different types of data. Often these are regarded as being useful for law enforcement purposes in order to prevent or combat serious crimes such as terrorism even if the primary objective of the measures may have been different. It can be noted that the pressure to guarantee public security often leads to the proposal of using ever-growing technological abilities in surveillance and monitoring efforts. The legislative bodies of the European Union have contributed with their share of instruments introducing such measures and adding to activities of the Member States. Notably, both for purposes within the European Union, but also in its external relations, instruments were proposed and introduced that allow the following of communications or travel activities by EU citizens as well as Third Country Nationals.

The increasing number of such proposals or legislative acts is in stark contrast to the legal evaluation of these instruments by courts, most notably the Court of Justice of the European Union (CJEU): just as frequently as measures are adopted and introduced it seems that the analysis of them results in finding a fundamental rights violation due to an unjustified intrusion of privacy or infringement of data protection rights. The more general, all-encompassing and wide-ranging the collection and retention of data, the less targeted and limited, the more likely it is that the measure will be struck down.[1]

The present legal opinion is prepared in light of this development on the one hand and a very recent development in which context data retention and its limitations by fundamental rights will play an important role again. Since a few years border control has become a crucial element in the debate of internal security concerns within the European Union. Additionally, very recent terrorist attacks have given rise to increased security and surveillance measures, including data retention and analysis as means for crime investigation in the context of migration monitoring.

---

[1] See generally on this development Mark D. Cole and Teresa Quintel, ""Is there anybody out there?" – Retention of Communications Data. Analysis of the status quo in light of the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR), in: Weaver et al. (ed.), Privacy in an Internet Age, CAP 2018 (forthcoming); Mark D. Cole and Annelies Vandendriessche, "Case Note:From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance Roman Zakharov v Russia (App no 47143/06) and Szabó andVissy v Hungary (App no. 37138/14)", (2016) 2(1) *European Data Protection Law Review* (EDPL), p. 121-129. On the groundbreaking judgment of the CJEU declaring the Data Retention Directive void cf. Franziska Boehm and Mark D. Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union', study for the Greens/EFA Group in the European Parliament. Münster/Luxembourg, 30 June 2014, especially concerning measures such as PNR and border control p. 73 et seq., 89 et seq., 101 et seq., available at http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm-Cole-data_retention-study-print-layout.pdf.

Due to the absence of internal borders in the EU between Member States that are part of the Schengen area, new information tools were set up at the EU's external borders to strengthen border management and security cooperation between Member States' Law Enforcement Authorities (LEAs)[2], being assisted by EU actors such as Europol. In the past months, the Commission proposed several changes to expand existing databases, widen access to relevant data for LEAs and to examine the possibility of a legal framework to enable the sharing of information among different IT systems.[3] Furthermore, several proposals for the establishment of additional databases have been put forward by the Commission.[4] One of the proposed databases which is now up for decision in the legislative procedure is the Entry/Exit System (EES). It builds on the "Smart Borders Package"[5] presented in 2013, which at the time did not secure consensus among the co-legislators. It was since subject to additional technical and operational studies completed in 2015[6] which were preparatory steps for the new proposal of an EES that was put forward in April 2016.[7] This seeks to establish a system that stores alphanumeric and biometric data (a combination of four fingerprints and the facial image), that would allow to record information on the time and place of entry and exit of Third Country Nationals (TCNs) when travelling into the Schengen area, and to grant LEAs access to retained data for the prevention, detection and investigation of terrorism and other serious criminal offences.

There have been many concerns expressed already in the early negotiation phase preparing the establishment of an EES. Apart from political considerations about the usefulness of such a system, the main concern that has been addressed by several actors, is the question of the system's compatibility with fundamental rights, in particular the right to privacy and data protection as they are laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the EU as well as in Article 16 TFEU in addition to the provision of the European Convention on Human Rights (ECHR)'s Article 8 ECHR. Various actors, such as the Article 29 Working Party[8], the European Data Protection Supervisor (EDPS)[9] and scholars[10], as well as the

---

2 In the following the abbreviation "LEAs" will be used for both terms, Law Enforcement Authorities as well as Law Enforcement Agencies, the abbreviation "LE" for Law Enforcement respectively.

3 Cf. for details European Commission, "Communication from the Commission to the European Parliament and the Council: Stronger Smarter Information Systems for Border and Security", COM(2016) 205 final, Brussels, 6 April 2016.

4 See for instance, Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM(2016) 731 final, Brussels, Brussels, 16 November 2016.

5 European Commission, 'Smart Borders': for an Open and Secure Europe, http://europa.eu/rapid/press-release_MEMO-13-141_en.htm.

6 http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586614.

7 Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011.

8 The Article 29 Working Party commented on the Communication from the Commission on Smart Borders in a letter addressed to Commissioner Malmström of 12 June 2012.

9 EDPS Opinion 06/2016 on the Second EU Smart Borders Package. Recommendations on the revised Proposal to establish an Entry/Exit System, 21 September 2016.

10 Cf. Julien Jeandesboz, Susie Alegre, and Niovi Vavoula, "European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection", January 2017; FRA-2017

institutions' legal services elaborated intensively what is problematic about mass retention of personal data, and, linked to that, the establishment of large scale databases. These contributions already shed light on why some of the issues dealt with in this legal opinion are problematic from the outset. The present opinion will focus on whether the planned EES meets the strict necessity and proportionality test in the specific way it was developed by the CJEU for mass data retention instruments to be justifiable.

It is worth mentioning that the EES if realized will become (one of) the largest EU databases, also storing biometric identifiers of TCNs and being interoperable with the Visa Information System (VIS).[11] The EES, therefore, constitutes one further step in a line of IT systems that are being established on EU level, with a primary purpose of migration management and border control, and a secondary objective to allow law enforcement access to retained data for the purpose of crime prevention and prosecution. All of these databases and the periods for retention of data in these databases must fulfil the above mentioned test by providing a legitimate aim that is pursued and proportionate measures as to how the aim is reached.

The CJEU has, on several occasions, ruled on the legitimacy of general data retention regimes that are (also) used for subsequent access by LEAs. These decisions are briefly recalled below to illustrate they contribute to the development of general principles for (bulk) data retention measures. Most recently, on 26 July 2017, the CJEU issued an Opinion[12] on the Draft Agreement between the EU and Canada on the transfer and use of Passenger Name Records (PNR) data, holding that the agreement may not be concluded in its current draft form. This decision does not only significantly change the scope and form of a possible future PNR Agreement concluded with Canada and other States as well as existing PNR arrangements, it is also highly important for data retention schemes in general as it builds on and expands the findings of previous decisions of the CJEU on such schemes. Although *Opinion 1/15* does not prohibit the systematic transfer and automated analysis of all PNR data of passengers travelling to Canada as such, the Court strongly criticized the conditions for judicial authorization prior to LE access to retained data. This concern it had already pointed out in both the *Digital Rights Ireland*[13] and the *Tele2/Watson*[14] judgments which dealt with EU and national rules about communications data retention obligations on private operators.

As will be shown, just like the EES can be seen as yet a further step towards an integrated border management system, *Opinion 1/15* is a further step in the Court's consistent line of case law concerning mass data retention regimes. The CJEU followed the general principles that it had established in previous judgments and which it cites throughout the Opinion.

Report, "Fundamental rights and the interoperability of EU information systems: borders and security", July 2017; FRA 2014, "Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data"; Dennis Broeders et al., "Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data", Computer Law & Security Review 33, no. 3 (June 2017).

11 Regulation (EC) No 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) [2008] OJ, L 218/60.

12 Opinion 1/15 of the Court of Justice of the European Union of 26 July 2017 pursuant to Article 218(11) TFEU on the Draft agreement between Canada and the European Union (Passenger Name Records) [2017] ECLI:EU:C:2017:592.

13 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* (CJEU, 8 April 2014) ECLI:EU:C:2014:238.

14 Joined Cases C-203/15 and C-698/15, *Tele2/Watson* (CJEU, 21 December 2016) ECLI:EU:C:2016:970.

Thereby, a list of limitations, requirements and tests concerning data retention schemes has been established, which allows its application also in the present context of the planned EES.

II. Scope and Structure of the Legal Opinion

Against this background the Greens/EFA in the European Parliament have requested a legal analysis of the implications the most recent CJEU Opinion 1/15 has for the planned EES. In order to fully assess the extent of the impact the present opinion will present the specificities of the EES measured against the conclusions to be drawn from the Opinion 1/15. It is not within the scope of this study to extensively analyse the EES Proposal as it stands now, but the focus is on the explanation why the EES cannot be regarded as standing separate from the requirements set by the CJEU for data retention schemes in other contexts.

The legal opinion will present the findings based on the following structure: first, the relevant legislative framework will be briefly mentioned including the provisions in primary law that need to be respected in the creation of secondary EU law (B. I.). This will be followed by an overview of the previous case law of the CJEU that is of relevance in the context of evaluating the EES (B. II.) and what can be concluded already from the case law prior to Opinion 1/15, including the relevance of the ECtHR's case law on mass surveillance and Article 8 ECHR infringements generally. Part C. will give an overview of those parts of the EES that are specifically impacted by the holding of the CJEU in that Opinion. The extensive analysis of Opinion 1/15 follows (D.) with an overview of all important points made by the Court, before putting these in context with the earlier case law and concluding which findings are to be tested with the EES proposal.

