Faculty of Law,
Economics
and Finance

Law Working Paper Series
Paper number 2018-002

Connecting personal data of Third Country Nationals

Interoperability of EU databases in the light of the CJEU's case law on data retention

Teresa Quintel, University of Luxembourg
teresa.quintel@uni.lu

28/02/2018

UNIVERSITÉ DU
LUXEMBOURG

Connecting personal data of Third Country Nationals

Interoperability of EU databases in the light of the CJEU's case law on data retention

Teresa Quintel*

Abstract

On 12 December 2017, the EU Commission presented a proposal on the interoperability of EU large-scale Information Systems. The proposal seeks to enable all centralised EU databases for security, border and migration management to be interconnected by 2020. The underlying IT systems retain data of Third Country Nationals (TCNs), namely travellers, applicants for international protection, information relating to visa applications or data on missing persons and criminals. With the proposal, the Commission seeks to create new possibilities to exchange information, manage migration challenges and to enhance the Union's internal security

The interconnectivity of databases would introduce fundamental changes to the current structure of EU IT-systems and requires careful consideration and assessment of compliance with EU data protection standards. This also means that access to information in an interoperable system must be strictly aligned to the access rights of the underlying databases and that requesting authorities only obtain the data that they are authorized to access.

With interoperability, data once held in silos would be retained in three new centralized databases and would be more easily accessible, also for the prevention, investigation and prosecution of crime. Where criminal investigations previously required multiple searches in separate databases, this cascading safeguard shall progressively be abandoned to streamline access to personal data by law enforcement authorities. Despite simplified access conditions, this would require new types of processing operations for which the interoperability proposal does not provide a legal basis.

During recent years, several judgments of the Court of Justice of the European Union (CJEU) have highlighted the difficulty of striking a proper balance between the fundamental rights to privacy and data protection, enshrined in Article 7 and 8 of the Charter of Fundamental Rights of the European Union (EU Charter) with an increased demand for security and the surveillance of potential criminals. The Court repeatedly pointed out the need to strike a fair balance between these (allegedly) competing interests and emphasised that law enforcement authorities should not be granted access to personal data without prior authorization.

Using the CJEU's judgments as vehicle and considering the assumption that TCNs risk to become subject to data retention measures in a disproportionate manner, the following analysis seeks to assess both existing EU databases and their foreseen interoperability against the requirements established by the Court in order to evaluate their (in)-compatibility with the fundamental rights standards enshrined in the EU Charter.

Key words: Interoperability, Data Protection, EU Databases, CJEU, Third Country Nationals

Note: This paper is an extended version. A final version will be published in: Europarättslig tidskrift nr 2/2018.

* FNR funded PhD Candidate at the Université du Luxembourg and Uppsala University under the supervision of Prof. Mark D. Cole and Assistant Prof. Maria Bergström. Contact: teresa.quintel@uni.lu.

1. Introduction

Over the past decades, several EU databases were set up within the Area of Justice and Home Affairs in order to store the personal data of Third Country Nationals (TCNs) intending to enter the Schengen Area.

Substituting the abolition of checks at the internal borders, the EU stepped up the protection of its external borders, inter alia, by establishing large scale IT-systems to better monitor the movement of persons to and from the Union, and to improve police and judicial cooperation regarding cross-border issues.[1] The trend to further exploit personal data by expanding existing immigration and border management databases or establishing new systems with similar purposes is likely to continue, as may be observed by the pace at which databases are being proposed at EU level. These databases include IT-systems to retain personal data for asylum purposes, other databases store travellers' or visa information, data on missing persons or criminals. Interestingly, all of the relevant EU border management databases allow, as a secondary purpose, for access to stored data by law enforcement (LE) authorities for the prevention, investigation and prosecution of serious crime.

Against the background of reinforcing the EU's internal security[2] and due to the insufficient capability of EU databases to exchange information between each other, the Commission presented in December 2017 two proposals on a framework for interoperability between EU information systems[3] to enable all centralised EU databases for security, border and migration management to be interconnected by 2020.[4] The Commission thereby sought to create new possibilities to exchange information, manage migration challenges and to enhance the Union's internal security.[5]

The interconnectivity of databases would introduce fundamental changes to the current structure of EU IT-systems and requires careful consideration and assessment of compliance with data protection standards. While interoperability[6] aims at changing the way of processing and cross-matching personal data in order to improve the use of the current databases, it is essential that processing operations are carried out in a manner that is proportionate in relation to the stated objectives, limited to what is strictly necessary and solely performed within clearly defined legal instruments.[7] This also means that access to information in an interoperable system must be strictly aligned to the access rights of the underlying databases and that requesting authorities only obtain the data that they are authorized to access.

On the one hand, the right to data protection has received growing attention due to the Snowden revelations and reoccurring data leaks or breaches. On the other hand, terrorist attacks have given rise to increased surveillance programs such as data retention schemes, the interception of communications, or profiling measures.

In many EU Member States, the security-versus-privacy debate reached new dimensions during the aftermath of the arrival of great numbers of individuals seeking asylum in the European Union.[8] In several cases, the assumption that those arriving in Europe could be infiltrated by radicals and might commit terrorist acts in the

[1] "EUROPA Justice and Home Affairs", June 16, 2016, https://europa.eu/european-union/topics/justice-home-affairs_en.
[2] Communication from the Commission to the European Parliament and the Council on Stronger and Smarter Information Systems for Borders and Security, COM (2016) 205 final, Brussels, 6 April 2017.
[3] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), COM(2017) 794 final, Brussels, 12 December 2017. And Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, COM(2017) 793 final, Strasbourg, 12 December 2017.
[4] European Commission press release, "Security: the EU is driving work to share information, combat terrorist financing and protect Europeans online", Brussels, 27 July 2017.
[5] European Data Protection Supervisor statement on the concept of interoperability in the field of migration, asylum and security, 15 May 2017.
[6] Interoperability is commonly referred to as the ability of different information systems to communicate, exchange data and use the information that has been exchanged, cf. European Data Protection Supervisor "Reflection on the interoperability of information systems in the Area of Freedom, Security and Justice", 17 November 2017, p. 6.
[7] Ibid, p. 3.
[8] European Data Protection Supervisor "Reflection on the interoperability of information systems in the Area of Freedom, Security and Justice", 17 November 2017.

receiving Member States became reality.[9] This led to strong political responses in favour of new initiatives to enhance the use and exchange of personal data of these incoming persons.

During recent years, several judgments of the Court of Justice of the European Union (CJEU)[10] have highlighted the difficulty of striking a proper balance between the fundamental rights to privacy and data protection, enshrined in Article 7 and 8 of the Charter of Fundamental Rights of the European Union (EU Charter) with an increased demand for security and the surveillance of (potential) criminals.[11] The Court repeatedly pointed out the need to strike a fair balance between these (allegedly) competing interests and emphasised that LE authorities should not be granted access to personal data without prior authorization.

Using the CJEU's judgments as vehicle and considering the assumption that TCNs risk to become subject to data retention measures in a disproportionate manner, the following analysis seeks to assess both existing EU databases and their foreseen interoperability against the requirements established by the Court in order to evaluate their (in)-compatibility with the fundamental rights standards enshrined in the EU Charter. These fundamental rights issues need to be considered against the background that there might be a justified interest of LE authorities to introduce effective anti-terrorism measures and to analyse personal data for investigation purposes.

Following a brief overview of the CJEU case law on this matter (2.), section 3. will give a general description of the relevant EU large-scale IT-systems that store personal data of TCNs, namely the Schengen Information System (**SIS II**)[12], the Visa Information System (**VIS**)[13], the **Eurodac** database[14], the recently adopted Entry/Exit system (**EES**)[15], the anticipated European Travel Information and Authorisation System (**ETIAS**)[16], and the proposed European Criminal Records System for Third Country Nationals (**ECRIS-TCN**)[17]. Thereafter, potential shortcomings of these systems will be illustrated and set against the conditions developed by the Court in section 4. In section 5., the developments towards interoperability of these IT-systems, as presented in the Commission proposals on interoperability from 12 December 2017, will be scrutinized along the CJEU's requirements. Finally, the conclusion will briefly summarize the main findings of the analysis, acknowledging major shortcomings of the interoperability proposal.