The application of these standards to the EES in part E. will show how the EES needs to be evaluated in light of the Opinion 1/15; the focus will be on the different retention periods in light of the data stored (E. II.) as well as on the question of LE access to the retained data based on evidence of its relevance and what procedures are foreseen for judicial or independently given authorization prior to such access (E. III.). The final part concludes the findings and will underline that the EES does not respect the standards developed by the CJEU and therefore should not be passed in the current form.

B. The Applicable EU Legal Framework for Data Retention

I. Primary and Secondary Law

In order to evaluate the impact of the recent case law of the CJEU on the Proposal for a Regulation on the EES, it will briefly be recalled which acts and provisions in EU law can be of relevance.

1. Relevant provisions in the Treaties and Charter

Article 16 Treaty on the Functioning of the European Union (TFEU) lays down already in the Treaty as primary law a specific right to data protection. This underlines the importance of the fundamental right as typically the fundamental rights provisions are now to be found in the Charter of Fundamental Rights of the European Union which has the same legal value as the Treaties since entry into force of the Lisbon Treaty. The Charter also prominently displays the right to privacy and – in addition, which is a noteworthy difference to the provision in the Convention – to data protection in Articles 7 and 8 respectively. The European Convention on Human Rights (ECHR) of the Council of Europe includes a right to privacy which is laid down in Article 8. This provision has been interpreted widely by the European Court of Human Rights (ECtHR) in Strasbourg. Both the provision and its interpretation are to be considered within the context of EU law and specifically the Charter as Article 7 copies the contents of Article 8 ECHR.

2. Relevant Regulations and Directives

In the field of data protection and specifically data retention the following secondary law was created based on the relevant provisions in primary law:

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

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Di-rective on privacy and electronic communications) Official Journal L 201/37, as amended by Directive 2009/136, OJ L 337/11 (Proposal by Commission for Repealing this Regulation is currently under debate, see below).

Directive 2006/24/EC 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, OJ L 105/54 (declared void by the CJEU).

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. OJ L 350/60.

Regulation (EC) 45/2001 of the European Parliament and of the Council on the protection of the individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1 (Proposal by Commission for Repealing this Regulation is currently under debate, see below).

Regulation (EU) 2016/679 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, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1 (the GDPR will replace Directive 95/46/EC as of 25 May 2018).

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.

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119/132.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals 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, COM(2017) 8 final, Brussels,10 January 2017.

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, Brussels,10 January 2017.

II. Relevant case law of the Court of Justice of the European Union

In the context of mass data retention schemes, the CJEU delivered several judgments during the past years, the most relevant for this opinion being *Digital Rights Ireland*, *Tele2/Watson* and *Schrems*[15]*.* In *Opinion 1/15* the Court relied on these judgments to determine the requirements that must be fulfilled when introducing mass data retention schemes that provide for subsequent access for crime investigation purposes. Those requirements include, inter alia, the principle of proportionality and strict necessity regarding data retention periods, conditions for LE access to retained data, and the existence of objective evidence when granting such access for the purpose of the prevention, detection, investigation and prosecution of serious crime.

[15] Case C-362/14, *Schrems* (CJEU, 6 October 2015) ECLI:EU:C:2015:650.

1. Data Retention Schemes and Fundamental Rights

In *Digital Rights Ireland,* the Court found that:

> "[…] retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article".[16]

> "[…] data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive".[17]

However:

> "[The retention] period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary".[18]

In *Tele2/Watson,* the CJEU considered that:

> "Having regard, inter alia, to the close relationship between the retention of data and access to that data, it was essential that that directive should incorporate a set of safeguards and that the Digital Rights judgment should analyse, when examining the lawfulness of the data retention regime established by that directive, the rules relating to access to that data".[19]

The Court added:

> "In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary".[20]

---

16 CJEU, Case C-293/12 and C-594/12 Digital Rights Ireland para 29.

17 CJEU, Case C-293/12 and C-594/12 Digital Rights Ireland para 49.

18 CJEU, Case C-293/12 and C-594/12 *Digital Rights Ireland* para 64.

19 CJEU, Case C-203/15 and C-698/15 *Tele2/Watson* para 57.

20 CJEU, Case C‑203/15 and C‑698/15 *Tele2/Watson* para 109.

2. Access to Retained Data by Competent Authorities for LE Purposes

The conditions for LE access to data are somewhat clearer than the limits on the retention of data. The Court consistently held that, as a general rule, such LE access must be subject to prior review by a court or an independent authority.

In *Digital Rights Ireland,* the CJEU held that:

> "the access of the competent national authorities to the data constitutes a further interference with that fundamental right (see, as regards Article 8 of the ECHR, Eur. Court H.R., *Leander v. Sweden*, 26 March 1987, § 48, Series A no 116; *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI)".[21]

> "It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest".[22]

In *Schrems,* the Court maintained that:

> "The right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards".[23]

In *Tele2/Watson,* the Court found that:

> "In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime".[24]

3. Objective Evidence to justify LE Access and Strict Necessity

In order to make LE access to retained data lawful, objective evidence must exist that there is a link between the data and the objective to fight serious crime. Thus, only where LE access is strictly necessary to achieve that objective, such access may be granted.

In *Digital Rights Ireland,* the CJEU acknowledged that:

---

21 CJEU, Case C-293/12 and C-594/12 *Digital Rights Ireland* para 35.

22 CJEU, Case C-293/12 and C-594/12 *Digital Rights Ireland* para 44.

23 CJEU, Case C-362/14 *Schrems* para 34.

24 CJEU, Case C-203/15 and C-698/15 *Tele2/Watson* para 120.

"[The Directive] therefore applies 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".[25]

"It must therefore be held that Directive [2006/24] entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to **ensure that it is actually limited to what is strictly necessary**".[26]

The Court concluded:

"Having regard to all the foregoing considerations, it must be held that, by adopting Directive [2006/24], the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter".[27]

"Legislation is not limited to what is **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".[28]

In *Tele2/Watson,* the Court confirmed that:

"Due regard to the principle of proportionality also derives from the Court's settled case-law to the effect that the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply **only in so far as is strictly necessary**".[29]

Therefore:

"As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national **legislation 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".[30]

---

25 CJEU, Case C-293/12 and C-594/12 *Digital Rights Ireland* para 58.

26 CJEU, Case C-293/12 and C-594/12 *Digital Rights Ireland* para 65.

27 CJEU, Case C-293/12 and C-594/12 *Digital Rights Ireland* para 69.

28 CJEU, Case C-362/14 *Schrems* para 93.

29 CJEU, Case C-203/15 and C-698/15 *Tele2/Watson* para 96.

30 CJEU, Case C-203/15 and C-698/15 *Tele2/Watson* para 111.

4. The impact of the Convention and ECtHR Case Law on the interpretation by the CJEU

An important further development in the case law of the Court of Justice in the context of the interpretation Articles 7 and 8 of the Charter is the increasing reliance on the case law of the European Court of Human Rights (ECtHR).[31] This was very explicit in the cases of *Tele2 / Watson* and *Digital Rights Ireland*[32] when it narrowly limited data collection and storing activities based on EU law with a reference to the case law of the Strasbourg Court.[33] The CJEU in *Tele2/Watson* followed the approach of the Strasbourg Court and required similar prerequisites to safeguard data subjects' rights, as well as objective criteria in order to define the circumstances under which LEAs may be granted access to retained data.[34]

Interestingly, in the meanwhile the ECtHR – even though not interpreting EU law or its transposition in national law – in order to substantiate its interpretation of Article 8 ECHR also explicitly[35] or implicitly[36] referred to the judgements of the CJEU[37] when declaring national laws on mass surveillance incompatible with the Convention.

Particularly the principle of proportionality in the framework of data retention and mass surveillance plays a crucial role in all of the judgments by both Courts. Moreover, the Courts are critical about lacking ex ante authorization procedures and missing judicial control.[38] Therefore, it is crucial to also take into account the approach taken by the ECtHR in that field of case law, when assessing the CJEU's findings regarding (mass) data retention. More specifically, when looking at the impact specific CJEU decisions giving further clarity to the understanding of Articles 7 and 8 of the Charter have for related areas of law, one needs to read these in conjunction with the holdings of the ECtHR on Article 8 ECHR.

---

31 Mark D. Cole and Annelies Vandendriessche, "Case Note:From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance. Roman Zakharov v Russia (App no. 47143/06) and Szabó and Vissy v Hungary (App no. 37138/14)", (2016) 2(1) *European Data Protection Law Review* (EDPL), p. 121-129 and previously: Franziska Boehm and Mark D. Cole, 'EU Data Retention – Finally Abolished? Eight Years in the Light of Article 8', in: CritQ, Critical Quarterly for Legislation and Law, Volume 1, 2014, 58 et seq..

32 As mentioned above, in *Digital Rights Ireland,* the CJEU referred to *Leander v. Sweden*; *Rotaru v. Romania* [GC]; and *Weber and Saravia v. Germany*. On the significance of the ECtHR case law also Mark D. Cole and Franziska Boehm, "Data Retention after the Judgement of the Court of Justice of the European Union," June 30, 2014, p. 27-35.

33 See for instance paras 119 and 120 of the *Tele2/Watson* judgment, where the CJEU refers to case *Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) and case *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016).

34 CJEU, Case C-203/15 and C-698/15 *Tele2/Watson* para 119.

35 *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016)

36 *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015).

37 See for instance *Zakharov v Russia,* where the ECtHR refer to *Digital Rights Ireland* at para 147.

38 Mark D. Cole and Teresa Quintel, ""Is there anybody out there?" – Retention of Communications Data. Analysis of the status quo in light of the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR), in: Weaver et al. (ed.), Privacy in an Internet Age, CAP 2018 (forthcoming).