[9] Refer for instance to the case of Anis Amri, a rejected asylum seeker who committed a terrorist attack in Berlin in December 2016, an attack by a rejected asylum seeker in Stockholm in April 2017.

[10] See for instance: Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* (C-293/12) and *Seitlinger* (C-594/12), ECLI:EU:C:2014:238, 8 April 2014; Case C-362/14, *Maximilian Schrems*, ECLI:EU:C:2015:650, 6 October 2015; Joined Cases C-203/15 and C-698/15, *Tele2 Sverige* AB (C-203/15) and *Watson* (C-698/15), ECLI:EU:C:2016:970, 21 December 2016 and *Opinion 1/15* on the background of the envisaged agreement concerning the transfer and processing of PNR data between the EU and Canada, ECLI:EU:C:2017:592, 26 July 2017.

[11] On this topic, cf.: 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).

[12] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), OJ, L 205/63, 7.8.2007.

[13] Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ, L 218/60, 13.8.2008.

[14] Regulation (EU) No 603/2013 of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013, OJ, L 180/1, 29.6.2013.

[15] 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 LE purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011. COM(2016) 194 final, Brussels, 6 April 2016.

[16] 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, 16 November 2016.

[17] Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011, COM(2017)344 final, Brussels, 29 June 2017.

2. General principles established by the CJEU case-law on data retention

With *Digital Rights Ireland*[18] and *Tele2*[19], the CJEU handed down two landmark decisions concerning the retention of data for the purpose of crime prevention and investigation. The Court emphasised that, even in times of terrorist threats, fundamental rights cannot be compromised by retaining data in a general and indiscriminate manner for the purpose of granting LE-access. The Court continued this privacy-friendly position with its *Opinion 1/15*[20] that concerned the Draft Agreement between the EU and Canada for the transfer of passenger name record (PNR) data.[21] The CJEU confirmed that the mass collection of personal data from unsuspicious individuals is a serious interference with the right to privacy and data protection enshrined in Articles 7 and 8 of the EU Charter. The Court further found that data retention measures for LE purposes should solely target individuals who are under a reasonable suspicion of participating in terrorist offences or other serious crime, and should not be discriminatory.[22] In *Opinion 1/15*, particular attention was given to the protection of sensitive data[23], which, according to the Court, should only be processed where sufficient safeguards and a particularly solid justification exist.[24] Moreover, LE authorities should only be granted access to stored data where such access was based on objective evidence that the data may effectively contribute to the fight against serious crime.[25] The CJEU required judicial authorization or review by an independent authority prior to LE-access to data where those data were necessary for the purpose of safeguarding public security.[26] In all of the judgments dealing with data retention measures, the Court required strict necessity and proportionality in order to render the interference with the rights to privacy and data protection lawful.[27]

The processing and analysis of personal data of TCNs, coming to the EU either with a valid travel document, or irregularly[28], not only takes place in the event of (suspected) crime, but generally starts as soon a TCN enters the territory of a Member State. Taking a closer look at the definition of serious crime[29], many of the offences referred to in relevant EU provisions[30] are attributable to irregular migration, irrespective of the fact that TCNs may be offenders or victims.[31]

Adding these findings, it may seem logical to assume that TCNs are, therefore, particularly likely to become subject to data retention and profiling measures, whether on justified grounds or not. At the same time, this

[18] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* (C-293/12) and *Seitlinger* (C-594/12), ECLI:EU:C:2014:238.
[19] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige* AB (C-203/15) and *Watson* (C-698/15), ECLI:EU:C:2016:970.
[20] *Opinion 1/15* on the background of the envisaged agreement concerning the transfer and processing of PNR data between the EU and Canada, ECLI:EU:C:2017:592.
[21] For an in-depth analysis of the Opinion, cf. Mark D. Cole and Teresa Quintel, "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 for the Greens / European Free Alliance in the European Parliament. Brussels, October 2017. https://www.greens-efa.eu/files/doc/docs/c1dc866168f947309cc1f26835a07c14.PDF
[22] *Opinion 1/15* para 172.
[23] So-called special categories of data, for instance the processing of genetic data and biometric data for the purpose of uniquely identifying a natural person.
[24] *Opinion 1/15* paras 141 and 165.
[25] *Tele 2/Watson* judgment, at paras 111 and 119.
[26] Except in cases of validly established urgency, cf. Statement of the Article 29 Working Party, "Data protection and privacy aspects of cross-border access to electronic evidence", Brussels, 29 November 2017, p. 8.
[27] See for instance *Digital Rights Ireland* at para 51 and the *Tele2/Watson* judgment, para 103.
[28] For instance, if a person is not in possession of a valid travel document or a visa.
[29] Refer for instance to Article 2(2) Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States; Articles 1 to 4 of Council Framework Decision 2002/475 of 13 June 2002 on combating terrorism, Article 3(9) Directive 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 2016, L 199/132.
[30] Listed in Article 2(2) of Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ, L 190, 18.07.2002.
[31] Examples for offences that may give rise to surrender pursuant to a European arrest warrant that might be attributable to irregular migrants are, e.g.: forgery of administrative documents, participation in a criminal organisation or facilitation of unauthorised entry and residence. Furthermore, individuals may become victims of rape, sexual exploitation or trafficking in human beings. See Article 2(2) of the EAW.

explains why access to systems that store personal data of TCNs is useful for LE authorities and why combining these data would be a valuable tool to obtain a full record of individuals coming to the EU.

3 Monitoring migration: databases as digital borders

Systems that were developed with a view to monitor migration, facilitate the implementation of the European visa policy, to improve the exchange of personal data between LE authorities or, in the case of Eurodac, as a database to better manage asylum applications, exist since several years.[32] However, the so-called *refugee crisis* in 2015 catapulted the issue of (irregular) migration, asylum and related security threats on the top of the political agenda and thus, contributed to an acceleration of legislative amendments to upgrade existing IT-systems and the proposal of new databases.

Generating in-depth knowledge of migration routes and improving the identification of individuals increases the control over TCNs coming to the EU and opens up possibilities to better monitor immigration.[33] At the same time, those whose data are stored in the databases risk to become subject to disproportionate processing measures, particularly where systems that pursue different purposes allow for an automatic exchange of data.

In the following, the six most relevant databases in the context of border controls will briefly be described chronologically along their objectives as well as the types of data to be stored, retention periods and the provisions on LE-access. In view of the proportionality requirement it is crucial to consider whether the objectives for setting up these databases could be achieved by less intrusive means.

3.1 Schengen Information System

The main purpose of the Schengen Information System[34] (SIS II) is, in the absence of internal border checks, the maintenance of public security in the Schengen States through border control and police cooperation.[35] SIS II enables competent authorities such as national border guards, police, customs, judicial, visa and vehicle registration authorities to enter alerts into the system and to consult the stored data where relevant for the performance of their tasks.[36] It therefore differs from the other five databases, as instead of LE authorities accessing data that were stored for purposes other than for the prevention, investigation and prosecution of crime, LE authorities are the ones creating alerts in SIS II. The system registers databased alerts on wanted or missing persons and objects, alerts on persons sought in relation to criminal activity and those who do not have the right to enter the Schengen Area. The alerts permit accessing authorities to identify a person via alphanumeric and biometric data and provide additional information on whether that person is armed, violent or has escaped.[37] The Schengen Information System is twinned with national SIRENE[38] Bureaux, auxiliary systems responsible for any supplementary information exchange and the coordination of activities related to SIS II alerts on national level.[39] As large-scale centralized information-system, SIS II is composed of two constitutive legal instruments,