III. Interim Conclusion on the Impact of the existing CJEU case law

During recent years, and particularly after the entry into force of the Lisbon Treaty and the EU Charter becoming a legally binding instrument, the CJEU has on several occasions ruled on the compatibility of mass data retention schemes with the fundamental rights to privacy and data protection. Several requirements for the establishment of such schemes are reoccurring in all of these judgments and may be regarded as general principles that, like a 'red thread', navigate through the Court's jurisprudence on data retention. These general principles include *inter alia* the setting of limited data retention periods, judicial authorization prior to LE access to retained data, objective evidence of crime in order to grant such access, and strict necessity as to the objective pursued by the legislative measure.

On that account, the CJEU rulings in the context of data retention leave no doubt that the findings of the CJEU concerning the applicability of the Charter provisions as well as the approach of the ECtHR in Strasbourg, where an elaborate case law also exists, need to be read into further fields where data retention takes place, and are not limited to relevant provisions concerning telecommunications or PNR data.

C. The Proposal for a Regulation on an Entry/Exit System (EES)

In order to be able to evaluate the impact of the CJEU *Opinion 1/15* on the anticipated Entry/Exit System, it is first necessary to briefly present the main elements of the EES that are relevant in the context of this legal opinion. This presentation will contribute to understanding – after having analysed the Opinion in more depth in the next chapter – whether or not elements of *Opinion 1/15* can be transferred to further areas concerned with data protection.

The following section will therefore give a brief overview of the system's structure and subsequently illustrate both the legal basis and the purpose of the proposed EES Regulation, thereby particularly focussing on retention periods and LE access to retained data. Thereafter, the analysis will address the main findings of the CJEU in *Opinion 1/15* with regard to retention periods and LE access as well as the limitations and safeguards that must be satisfied when implementing mass (PNR) data retention schemes.

I. Background

The Schengen Borders Code[39] has no provisions on the recording of travellers' cross border movements into and out of the Schengen area. As a general rule, TCNs have the right to enter the Schengen area for a short stay of up to 90 days within any 180-day period either with or without the need for the prior granting of a visa.[40] Currently the stamping of the travel documents indicating the dates of entry and exit is the sole method available to border guards and immigration authorities to calculate the duration of stay of TCNs and to verify if a person is overstaying the authorized period of a visa.[41]

In a nutshell, the proposed Regulation establishing an EES addresses TCNs entering the Schengen area for a short stay. The proposed EES Regulation excludes from its scope on the other hand TCNs holding a long-stay visa as well as EU citizens and residents, persons enjoying the right of free movement and other TCNs under Article 2(3) of the proposed EES Regulation. The EES Regulation was proposed by the Commission in order to improve the management of external borders, prevent irregular immigration and facilitate the management of migration flows. Recital (16) states that, in the fight against terrorist offences and other serious criminal offences, it is vital that law enforcement authorities have the most

---

39 Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) [2016] OJ L 77/1 and Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders [2017] OJ L 74/1.

40 Generally, a short-stay visa issued by one of the Schengen States entitles its holder to travel throughout the 26 Schengen States for up to 90 days in any 180-day period. Visas for visits exceeding that period remain subject to national procedures. European Commission, "Visa Policy", Migration and Home Affairs - European Commission, December 6, 2016, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-policy_en.

41 COM(2016) 194 final, p. 2.

up-to-date information. Consequently, the information contained in the EES should be available to the competent LEAs of the Member States and Europol[42], as according to the Commission, it is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest.[43]

II. Overview of the draft Regulation

1. Structure

The EES is divided in nine chapters, the first dealing with general provisions, principles, scope, purpose and the technical architecture of the system, including the foreseen interoperability of the EES with the VIS. In addition, Chapter I defines the competent authorities that are authorized to enter, amend, delete and consult data stored in the EES. Furthermore, the chapter includes provisions on the automated calculation of the duration of authorized stays, information to be given to data subjects on the remaining period of their authorized stay, as well as the information mechanism to be set up for the identification of TCNs exceeding the period of their authorized stay.

Chapter II contains provisions stipulating the conditions for the use of data stored in the EES by competent authorities, data to be entered into the EES according to different types of visa, in case of refusal of entry and in the event of a change of a visa status. Finally, Article 23 lays down the conditions for both verification and comparison of identity and prior registration of TCNs in the system for the performance of border checks. Chapter III specifies the requirements for other authorities to examine visa applications and to decide on access of TCNs to national facilitation programs. Moreover, Articles 26 and 27 stipulate the conditions for immigration authorities to access data of TCNs for verification and identification purposes and to determine cases in which data retrieved from the EES may be kept in national files.

Chapter IV lays down the procedures and conditions for access to the EES by competent authorities and Europol for law enforcement purposes and Chapter V stipulates the retention periods for data storage, as well as the condition for amendments of data. Both chapters are highly important when considering the impact of existing case law of the CJEU in data retention cases has on the proposed EES. Therefore, these will be further discussed below with regard to the requirements set out in CJEU judgments and, in particular, its *Opinion 1/15*.

---

42 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "Opinion on the legal basis of the Proposal for a Regulation establishing an Entry/Exit System", 14 June 2017, p. 4. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-603.073%2b01%2bDOC%2bPDF%2bV0%2f%2fEN.

43 Commission Staff Working Document, Impact Assessment, Annexes to the Impact Assessment report on the introduction of an Entry Exit System, part 3/3, SWD(2016) 115 final, Brussels April 2016, p. 136. Cf. cases cited by the Commission: Cases C-402/05 P and C-415/05 P; *Kadi and Al Barakaat International Foundation v Council and Commission* EU:C:2008:461, para 363 and Cases C-539/10 P and C-550/10 *P Al-Aqsa v Council* EU:C:2012:711 para 130.

Chapter VI defines both the operational development of the EES and the responsibilities of the Member States and Europol when collecting, retaining and transferring data to third countries and to those Member States that do not operate the EES. Furthermore, the chapter addresses provisions relating to data protection and data security, liability in the event of unlawful processing, keeping of logs, self-monitoring and penalties to be imposed for wrongfully entered data. Chapter VII provides for data subjects' rights of information, access, rectification, completion, erasure and restriction of processing, as well as documentation, remedies and supervision by the supervisory authorities and the EDPS. Article 52 lays down the condition for the protection of data accessed and used by LEAs pursuant to chapter IV. Once accessed by national LEAs, those data are to be processed in accordance with the provisions of Directive 2016/680.

Finally, Chapters VIII (amendments to other Union instruments) and IX (Final provisions) contain standard and more technical provisions. One important aspect to be mentioned with regard to the amendments to other Union instruments is the above-mentioned interoperability, which requires the amendment of certain provisions under the VIS Regulation. The interoperability of databases and the impact on fundamental rights will be taken into consideration below with regard to concerns regarding the development of further (interoperable) databases in the future.

2. Purpose and Legal basis of the EES

a) Legal basis

The Commission proposed Article 77(2)(b) and (d) of the Treaty on the Functioning of the European Union as the appropriate legal basis for the establishment of the EES. In addition, the revised proposal relies on Article 87(2)(a) TFEU, which falls under Chapter 5 (police cooperation) and has thus been considered the appropriate legal basis to allow access to the Entry/Exit system by national LEAs. Finally, Article 88(2)(a) TFEU regarding the adoption of Regulations by the European Parliament and the Council in accordance with the ordinary legislative procedure for the determination of among others Europol's tasks was initially proposed as additional legal basis.

In April 2017, it was agreed to delete one of the legal bases provided in the Commission proposal, namely Article 88(2)(a) TFEU.[44] Article 77(2)(b) and (d) TFEU in conjunction with Article 87(2)(a) TFEU are presented as the legal basis in the proposal as of June 2017.

b) Objectives of the EES

The EES proposal pursues a twofold objective, namely the management of external borders *and* the access to EES data by law enforcement authorities for the prevention, detection and

[44] The proposed Regulation does not establish new tasks and does not aim to modify the existing tasks of Europol on the collection, storage, processing, analysis and exchange of information as provided for in Article 88(2)(a) TFEU and Article 17(3) of the Europol Regulation, which already provides for Europol's access to data from Union information systems, European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "Opinion on the legal basis of the Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES)", 14 June 2017, p. 2.

investigation of terrorist offences and other serious criminal offences. The proposed Regulation aims to establish an Entry/Exit system that will register information on the entry, exit and refusal of entry of TCNs crossing the external borders of the Schengen area. [45]

Based on the first objective of the EES, the system seeks to improve i) border checks for TCNs by reducing delays and enhancing the quality of border checks by automatically calculating the authorised stay of each traveller; ii) the systematic and reliable identification of 'overstayers'; and iii) the internal security in the EU and the fight against terrorism and serious crime by granting law enforcement authorities access to travel history records.[46]

The EES will collect data, create and store entry and exit records of TCNs with a view to facilitating the border crossings of *bona fide* travellers, identifying refused TCNs at the border and better detecting overstayers. The EES will record refusals of entry of TCNs falling within its scope and give access to LEAs to perform queries in the database for criminal identification and intelligence for purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.

aa) Data registered for the purpose of border control

The Entry-Exit system will apply to TCNs who are admitted for a short stay in the territory of the Member States and who are subject to border checks in accordance with the Schengen Borders Code when crossing the external borders of the Schengen area. The Entry/Exit system will apply to visa-exempt TCNs as well as those who are admitted for a short stay of maximum 90 days in any 180-day period and can enter, leave and re-enter in that time period, which is why the EES information allows for a tracking of movements in a more detailed manner than for holders of other types of visa. The scope of the EES, thus, includes border crossings by all TCNs visiting the Schengen area for a short stay (both visa-required and visa-exempt travellers).