[32] For the first comprehensive overview of data exchange possibilities and data protection rights in the Area of Freedom, Security and Justice, cf. Franziska Boehm, "Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level", Berlin Heidelberg, 2012.
[33] Dennis Broeders, "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants" International Sociology, Vol. 22, Issue 1, 2007, p. 89.
[34] The rapid growth of the Schengen group, even outside the EU through association agreements with Norway, Iceland and Switzerland, and the prospect of further enlargement of the EU, led to the decision to develop a second generation of the system as early as December 1996. Cf.: Paul De Hert, "Trends in de Europese politiële en justitiële informatie samenwerking", Panopticon jrg. 25, January/February 2004.
[35] European Commission, "Schengen Information System," Migration and Home Affairs, December 6, 2016, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en.
[36] Ibid.
[37] Article 20(3) and concerning additional information Article 30(3)(h) of the SIS II Regulation.
[38] Supplementary information request at national entry (additional data exchange possibility in the framework of the SIS II).
[39] European Commission, "SIRENE Cooperation," December 6, 2016, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/sirene-cooperation_en.

which address law enforcement[40] and border control[41]cooperation. These instruments are complemented by a regulation[42] on vehicle registration.[43]

The SIS II system is, however, currently under revision and supposed to become de-pillarized into three new SIS Regulations.[44] The proposals on the reform of the SIS II system[45] add 'unknown wanted person' as a new category to be stored in the SIS II databases, encourage better enforcement of return decisions issued to irregularly staying TCNs and expand the list of alerts to be issued.[46] The Commission also identified SIS II shortcomings such as suboptimal functionalities, gaps in the system's architecture, fragmented policy frameworks, and its limited interoperability.[47]

Pursuant to Article 6 of the proposed SIS II Regulation on the return of illegally staying TCNs, alerts on return shall be deleted where the TCN can demonstrate that he or she has left the territory of the EU Member States and where the decision upon which the alert was based has been withdrawn or annulled. In accordance with Article 34 of the proposed SIS II Regulation on border checks, alerts on persons shall be retained for the period required to achieve the purpose for which they were entered and shall be reviewed by the Member State that issued the alert within an extended period of five years.[48] The same period applies for alerts entered under the proposed SIS II Regulation on police cooperation and judicial cooperation in criminal matters.[49] Thereby, the proposed SIS II Regulations seek to align the retention periods with other databases, such as Eurodac.[50]

3.2 Visa Information System

The initial SIS system served as a model for the Visa Information System (VIS), a large-scale IT-system, seeking to facilitate the administration, issuance and checks of short-stay visas to the Schengen area by enabling the exchange of visa information and the matching of biometric data to verify the authenticity of a visa.[51] Further objectives of the VIS are the prevention of 'visa shopping' in different Member States, and to impede individuals

[40] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), OJ, L 205/63, 7.8.2007.
[41] Regulation (EC) 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ, L 381/4, 28.12.2006.
[42] Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, OJ, L 381/1, 28.12.2006.
[43] While Decision 2007/533/JHA primarily concerns LE purposes, the two Regulations on border control and cooperation on vehicle registration focus on non-LE purposes.
[44] Three proposals for: a Regulation on the establishment, operation and use of the Schengen Information System in the field of police cooperation and judicial cooperation in criminal matters, COM(2016) 883 final, a Regulation on the establishment, operation and use of the SIS in the field of border checks, COM(2016) 882 final, and a Regulation on the use of the SIS for the return of illegally staying third country nationals, COM(2016) 881 final, all Brussels, 21 December 2016.
[45] Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, COM(2016) 883 final, Brussels, 21 December 2016.
[46] Adding, for instance, an obligation to create a SIS alert for terrorist offences, a new alert category for return decisions and alerts on a wider range of stolen and falsified goods and documents. European Commission Press Release "Security Union: Technical and Operational Updates of the Schengen Information System Questions & Answers", http://europa.eu/rapid/press-release_MEMO-16-4427_en.htm.
[47] European Parliament, "Legislative Train Schedule, Area of Justice and fundamental Rights: The Revision of the Schengen Information System II", http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-the-revision-of-the-schengen-information-system-ii.
[48] The extension period was extended from three years; however, Member States may decide to set shorter review periods in accordance with national law. Member States may also regularly extend the expiry date of alerts on persons if the required action could not be taken within the original period.
[49] Except for alerts for discreet inquiry or specific checks, where the retention period remains one year.
[50] COM(2016) 883 final, p. 20.
[51] European Commission, "Visa Information System (VIS)," Text, December 6, 2016, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en.

from 'overstaying', as a legal stay in the EU may easily turn into an illegal one when a person did not leave the Union after the period of an authorized stay[52] expired.

The VIS allows for both the verification of visas and the identification of persons. During the verification process, the visa holders' fingerprints are compared with those stores in his or her visa file at the border crossing before entry. For identification purposes, competent border authorities may compare the fingerprints of a visa holder against the entire VIS database. In accordance with Article 23 of the VIS Regulation, visa application files shall be retained for a maximum period of five years, starting from the expiry date of the visa.[53] A proposal for a new legal basis for the VIS is currently under preparation and will, according to the Commission, be presented in the second quarter of 2018.[54]

Under both the VIS and the proposed SIS II Regulations, access by LE authorities may be granted for identification and return purposes[55], police and customs checks[56], for preventing and combating migrant smuggling[57], and, where necessary for the purpose of the prevention, detection or investigation of criminal offences.[58]

3.3 Eurodac

The purpose of the Eurodac database[59] is the determination of the Member State responsible for processing an asylum application by checking in the system whether a person previously applied for international protection in another EU Member State. Eurodac thereby assists the implementation of the Dublin system in order to ensure that an individual applies for asylum in the first country of entry and to prevent 'asylum shopping' in different Member States. In the future, the Eurodac database will also hold data from irregular migrants and persons illegally staying on the territory of a Member State, for the purpose of expulsion. The Commission proposal[60] from May 2016 on the reform of Eurodac, therefore, aims to expand the system's scope to wider objectives of immigration control, such as the monitoring of illegal migration and secondary movements[61] of irregular migrants within the EU.[62] This shall, inter alia, be achieved by storing the personal data of TCNs for longer periods, to investigate travel routes and to identify unauthorized stays. Retention periods under the proposal

[52] For short-stay visas in the Schengen Area, this period is normally 90 days within six months (multiple-entry visas).
[53] In cases where the applicant withdrew the application, or the visa was not granted, the period starts from date of withdrawal or the date of refusal respectively.
[54] COM(2017) 794 final, p. 80.
[55] Article 12(1) of the SIS II Regulation on Return of illegal TCNs, COM(2016) 881 final.
[56] Article 29(1)(b) of the proposed SIS II Regulation on border checks, COM(2016) 882 final.
[57] Article 12(2) of the Regulation on Return of illegal TCNs, COM(2016) 881 final.
[58] Article 29(1)(c) of the proposed SIS II Regulation on border checks and Article 43 of the proposed SIS II Regulation on police cooperation and Article 5 (1)(a) of the VIS Regulation. That Article, however, limits access to "the prevention, detection or investigation of terrorist offences and of other **serious** criminal offences". Yet, it remains to be seen whether the 2018 proposal will water down this limitation and refer to "criminal offences" only.
[59] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ, L 180/1, 29.6.2013.
[60] Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM(2016) 272 final. Brussels, 4 May 2016, p. 12.
[61] In this context, secondary movements occur when refugees or asylum-seekers move from the Member State in which they first arrived to seek protection in another Member State.
[62] The legal basis for the proposed Eurodac Regulation is Article 79(2)(c) TFEU, whereas the legal basis of Regulation 603/2013 was Article 78 (2)(e), the wider purpose remains immigration.

range from five years for data of illegally staying TCNs who do not claim asylum[63], to ten years for data of applicants for international protection. Following judicial or administrative authorization, Eurodac allows for access by LE authorities and Europol where there is substantiated suspicion that the data of a suspect or perpetrator of a terrorist offence and other serious crime, or data of a potential victim is stored in Eurodac, and where data from other (national) databases did not lead to the establishment of the identity of a data subject.[64]

3.4 Entry/Exit System

In October 2017, the Entry/Exit system (EES) was adopted to improve the management of the external Schengen borders, prevent irregular immigration and facilitate the management of migration flows.[65] As secondary purpose, the EES grants LE-access to stored data for LE purposes.[66] Thus, both national LE authorities and Europol may be granted access to the EES to process data for the prevention, detection and investigation of terrorist offences and other serious crime. The EES will register all entries and exits of short-term visa holders and visa-exempted travellers to and from the Schengen area. The system thereby functions similar to a 'tracking tool' and will be interoperable with the VIS to complement the information stored on visa applications and rejected visas. This is the first logical step towards facilitating the exchange of information and achieving full interoperability between the remaining databases. Retention periods for entry/exit records and refusals of entry were set to a maximum period of five years in the initial proposal to align them with the retention periods in other systems. However, due to criticism during the negotiations, retention periods were ultimately shortened to three years.[67]