The EES will register entry, exit and refusal of entry of TCNs storing information on their identity, their travel documents as well as biometric data (four fingerprints and the facial image). Pursuant to Article 14 of the draft EES Regulation, the competent border authorities shall create an individual file of each TCN who is subject to a visa requirement when crossing the external borders of the Member States. This individual file contains information concerning name(s), date of birth, nationality, sex, type and number of travel document(s) and the three-letter code of issuing country of the travel document(s). Moreover, the EES will retain biometric data such as a facial image and finger prints. Finally, the exact information on date and time of entry, border crossing point and the authority that authorized the entry, shall be entered. Once the TCNs left the EU, date and time of exit, as well as the border crossing point of the last exit shall be registered. Where there is no exit at the end of a TCN's stay, the entry/exit record shall be marked with a flag. Articles 15, 16 and 17 specify the data that are to be retained for TCNs who are exempt from the visa obligation, TCNs who have been refused entry and information that is to be added when authorization for short stay is

---

45 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "Opinion on the legal basis of the Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES)", 14 June 2017.

46 http://www.consilium.europa.eu/en/press/press-releases/2017/06/30-entry-exit-system/.

revoked, annulled or extended. Moreover, Article 18 of the proposed Regulation provides for interoperability between the EES and VIS for those TCNs who require a visa to cross the EU external border.

bb) Law enforcement access

Chapter IV of the proposed EES Regulation focuses on the procedures and conditions for access to the EES by Member States' designated LEAs for the prevention, detection and investigation of terrorist offences and other serious criminal offences (Articles 26, 28 and 29) and by Europol's designated authority (Articles 27 and 30).[47] Member States' LEAs and Europol will be granted access to the EES from the start of operations[48] in order to *inter alia* contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences and by that, attain the secondary objective of the EES.[49]

According to the Commission, the EES will contain reliable data on entry and exit dates of TCNs falling within the scope of the EES that can be of decisive importance in individual law enforcement files[50]: "As such, for the purposes of criminal investigations, the EES is said to provide data to confirm or not the presence of specific TCNs in the Schengen area. The EES also uses the identification data to link entries and exits and can act as the database of last resort for identifying persons when more focused databases did not yield a result".[51] Thus, the EES will be the only system that collects and stores the entry/exit data of all TCNs entering the Schengen area for a short stay, whether via a land, sea or air border and therefore, will by far be the most complete database storing such data.[52]

---

47 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "Opinion on the legal basis of the Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES)", 14 June 2017, p. 4.

48 COM(2016) 194 final, p. 6.

49 SWD(2016) 115 final, p. 136.

50 COM(2016) 194 final, p. 6.

51 SWD(2016) 115 final, p. 136.

52 SWD(2016) 115 final, p. 136.

D. The CJEU *Opinion 1/15* on the EU-Canada PNR Agreement

I. Background

In 2005 the European Commission adopted an Adequacy Decision under Article 25(2) of the EU Data Protection Directive 95/46/EC in which it considered the Canadian Border Services Agency (CBSA) to provide an adequate level of protection for the transfer of PNR data for flights from the EU to Canada.[53] In the following year an agreement between the EU and Canada concerning the processing of advance passenger information (API) and PNR data came into force. Both Decision and Agreement expired three and a half years in September 2009, but Canada declared that it would continue to apply these protections voluntarily.[54]

On 2 December 2010, the Council adopted a decision, authorising the Commission to open negotiations with Canada on a new agreement on the transfer and use of PNR data to prevent and combat terrorism and other serious transnational crime. This new agreement for the transfer and use of PNR data between the EU and Canada was signed on 25 June 2014, after the European Data Protection Supervisor (EDPS) had delivered an opinion on the proposal. Thereafter, the Council sought approval of the draft agreement by the European Parliament, which on 25 November 2014 decided to request an opinion from the CJEU pursuant to Article 218(11) on two questions.[55]

The first question raised concerned the compatibility of the draft PNR agreement with the EU Charter, in particular Articles 7 and 8. The second question concerned the choice of legal basis of the PNR Agreement, which the Council had proposed to be concluded on the basis of Article 82 (judicial cooperation in criminal matters) and Article 87 (police cooperation) TFEU. The question raised by the European Parliament was whether Article 16 TFEU would not be the appropriate legal basis. The application was lodged with the Court on 10 April 2015 and on 26 July, the CJEU delivered its final Opinion on the questions concerning the draft agreement. It was the first time that the Court had ruled on the compatibility of a draft international agreement with the EU Charter. In general, the CJEU followed the opinion of Advocate General (AG) Mengozzi that was issued on 8 September 2016, holding that the PNR Agreement in the form signed by the Council cannot be concluded.[56] First, the CJEU found that the agreement was based on the wrong legal basis and that instead Article 16(2) and Article 87(2)(a) TFEU were the correct legal basis. Secondly, the Court held that the PNR Agreement, in its current form, was not fully compliant with the EU Charter.

---

53 Decision 2006/253/EC on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency [2006] OJ L 91, p. 49.

54 Christopher Kuner, *"Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15", VerfBlog,* 2017/7/26, http://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/, DOI: https://dx.doi.org/10.17176/20170727-094655 .,

55 More on the background and history of the Agreement cf. *Opinion 1/15* paras 16-24.

56 Hielke Hijmans, "PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators", in (2017) 3(3) *European Data Protection Law Review* (EDPL), p. 407.

II. Main Findings of the Court

As in previously established case law, the CJEU followed an approach of different stages in order to assess whether the draft PNR Agreement satisfied the criteria of strict necessity and proportionality: The Court first sought to ascertain whether certain articles of the Charter were applicable to the Draft Agreement and further questioned whether there was an infringement of the fundamental rights enshrined in those articles. Once the Court found an infringement of these rights, the Court assessed the seriousness of the fundamental rights infringement and analysed very carefully whether the infringement was justified. In that regard, the Court analysed the seriousness of the infringement and the justification along the principles of necessity and proportionality.

For the purpose of this opinion, the assessment will primarily concentrate on those matters addressed in *Opinion 1/15* that might have an impact on disputed provisions of the anticipated EES, namely the retention periods foreseen under the EES and the conditions for LE access to retained data. Therefore, the following section will first show that the standards set by the CJEU in *Opinion 1/15* concerning the PNR Agreement should be regarded as general principles, which should not only be applied solely in a particular context. Built on this first assumption, the analysis will proceed on the assertion that it should not be relevant for the applicability of Charter rights whether data undergo processing that is of commercial nature, or are being processed by public authorities. Moreover, whether or not data are sensitive, or processing inconvenienced the data subject should not change the fact that general principles regarding the legitimate aim of processing and appropriate safeguards must be followed. Thus, any interference with the right to privacy and the right to data protection should require similar safeguards, irrespective of the types of data being processed or the purpose of the processing.

In order to further address the concerns raised by data retention periods, the analysis will follow the Court's line in *Opinion 1/15*, and assess the strict necessity of data retention by distinguishing between the retention of passengers' PNR data *before, during* and *after* their stay in Canada. The assessment will then take into account the principles of objective evidence and judicial authorization prior to law enforcement access to retained data for the purpose of the fight against (serious) crime. Finally, the next section will substantiate the arguments with further CJEU judgments that have to be read in conjunction and not isolated from the Opinion, namely the *Digital Rights Ireland, Schrems* and *Tele2/Watson* judgments.

1. International Agreements as integral part of the EU legal system

Holding that the provisions of international agreements entered into by the European Union under Articles 217 and 218 TFEU form an integral part of the EU legal system, the CJEU confirmed that such provisions must be entirely compatible with the Treaties and thus, in accordance with the principles stemming therefrom.[57] The Court thereby acknowledged that *all* EU legislation must be in compliance with the fundamental rights standards enshrined in

[57] *Opinion 1/15* para 67.

the Charter and thus, processing under the PNR Draft Agreement should comply with Article 8 of the Charter.[58]

2. Significance of Types and Purpose of the Data retained

The CJEU held that the fact that the PNR data under the Draft Agreement were initially collected by air carriers for commercial purposes, and not by competent authorities for the purpose of the prevention, detection and investigation of criminal offences would not preclude Article 87(2)(a) TFEU (police cooperation) from also constituting an appropriate legal basis for the Council decision on the conclusion of the envisaged agreement.[59]

The Court thereby followed the AG, who found that the Draft Agreement did not govern the collection of PNR data (by the air carriers) and that therefore the initial collection of data did not constitute processing of personal data that resulted from the Draft Agreement.[60] The AG further held that, since the air carriers were obliged to transfer the PNR data to the Canadian authorities, the Draft Agreement was not based on the passengers' consent and the possibility to object those transfers was barred.[61] This confirms that both the CJEU and the AG differentiate between the data initially collected by the air carriers for commercial purposes and those data that were to be transferred to the Canadian authorities for the prevention, detection and investigation of criminal offences.

Although not directly concerning the type of data as such, this fact may be substantiated by the Court's finding 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'.[62]

3. Applicability of the EU Charter to different forms of processing

The Court held that the various forms of processing under the Draft Agreement, namely the transfer, access, use and retention of personal data, would affect the fundamental right to respect for private life guaranteed in Article 7 of the Charter, as that data included information relating to an identified or identifiable individual.[63]

The CJEU further maintained that the communication of personal data to third parties would constitute an interference with the fundamental right enshrined in Article 7, irrespective of the subsequent use. This would equally apply to both the retention of and access to those data, regardless of whether the information in question was sensitive or whether the persons concerned had been inconvenienced by the interference.[64] Moreover, the "subsequent transfer of personal data to other Canadian authorities, Europol, Eurojust, judicial or police

---

58 *Opinion 1/15* para 48.

59 *Opinion 1/15* para 101.

60 AG Opinion, *Opinion 1/15* paras 178 and 179.

61 AG Opinion, *Opinion 1/15* para 184.

62 *Opinion 1/15* para 142.

63 *Opinion 1/15* para 122.

64 *Opinion 1/15* para 124.

authorities of the Member States or indeed authorities of third countries […] constituted interferences with the right guaranteed in Article 7 of the Charter".[65]

The processing of the PNR data covered by the Draft Agreement also falls within the scope of Article 8 of the Charter, as it constitutes processing of personal data within the meaning of that article. Accordingly, all forms of processing under the Draft Agreement must necessarily satisfy the data protection requirements laid down in Article 8 of the Charter.[66]

4. Justification for the interference with Article 8 CFR

Although the Court acknowledged that, for assessing whether the Draft Agreement was compatible with the right to the protection of personal data both Article 16(1) TFEU and Article 8 of the Charter would be material, the CJEU primarily considered Article 8, with the argument that paragraph 2 of that Article would be more extensive and lay down in detail the conditions under which personal data may be processed.[67] This indicates that the Court sees Article 8 as the more specific regulation of the matter and will in future preferably turn to that in the interpretation, but irrespective of that it certainly means that the standards developed by the CJEU in connection with Article 8 have to be considered whenever an infringement by data processing takes place. According to the CJEU, since the processing of the PNR data covered by the Draft Agreement would fall within the scope of Article 8 Charter, such processing must necessarily satisfy the data protection requirements laid down in that article.[68]

Consequently, 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'[69] and – in accordance with the first sentence of Article 52(1) of the Charter – 'any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms'. The term 'provided for by law' would, according to the CJEU, require that the legal basis permitting the interference with any Charter right must define the scope of such limitation.[70] Furthermore, the principle of proportionality under Article 52 (2) would require that limitations of the rights and freedoms enshrined in the Charter would be permissible only if they were 'necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.[71] In accordance with the CJEU's jurisprudence, the principle of proportionality would further require "that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary".[72]

The Draft Agreement would therefore have to indicate in what circumstances and under which conditions a measure providing for the processing of personal data may be adopted

---

65 *Opinion 1/15* para 125.
66 *Opinion 1/15*, para 123.
67 *Opinion 1/15* para 120.
68 *Opinion 1/15* para 123.
69 *Opinion 1/15* para 137.
70 *Opinion 1/15* para 139.
71 *Opinion 1/15* para 138.
72 *Opinion 1/15* para 140.

and guarantee sufficient safeguards for the protection of personal data from abuse and unauthorized access. The Court added that "the need for such safeguards is all the greater where personal data is subject to automated processing" or where sensitive data were at stake.[73]

Drawn from the findings of the Court, it is evident that, in order to be proportionate, limitations to the fundamental rights to privacy and data protection are possible only if they are strictly necessary and genuinely meet objectives of a general interest that is recognized by the EU. In other words, the Court has underlined that this is an especially intense proportionality test that has to be passed.

5. The retention and use of PNR data before and during passengers' stay in Canada

The Court accepted that, for the purpose of the Draft Agreement, the PNR data of all passengers travelling to Canada may be transferred by the air carriers to the Canadian authorities and further be retained during the passengers' stay in Canada. The CJEU argued that since the provisions under the Draft Agreement would not differentiate between the passengers concerned, the retention of the PNR data of all air passengers would be permissible.[74] In that regard, the AG had rightly pointed to the fact that the processing of data must apply to all passengers on an equal basis to prevent unlawful discrimination[75] and therefore, distinguishing passengers according to, for instance, geographic areas of origin[76] would seem illegitimate. In that regard, the CJEU added that retention and use of PNR data for security checks and border control checks may not be restricted to a particular circle of air passengers.[77]

The Court stipulated, however, that the legislation in question must 'satisfy objective criteria that establish a connection between the personal data to be retained and the objective pursued'[78] by the Draft Agreement, namely the fight against terrorism and serious transnational crime.[79]

6. Retention of data after passengers' departure from Canada

Since passengers leaving Canada had been subject to border checks prior to their arrival in Canada and their PNR data had also potentially been verified before their departure, the Court found that the continued storage of the PNR data of all passengers after their departure from Canada would not be limited to what is strictly necessary.[80]

---

73 *Opinion 1/15* para 141.

74 *Opinion 1/15* para 194.

75 AG Opinion, *Opinion 1/15*, para 254.

76 Reference to the *geographic criterion* in *Tele2/Watson* para 111.

77 *Opinion 1/15* para 197. Cf. FRA-Gutachten 1/2011 Fluggastdatensätze (Passenger Name Records, PNR-Daten), Vienna 14 June 2011, p. 7.

78 Thereby, the Court cited *Schrems* and *Tele2/Watson* para 110.

79 *Opinion 1/15*, para 191.

80 *Opinion 1/15* para 206.

The Court therefore concluded that the Draft Agreement does not ensure that the retention and use of PNR data by the Canadian authorities after the air passengers' departure from Canada is limited to what is *strictly* necessary.[81]

The Court, however found that, in particular cases, where there is objective evidence that certain air passengers may represent a risk for public security *after* their departure from Canada, it would be permissible to store the PNR data beyond the passengers' stay in Canada.[82] In that regard, the CJEU points to the findings in *Tele2/Watson,* where the Court permitted targeted retention as a preventive measure.[83]

Provided that the continued storage and use of the PNR data would be based on objective criteria showing that they could contribute to the fight against terrorism and serious transnational crime, and considering that access to the data by Canadian authorities would be subject to prior review carried out either by a court, or by an independent administrative body,[84] the CJEU held that a five-year retention period would not exceed the limits of what is strictly necessary for the purposes of combating terrorism and serious transnational crime.[85]

7. Objective evidence and prior review to LE access to retained data

With regard to the retention of the PNR data during the passengers' stay in Canada, the Court found a connection between that data and the objective pursued by the Draft agreement necessary in order to ensure that the Draft Agreement would not exceed the limits of what is strictly necessary.[86]

As the data had been analysed before the passengers' arrival in Canada, the use of that data during their stay would presuppose new circumstances in order to be legitimate. Any use of the stored data during that period would, therefore, require 'rules laying down substantive and procedural conditions governing that use' would have to be based on objective criteria in order to define the circumstances and conditions under which the Canadian authorities would be authorised to use the stored data.[87] Only where there would be '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', the use of that data would not exceed the limits of what is strictly necessary. [88]

Moreover, the Court found that it would be essential that the use of retained PNR data, during the passengers' stay in Canada would be subject to a prior review carried out either by a court, or by an independent administrative body. An exception to that requirement would solely arise in cases of validly established urgency.[89]

---

81 *Opinion 1/15* para 211.

82 *Opinion 1/15* para 207.

83 *Tele2/Watson* para 108.

84 *Opinion 1/15* para 208.

85 *Opinion 1/15* para. 209.

86 *Opinion 1/15* para 197.

87 *Opinion 1/15* para 200.

88 *Opinion 1/15* para 201.

89 *Opinion 1/15* para 202. In that context, the Court also referred to para 120 of *Tele2/Watson.*

III. *Opinion 1/15* in context with other case law of the CJEU

In *Opinion 1/15*, the CJEU reiterated the standards that it had established in *Digital Rights Ireland*, *Schrems* and *Tele2/Watson,* and further extended these principles with regard to their applicability to international agreements.

The Court particularly referred to those three cases regarding the principle of strict necessity[90] and to the *Schrems* and *Tele2/Watson* decisions in the context of data retention.[91] Citing *Tele2/Watson,* the Court recalled that in order to retain PNR data there must be a link from which it may be inferred that that data "might make an effective contribution to combating [serious crime]"[92] and, further, access to retained data must "be subject to a prior review carried out either by a court, or by an independent administrative body".[93] Thus, the application of the main principles laid down by the Court in *Digital Rights Ireland* and *Tele2*/*Watson* generally remain the same in respect to the necessity test, which is not met where a legislative basis provides for indiscriminative and generalized retention of all (traffic) data for subsequent LE access, without a relationship between the data retained and a threat to public security.[94]

With regard to transfers of data to public authorities outside the EU and effective oversight mechanisms, the Court included in its *Opinion 1/15* the approach developed in *Schrems*, arguing that transfers of data to a non-EU country are only lawful when that country ensures a level of protection "essentially equivalent to that guaranteed within the European Union".[95] Moreover, the Court limited the possibility for Canadian authorities to disclose PNR data to other Canadian government authorities and to government authorities of third countries. As regards the latter, the Court referred to *Schrems*, highlighting the risk of circumventing the rules on transfers of personal data to third countries if such follow-on transfer were able without guaranteeing the essentially same level of protection all along.[96]

The Court left no doubt that the transfer and use of PNR data under the Draft Agreement constituted an interference with Articles 7 and 8 of the Charter and thereby confirmed that the principles of proportionality and strict necessity indeed have to be complied with in a more general manner irrespective of the nature of the instrument or act that potentially affects these rights. The Court went on to examine the justification for the interferences on the basis of the criteria laid down in Article 52(1) of the Charter as interpreted by its earlier case law on data protection, in that context also citing *Schecke*[97] beyond again *Schrems*,

---

90 *Opinion 1/15* para 140.