3.5 European Travel Information and Authorization System

The European Travel Information and Authorization System (ETIAS)[68], which will apply to visa-exempt persons[69] travelling to the EU, was proposed by the Commission on 16 November 2016. As currently no obligation for an advanced transfer of information, contrary to the case for visa applications, is required for visa-exempt travellers, border guards take their decisions on whether to allow or refuse entry without any prior knowledge concerning a person.[70] According to the Commission proposal, the ETIAS will be an automated system used to determine the eligibility of TCNs to cross the external borders of the EU.[71] Similar to the American ESTA[72], or the Canadian and Australian ETA[73], travellers will have to submit an online travel authorization request prior to their arrival at the border of a Schengen country.[74] Border guards would, however, still have the final say as to whether or not entry to the Schengen Area will be granted.[75] Thus, an ETIAS

[63] The retention period for data of irregular migrants was extended from 18 months to five years in order to monitor secondary movements within the EU, particularly where an irregular migrant makes efforts to remain undetected.
[64] And, if there are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question. Article 21 of the 2016-Eurodac Proposal.
[65] European Commission, "Security Union: Commission welcomes adoption of Entry/Exit system for stronger and smarter EU borders", Brussels 25 October 2017. For an analysis of the EES, refer to Mark D. Cole and Teresa Quintel, Legal Opinion for the Greens / European Free Alliance on the Entry/Exit System. Brussels, October 2017, pp. 16.
[66] For the prevention, detection and investigation of terrorist offences and other serious criminal offences.
[67] Article 34(1) and (2) of the EES Regulation, 2016/0106 (COD), Brussels, 8 November 2017.
[68] 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, 16 November 2016.
[69] Currently, nationals of around 60 countries worldwide do not need a visa to enter the EU.
[70] European Parliamentary Research Service, "European Travel Information and Authorisation System (ETIAS)", Briefing EU Legislation in Question, 3 October 2017, p. 3.
[71] European Commission "Feasibility Study for a European Travel Information and Authorisation System (ETIAS)", Final Report, 16 November 2016, p. 12.
[72] https://esta.cbp.dhs.gov/esta/application.html?execution=e1s1.
[73].https://www.canada.ca/en/immigration-refugees-citizenship/services/visit-canada/eta/facts.html, https://www.eta.immi.gov.au/ETAS3/etas.
[74] Not having a travel authorisation would always result in a refusal of entry.
[75] By checking the relevant databases against the person's travel document. According to Regulation (EU) 2016/399 (the 'Schengen Borders Code'), travellers need to comply with the conditions for short-term stay, which include not being a threat to public order and

authorization would not change the nature of the border controls currently performed.[76] LE authorities and Europol as well as consular posts, border and immigration authorities would be permitted to consult data stored in ETIAS for the purpose of the prevention, detection and investigation of terrorism and serious criminal offences.[77] Data entered in the ETIAS would be retained for five years, as is the case for the proposed SIS II and the VIS, thereby ensuring coherence and consistency with the EU legal framework.[78]

3.6 European Criminal Records Information System for Third Country Nationals

In June 2017, the Commission proposed the establishment of a European Criminal Records Information System for Third Country Nationals (ECRIS-TCN)[79], a centralized system for the exchange of criminal records on convicted TCNs and stateless persons.[80] ECRIS-TCN is supposed to complement the current ECRIS system for the exchange of criminal records of EU citizens[81] but, other than ECRIS, will store the data on a centralized basis, as TCNs cannot be identified by nationality (which is the case for EU citizens, where the Member State of nationality is requested to provide additional information under the ECRIS Framework Decision). The ECRIS-TCN is not a LE database, as its purpose is the identification of the Member State(s) holding criminal records of TCNs, not necessarily for LE purposes.[82] Only in a subsequent step, where a criminal record exists, would data be transferred by the convicting Member State to the requesting Member State on a bilateral basis. For the procedure of exchanging criminal records, the ECRIS-TCN would borrow from the current legal instruments governing ECRIS.