91 *Opinion 1/15* paras 191 and 192.

92 *Opinion 1/15* para 201.

93 *Opinion 1/15* para 202.

94 Council of the European Union, Information Note Legal Service Permanent Representative Committee (Part 2), 11931/17, Brussels, 7 September 2017, p. 9.

95 *Opinion 1/15* para 93.

96 Council of the European Union, Information Note Legal Service Permanent Representative Committee (Part 2), 11931/17, Brussels, 7 September 2017, p. 12.

97 Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR* (CJEU, 9 November 2010) ECLI:EU:C:2010:662.

Digital Rights Ireland and *Tele2/Watson.* In addition, it referred here explicitly to the ECtHR judgment *S. and Marper*.[98]

The Court very clearly underlined that *Digital Rights Ireland, Schrems* and the more recent *Tele2/Watson* judgments form part of a stream of decisions that confirm the fundamental right to data protection and should not be regarded as separate elements but jointly contributing to a clearer picture of that right.[99] From that reasoning, it is clear that the Court views also the *Opinion 1/15* as horizontal part of its case law on data retention that will have important implications for other areas concerned with that matter.

IV. Conclusions to be drawn from the findings of the CJEU

The CJEU accepted both the systematic transfer and the use of personal data, recognizing the protection of public security as a general interest of the European Union.[100] However, where a decision was to be taken based on the outcome of automated processing, any such "positive result must be subject to individual re-examination by non-automated means before any measure adversely affecting a passenger is taken".[101] This underlines that automated processing is especially problematic for individuals and therefore the general interest alone does not justify disrespecting the need for an intensified level of scrutiny by human involvement.

The Court discussed in detail the compatibility of the retention periods under the Agreement with EU law, distinguishing between the retention and use of the data before the arrival of the passengers to Canada, during their stay in the country and after their departure. The CJEU held that it would be legitimate to process and retain the data for the purpose of security checks and border control, and that the availability of data to LEAs for the prevention of terrorism and serious transnational crime might be necessary, also in combination with data collected in other databases.[102] However, the retention of that information for a particularly long period of time after the passengers' departure was not strictly necessary where the outcome of the (original) processing had not identified a person as representing a risk in terms of terrorism and international crime.[103] Only in the event that there was objective evidence that the retained data of certain passengers may contribute to prevent risks to public security, a five-year retention period would not exceed the limits of what is strictly necessary.[104]

The CJEU held that, as a general rule, access to and use of personal data by LEAs would only be permitted after prior review by a court or by an independent authority and following a

---

98 *Opinion 1/15* para 114, Council of the European Union, Information Note Legal Service Permanent Representative Committee (Part 2), 11931/17. Brussels, 7 September 2017 p. 5.

99 Christopher Kuner *"Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15", VerfBlog,* 2017/7/26, http://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/, DOI: https://dx.doi.org/10.17176/20170727-094655.

100 *Opinion 1/15* para 149.

101 *Opinion 1/15* para 173.

102 *Opinion 1/15* para 199.

103 Hielke Hijmans, "PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators", in (2017) 3(3) *European Data Protection Law Review* (EDPL), p. 408.

104 *Opinion 1/15* para 207 and 209.

reasoned request for access that was based on objective evidence.[105] These safeguards are obviously necessary from the viewpoint of the Court to ensure that the intensive infringement does not happen without a specific fact-checking by either a court or an authority independent of the one requesting access.

With regard to the disclosure of personal data to non-EU government authorities, the Court relied on the standard it had established in *Schrems*, holding that data transfers to third countries require a level of data protection in that country that is 'essentially equivalent' to that under EU law.[106] Furthermore, the CJEU held that individuals must have a right to have their data rectified[107], and that it would be necessary to notify data subjects individually when their data had been used[108], except where such notification would jeopardise ongoing investigations.[109]

While the AG had argued that data subjects were entitled to an effective *post factum* judicial review, which could substitute prior authorization by an independent administrative authority or judicial control before LE access to data[110], the CJEU went beyond this. It insisted on the existence of such a safeguard, meaning that either prior control by an independent administrative authority or by a court is necessary and it is not sufficient to justify the infringement by a review *after* it has taken place. The Court thereby confirmed that compliance with *all* safeguards would be essential to ensure fundamental rights compliance. Thus, even if some of the implemented safeguards are very strong, that does not exclude the obligation to also implement the remaining safeguards.

Especially important in the evaluation of the Court's Opinion 1/15 is the fact that it once again underlined that the proportionality test in connection with limitations to Article 7 and Article 8 Charter is to be understood as a very strict one because "simple" necessity and meeting objectives of general interest is not enough. The scrutiny requires that the objectives are genuinely met and the necessity is a strict one. Although this may not go as far as constituting a proportionality test that is different from the one applied to other fundamental rights in the Charter, it does indicate that the balancing of interests in data retention cases affecting Articles 7 and 8 Charter in principle tips in favour of the rights protection and that a justification for infringements therefore needs weighty reasons applied carefully.

---

105 *Opinion 1/15* para 201, 202, 207 and 209.

106 *Opinion 1/15* paras 134 and 214.

107 *Opinion 1/15* para 220.

108 *Opinion 1/15* para 223.

109 *Opinion 1/15* para 224. Cf. Christopher Kuner, "*Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15", VerfBlog,* 2017/7/26, http://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/, DOI: https://dx.doi.org/10.17176/20170727-094655. The transfers of data to third countries, access, rectification and notification rights under the EES will be subject to the provisions of Regulation 2016/679 and Directive 2016/680 and therefore, not further discussed in this legal opinion.

110 AG opinion, *Opinion 1/15* para 272.

E. Applying the standards of *Opinion 1/15* to the EES

I. General observations

Opinion 1/15 reinforces that the requirements established by the CJEU are applicable to further fields where data retention plays a prominent role, namely the domain of border control and migration management. The Court's approach should be seen as a reminder that if the rights enshrined in the Charter are applicable even to international agreements, these rights should all the more be taken into account when adopting secondary EU legislation which is directed 'internally' to the EU. The PNR Opinion must be seen in the context of a series of judgments that require strict proportionality and compliance with the fundamental rights under the Charter when adopting EU legislative measures in areas affecting the right to privacy and data protection. This confirms that whenever the Court applies the proportionality test, it must be seen as an overarching concept and cannot be applied in different ways according to specific sectors when the same fundamental right is concerned. Thus, for each measure adopted that infringes data protection rights, the legitimate aim for such measures has to comply with high standards.

The CJEU's jurisprudence on data retention leaves little room in interpreting what is to be regarded as general principles applied to such measures and it is crucial to see the PNR Opinion in the broader context of already prior existing case law in order to substantiate the assumption that certain criteria of the Opinion are also be applied for other data retention schemes such as the Entry/Exit System. Following the line of the CJEU's case law on data retention, four reoccurring criteria may be established emanating from *Digital Rights Ireland*, *Tele2/Watson* and now *Opinion 1/15*. Although these criteria might not have been applied in the exactly equivalent manner in those three cases a generally consistent application should be achieved in order to ensure compatibility with Articles 7 and 8 of the EU Charter. These criteria can in principle also be applied to bulk data retention schemes in other fields:

– Retention schemes must be justified and scrutinized based on the principles of proportionality and necessity, especially the categories of data and the retention periods adopted must be limited to what is strictly necessary.

– Judicial authorization or prior review by an independent authority is a mandatory requirement for lawful LE access to retained data.

– There must be provisions on the obligation to notify data subjects in the event of use of data concerning them (e.g. in the event of access, disclosure or further transfer).

– The data that may justifiably be retained must be stored within the territory of the EU.

The following section will focus on the first criteria and assess whether the retention periods provided for under the EES may be regarded as being justified and strictly necessary. Further, conditions for access by LEAs to the EES will be scrutinized along the second criteria. The third criteria will not be further analysed here, as rights of data subjects to be notified are subject to the provisions under Regulation 2016/679 and Directive 2016/680. The

fourth criterion will also not be addressed, but it needs to be pointed out that concerns regarding transfers of data to third countries may arise concerning the conditions provided for under Chapters V of both Regulation 2016/679 and Directive 2016/680.

II. Proportionality test and strict necessity in view of the retention periods under the EES

1. Proportionality in view of objective

As the Draft PNR Agreement and the anticipated Entry/Exit System pursue different objectives, it is essential to apply the proportionality test in accordance with the legitimate aim that may justify the interference with Articles 7 and 8 Charter in the particular context of the respective objectives. As opposed to the PNR Draft Agreement, which seeks to ensure public security and to contribute to the fight against terrorism and serious international crime, the primary purpose of the EES is the improvement of border checks at the EU's external borders and the identification of TCNs who no longer fulfil the conditions for entry or stay in the Schengen area.

The objective of the PNR Agreement constitutes an objective of general interest of the EU that is capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter.[111] In addition, "the protection of public security contributes to the protection of the rights and freedoms of others".[112] The CJEU, however, emphasises that – given the seriousness of the interference – *only* the objective of fighting terrorism and *serious* crime is capable of justifying the mass transfer[113], the use by competent authorities[114] and the continued storage of PNR data after passengers' departure from Canada.[115] Thus, the Court set a particularly high threshold as regards the legitimate aim to retain data and highlights that the interference limiting the rights to privacy and data protection must be based on objective evidence that it can actually contribute to the fight against terrorism and serious transnational crime.[116] In addition, the measure must be strictly necessary.[117]

---

111 *Opinion 1/15* para 148 et seq.; also already in *Tele2/Watson* para 102.

112 The Court referred in this context to Article 6 of the Charter "In this connection, Article 6 of the Charter states that everyone has the right not only to liberty but also to security of the person". See *Opinion 1/15*, para 149; CJEU, Case C‑293/12 and C‑594/12 *Digital Rights Ireland* paras 42 and 44; CJEU (15 February 2016), N., C-601/15 PPU, EU:C:2016:84, para 53.

113 *Opinion 1/15* para 149; *Tele2/Watson* para 102.

114 *Opinion 1/15* para 200.

115 *Opinion 1/15* para 207, *Tele2/Watson* para 108.

116 *Opinion 1/15* para 207.

117 *Opinion 1/15* para 141.

2. The purposes of the EES

a) Management of border crossing and migration

The justification for the three-years retention period under the EES for TCNs who respected the duration of authorized stay is based on border management purposes, decreased border crossing time and the facilitation of expedited border crossings.[118] Moreover, the retention is necessary to allow border guards to perform the necessary risk analysis, to analyse the travel history of the applicant and to check whether TCNs have previously exceeded the maximum duration of their authorized stay. Therefore, the system should cover a retention period which is "sufficient for the purpose of visa issuance". [119]

As mentioned, concerning the retention of PNR data, the Court underlined that the retention of PNR data must be "limited to what is strictly necessary". It is doubtful whether the general improvement of management of the EU's external borders can be regarded as an objective that is to be regarded as compelling in the same way as the fight against terrorism and serious crime. Therefore, it is to be questioned whether the CJEU would accept this purpose as a basis for extensive data retention. Certainly, the length of retention which is little less than what the CJEU accepted for the objective of combatting terrorism and comparable crime, is likely to fail the test of strict necessity. Therefore, the three-years retention period of data from TCNs for the establishment of an integrated management system for the EU's external borders, to manage migration flows and to prevent irregular migration will be difficult to uphold, as such purposes may be achieved with less intrusive measures.

b) Prevention of terrorism and serious crime

The ancillary objective pursuant to Article 5(2) of the proposed EES Regulation is granting LEAs access to the system for the prevention, detection and investigation of terrorist offences or of other serious criminal offences. Moreover, the EES data shall enable LEAs to generate information for investigations relating to terrorism or other serious criminal offences. The retention of data from TCNs registered in the EES may be proportionate with regard to the second objective of the EES insofar as the retained data relates to the prevention, detection and investigation of sufficiently serious crime. It is essential to pass the test developed by the CJEU that the data retained are not held on storage for long periods of time for improving the combatting or prosecution of any type of crime but that it is limited to a small number of types of crimes that have a similar seriousness as terrorism. Long periods of retention will not satisfy this requirement by the CJEU except if there are provisions guaranteeing a use merely in the context of crimes that are "sufficiently serious".

3. Differentiation of retention periods during and after stay in the EU

In *Opinion 1/15*, the CJEU held that in order to retain data after passengers' departure from Canada, "the legislation in question must, inter alia, continue to satisfy objective criteria that establish a connection between the personal data to be retained and the objective

---

[118] Consolidated version of the Proposal for a Regulation establishing an Entry/Exit System, Recital (25).

[119] Consolidated version of the Proposal for a Regulation establishing an Entry/Exit System, Recital (26).

pursued".[120] As regards air passengers in respect of whom no risk has been identified there is no connection after they have left Canada between their PNR data and the objective pursued by the envisaged agreement which would justify that data being further retained.[121]

Applying the reasoning of the CJEU to the retention of personal data for the periods foreseen under the EES of three and five years respectively, the retention of data from TCNs who do not represent a risk to public security seems disproportionate and not limited to what is strictly necessary. For the achievement of the primary purpose of the EES, border management and the facilitation of border crossings, a retention period of three years is not required, and thus, does not represent the least intrusive measure to achieve the objective pursued. However, the retention of data from over-stayers or persons with an entry ban may be justified for as long as the persons remain absconded or unidentified, or the respective period of the entry ban is still valid. But this necessitates a differentiation to be made between the group of individuals covered by the EES in total and those for which additional length of retention may be justified due to the circumstances of their stay.

The retention of TCNs after a person has left the EU in light of the argument of the CJEU in *Opinion 1/15* is only proportionate to achieve the second aim of the EES. Therefore it should only be retained in cases where that data may contribute to the fight against terrorism and other serious crime. But even in such circumstances it might be more adequate and therefore only then proportionate to store those data in databases established purely for LE purposes and not in a general border management database. This finding is supported by the Court's argument in *Opinion 1/15* and as suggested by the ECtHR in *S. and Marper v United Kingdom.*[122]

III. Objective evidence and judicial control prior to LE access

The EES should not be regarded as an isolated system, but must be evaluated together with already existing databases such as the VIS or the Eurodac database. These systems predate the CJEU's case law on data retention and, at least to some extent, do not fulfil the requirements established in *Digital Rights Ireland, Tele2/Watson* and *Opinion 1/15*. This is particularly true with regard to the role of courts for the authorization of LE access to retained data.

Review prior to LE access to data stored in the EES follows similar procedures as the ones under existing databases such as Eurodac or the VIS, and instead of judicial control, it is a verifying authority that validates the conditions for access. Access to the EES by LEAs under Article 29 (1) and (2) is granted, where the consultation of the EES data may substantially contribute to the prevention, detection or investigation of criminal offences, and where the search in other databases did not lead to a match. A prior search in the national databases may be refrained from, where reasonable grounds exist that such a search would not result

---

120 *Opinion 1/15* para 191.

121 *Opinion 1/15* para 205.

122 Argumentation in *Opinion 1/15* para. 172 where the Court characterizes the type of database the Canadian authorities should be using; cf. also *S and Marper v United Kingdom* [2008] ECHR 1581; Application nos. 30562/04 and 30566/04.

in a match. The 'reasonability' of the requests is verified by a designated law enforcement authority (the verifying authority).[123]

In exceptional cases of urgency, access to the EES may be granted immediately and compliance with the conditions under Article 29 only needs to be scrutinized on an ex post basis, including whether an exceptional case of urgency actually existed.[124] LE access to the EES as a criminal intelligence tool shall be allowed when the conditions are met and where there is a duly justified need to consult the entry/exit records of a person. Consultation of the EES, in case of a hit, shall give access to any other data taken from the individual file, thereby providing an extensive profile of the data subject concerned.

Review by a court or an independent authority as required by the CJEU in *Digital Rights Ireland*, *Tele2* / *Watson* and in *Opinion 1/15* is not an obligation foreseen under the current proposal for the EES. Compared to the PNR data that were to be retained for a maximum period of five years and only under the condition that LE access was subject to prior review by a court or an independent authority as well as depending on that the retained data are able to make an effective contribution to combatting serious crime, the retention periods under the EES are relatively long and include data that are originally processed for non-LE purposes. While access to EES data by LEAs might be a useful tool for the investigation and prevention of serious crime, the system of checks and balances established under the proposal lacks some of the conditions set out by the CJEU in previous cases.

123 COM(2016) 194 final, p. 11.

124 Where ex post verification determines that access was not justified, the data accessed shall be deleted by the authorities that were granted access.

F. Conclusion

The above analysis has shown that *Opinion 1/15* of the CJEU impacts other data retention schemes, including the one proposed for the EES, significantly and therefore cannot be ignored – neither in on-going legislative procedures nor in view of potential amendments to be made to existing instruments. The transferability of the general principles developed in previous case law and most recently in *Opinion 1/15* leads to the conclusion that at least some key elements of the EES are problematic in light of those findings as will be summarized below.

I. Setting General Standards for Data Retention Schemes

The requirement for a consistent application of the general guidelines that were established by the Court in earlier case law concerning mass data retention schemes has now been confirmed in *Opinion 1/15*. The approach adopted by the CJEU demonstrates that these general guidelines must be seen as a line of standard setting that is prevalent in all of the above-mentioned judgments and that must be adopted not solely for particular fields such as communications related data or instruments such as Directives, but applied consistently to all (general) data retention regimes, irrespective of the type of data that are being processed or the purpose justifying the retention.

On many occasions in *Opinion 1/15* the Court cites the *Digital Rights Ireland* judgment, the *Schrems* case as well as the *Tele2/Watson* decision, which are interlinked. This confirms that the approach of the Court taken in *Opinion 1/15* follows the reasoning assumed in earlier case law, which must be applied in a consistent manner as it constitutes guidance on the general approach of the CJEU concerning the protection of privacy and personal data. In *Opinion 1/15* the Court applied the same methods and principles that were elaborated in earlier case law (concerning telecommunications data), by transferring them to a different field, namely the retention of PNR data.

The Court confirmed that international agreements as the one at issue in *Opinion 1/15* "form an integral part of the EU legal system" that must be "entirely compatible with the Treaties and with the constitutional principles stemming therefrom".[125] Such interpretation indicates that the reasoning of the CJEU in *Opinion 1/15* has a very wide reach and will have an impact on any future legislation concerning (mass) data retention, because if international agreements have to reach the standards set by the CJEU's interpretation of the Charter, this applies without doubt to the "regular" legislative acts of the EU. Thus, the approach taken by the Court concerning the Draft PNR Agreement cannot be regarded as an isolated field of application, but must be evaluated as an overarching set of principles that can be applied to any general data retention scheme and therefore necessarily also impacts the proposed EES.

---

[125] *Opinion 1/15* para 67.

Furthermore, in evaluating measures that impact Articles 7 and 8 of the Charter it is important to take into account the jurisprudence of the ECtHR and its interpretation of Article 8 ECHR, as both the ECtHR and the CJEU irreversibly linked the two legal orders of the ECHR and the EU Charter in this specific area. This approach opens the possibility to interpret the fundamental rights to privacy and data protection under the Charter in a parallel way and permits to link these to comparable findings of the ECtHR. Both Courts established general principles for data retention measures that need to be taken into account when evaluating similar retention measures. These principles contain far-reaching minimum standards and guarantees that have to be linked to any data retention scheme, as is recalled below.[126]

II. Applicability of the Charter independent of Types of Data and Means for their collection

When determining the scope of Articles 7 and 8 of the Charter, the CJEU does not differentiate between data that are to be considered as being more relevant in terms of fundamental rights protection and other data that may be less protected. Whenever data reveal private information, these data must be considered as touching upon Article 7 Charter and the processing of such data to be falling within the scope of Article 8 Charter. Therefore, different types of data collected for different purposes and possibly by different bodies do not *per se* have an impact on the fundamental rights assessment. This is independent of these aspects, it only is based on whether an infringement is justifiable. The impact on the balancing test may be different depending on the severity of the infringement, which in turn can be different depending on the data collected and retained, but it cannot be argued from the outset that certain data are less problematic and therefore the standards developed for Articles 7 and 8 of the Charter can be disrespected. The same goes for the procedure in collecting the data: from the viewpoint of the Court it cannot make a difference if data are collected initially by private parties for a specific purpose and then made available to authorities or whether these data are directly collected by public authorities, because the infringement takes place by the mere fact of collection and processing.

Applying these standards, already in *Digital Rights Ireland* the Court found the Data Retention Directive to be void because it did not comply with the Charter obligations. In the *Tele2/Watson* decision the CJEU confirmed this reasoning, holding that "[Article 15 of the e-Privacy Directive shall be in accordance with] the general principles of [European Union] law, […], which include the general principles and fundamental rights now guaranteed by the Charter".[127] The logic assumed in both cases has now been adopted in *Opinion 1/15*, which demonstrates that the reasoning of the Court applies to general data retention regimes in other fields, and a similar line of reasoning concerning the applicability of the Charter and the requirements thereof must be followed. The Court very clearly underlined that it is not

---

126 Mark D. Cole and Teresa Quintel, ""Is there anybody out there?" – Retention of Communications Data. Analysis of the status quo in light of the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR), in: Weaver et al. (ed.), Privacy in an Internet Age, CAP 2018 (forthcoming).

127 *Tele2/Watson* para 91.

sufficient to comply with *some* of these requirements, but that all principles and safeguards have to be satisfied in order to ensure that data retention schemes are compatible with Articles 7 and 8 of the Charter.

Taking the assessment of the data retention schemes by the Court in all three decisions it is evident that such schemes by their nature are to be regarded as very critical in view of fundamental rights admissibility and, therefore, require a high level of justification. In order to meet the standards of proportionality and strict necessity, data retention schemes have to fulfil an objective of general interest and need to be balanced carefully, in order to ensure that limitations of privacy and data protection rights are based on the least intrusive measures. In that context it is noteworthy that the draft PNR Agreement was based on the use of data for concerns of public security and fighting crimes whilst the EES primarily shall be introduced only as a management element for border control while it only has as a secondary objective to fight serious crime. Whereas the CJEU has accepted this latter objective as genuinely meeting the general interest objective-test, this is not the case for a different objective such as the facilitation of managing border crossings. Even if it is not excluded that this is also an important objective of the EU, the necessity test about retaining certain amounts of data for certain periods of time needs to be applied in view of this likely lesser interest.

III. Proportionality in light of Objective and Strict Necessity of Retention Periods

The CJEU upheld in *Opinion 1/15* the high threshold as regards the legitimate aim to retain data and clarified that interferences limiting the rights to privacy and data protection must pursue an objective of general interest and should only be applied in so far as is strictly necessary. The Court accepted the continued storage and use of the PNR data only where retention would be based on objective criteria showing that the data could contribute to the fight against terrorism and serious transnational crime. Only then, a five-year retention period would not exceed the limits of what is strictly necessary and would meet the requirements stemming from the principle of proportionality.

The data retention periods as proposed under the EES Regulation for the purpose of improving the management of the Union's external borders cannot be justified in light of that holding. As mentioned above, the objective of border management cannot be regarded as objective of general interest that is as compelling as the fight against terrorism and serious transnational crime. Compared to the data that were to be retained under the Draft PNR Agreement for a maximum period of five years and under the condition that there was evidence that the retained data could make an effective contribution to combatting serious crime, the retention periods under the EES seem excessive. Moreover, other than the Draft Agreement, the EES does not provide for the depersonalization of data after a certain time has elapsed, but data subjects remain identifiable during the entire period of retention. As regards the objective to contribute to the identification of over-stayers, the retention periods under the EES proposal may be justified for as long as a person remains unidentified, but this again is not a fixed period of time.

With regard to the secondary objective of the EES, namely the protection of public security, longer retention periods may be justified insofar as retention is based on objective evidence that the retained data are necessary to contribute to the prevention, detection and investigation of terrorist offences and other serious offences. This must then be limited to only concern a selected group of persons filtered from the general scope of application. There is a need to find the least intrusive measures that can achieve the objective of crime prevention in the most efficient way whilst ensuring that these measures are compatible with elementary fundamental rights standards. The usefulness of having data available is no relevant criterion. Strict necessity concerning the primary objective of border management indeed means that it cannot justify long retention periods, whereas such longer periods for the secondary objective may be justifiable but the instrument foreseen is not targeted at reaching this goal which is why already the appropriateness of the solution can be questioned.

Although in the preparation of the proposed Regulation compared to an earlier draft a reduction of retention periods for some instances has been foreseen, it is not the actual length that decides necessity (i.e. whether it is five or three years), but whether it can be justified for reaching the objective. Again, any longer retention period may always potentially contribute better to reaching a specific goal – for example, a "permanent" registration for frequent travellers entering the EU regularly over the years, facilitates the border crossing more than if it is only for 6 months or 3 years. This, however, is irrelevant when assessing the fundamental rights violation, as the length has to be objectively justified and although shorter is less problematic than longer in view of the standards developed for Articles 7 and 8 of the Charter, shorter is not automatically proportionate. It is indeed not an easy task to identify what is an appropriate retention period as the Court rightly has not set a specific time-length that is acceptable, but it is one element of the justification that has to be fulfilled and the length has to be strictly necessary. Therefore, an objective argument concerning the primary goal of the introduction of a retention scheme is necessary for justifying a specific length. This is not at all evident for the retention periods foreseen in the proposal for an EES.

IV. Judicial or Independent Authorization prior to LE Access to Retained Data

Although evidence or reasonable grounds for serious crime is a mandatory condition to grant LEAs and Europol access to data stored in the EES databases as proposed currently, review by a court or an independent authority as required by the CJEU is not obligatory. The fact that the central access point, through which the requests for access are made and which verifies whether the conditions for access are satisfied, may be part of the same organization as the designated authority requesting access does not meet the requirements set by the CJEU. Therefore, the "objective evidence"-standard that needs to be fulfilled before LE access to retained data may be granted, does not seem to accomplish the expectation of the Court, which emphasises safeguards provided by independent bodies, ideally in form of a court review.

In a case of urgency, the central access point shall process the request immediately and shall only verify *ex post* whether access was necessary, proportionate and based on

objective evidence. Again, instead of a court or an independent authority, the *ex-post*-review will be carried out by the central access point, which will lead to the same concerns as regarding the procedures of granting access. Therefore, the proposed EES Regulation does not fulfil the requirements of the Court with regard to prior judicial review and lacks truly independent *ex post* review where access requests were granted in a case of urgency.

V. Additional Elements of Risk in EES Data Processing

In *Digital Rights Ireland* and *Opinion 1/15,* the CJEU pointed out that the need for safeguards is all the greater where personal data are subject to automated processing, where there is a risk of unlawful access to data and where sensitive data are at stake. As the processing foreseen under the EES is, at least partly, based on automated processing, this increases potential difficulties for a justification of infringements to Article 7 and 8 of the Charter compared to – already existing – more manual forms of processing comparable data. In addition, the data in the EES are very privacy intrusive as they include not only numerous elements of information about the private individual but even biometric data. This could raise concerns with regard to interoperable databases that will be able to automatically communicate information among each other and therefore enable the establishment of a more complete profile of individuals. Therefore, it is crucial that the conditions for LE access in the different databases are consolidated along a standard model that satisfies the CJEU's requirements of access authorization and aligns the retention periods along the principle of strict necessity.

In sum, the analysis above shows clearly that the conclusions to be drawn from *Opinion 1/15* in combination with the previous case law of the CJEU are that the principles developed therein also impact the admissibility and design of an EES and connected data collection and retention. Irrespective of the politically questionable signal if EU legislative bodies would agree on an instrument that does not fully meet the requirements for an international agreement as set by the Court in view of the protection of EU citizens, because it concerns Third Country Nationals, the proposal for the Regulation establishing the EES should in its current form be reconsidered, in order to avoid potential difficulties in a later review of the instrument by the CJEU. This review would certainly build on the established case law about data retention schemes and therefore likely result in the finding of a violation of fundamental rights standards due to above presented reasons.