The central ECRIS-TCN system, in which all queries shall be submitted, would contain identity information such as name, nationality or gender and the code of the convicting Member State, but also store fingerprints and facial images, where those are registered in criminal records by the Member States. The retention periods of data stored under the ECRIS-TCN will depend on the periods for retention of the criminal records in the national databases.[83]

Interim Conclusion

The abovementioned databases share similar, reoccurring characteristics. [84] With an exception of the proposed ETIAS, all the existing databases, amended versions or proposed systems store biometric data such as fingerprints and facial images. Due to their particularly sensitive nature, biometric data may only be processed under strict conditions and merit stronger data protection safeguards.[85]

security, holding valid travel documents, justifying the purpose and conditions of the intended stay, not being the subject of any alert in the Schengen Information System (SIS), and having sufficient means of subsistence.

[76] European Commission "Feasibility Study for a European Travel Information and Authorisation System (ETIAS)", Final Report, 16 November 2016, p. 13.

[77] Articles 43 and 44 of the ETIAS proposal and Article 46 for access to the ETIAS Central System by Europol.

[78] European Commission, "Feasibility Study for a European Travel Information and Authorization System (ETIAS)", Final Report, 16 November 2016, p. 255.

[79] Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011, COM(2017)344 final, Brussels, 29 June 2017.

[80] Meijers Committee (standing committee of experts on international immigration, refugee and criminal law), "CM1710 Note on the definition of third-country nationals in the Commission's ECRIS-TCN proposal", 2 October 2017.

[81] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ, L 93/23, 7.4.2009.

[82] Information on a criminal record could also be requested where the TCN in question applied for employment in a profession where such record is required.

[83] Article 8 of the ECRIS-TCN proposal, retention period for data storage.

[84] It needs to be mentioned that there are additional data exchange instruments on EU level, most notably the Prüm Framework and the Swedish Initiative. Both enable the participating Member States to exchange information for the purpose of preventing and investigating criminal offences by allowing for the consultation of DNA profiles or fingerprints, cf.: Paul de Hert and Juraj Sajfert, "Police, Privacy and Data Protection from a Comparative Legal Perspective", Forthcoming in *Research Handbook on Comparative Policing*, Monica den Boer (ed), Edward Elgar Publishing, 2018.

[85] Article 9 and corresponding Recital 51 of Regulation 2016/679 and Article 10 and corresponding Recital 37 of Directive 2016/680.

Secondly, all databases retain the information for a similar period, from three or five years and longer. Consequently, where data are being retained for comparable periods, competent authorities accessing and processing these data will be able to create very detailed profiles, provided they can connect the data of different databases during a long span.[86]

To use these profiles for investigation purposes, all systems, whether LE or non-LE databases, grant LE authorities and Europol access to stored data for specific purposes and under certain conditions. Such access has been progressively widened for already existing databases and became a standard feature for new systems. In particular with regard to interoperability, coherent retention periods and similar conditions for LE-access will pave the way for streamlined access conditions.

Much will depend on the knowledge and use of the databases by LE authorities, border guards, immigration officers and other competent authorities that have access to the stored data, because for the processing of retrieved data on national level, different legal instruments are applicable, depending on the purpose of the processing. For instance, processing of personal data for immigration purposes will fall within the scope of Regulation 2016/679 (GDPR)[87], while processing of personal data by competent authorities for LE purposes will fall within the scope of Directive 2016/680 (LE-Directive).[88] The concerns that may emerge regarding the applicability of the two instruments will be further elaborated in section 5.2.

4. Evaluation against the CJEU's requirements

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,[89] ruled on the compatibility of mass data retention schemes with the fundamental rights to privacy and data protection.[90] These judgments may be regarded as landmark decisions, starting with *Digital Rights Ireland*[91], in which the CJEU invalidated the Data Retention Directive[92], finding that the Directive exceeded the limits imposed for complying with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the EU Charter.

In 2015, the CJEU found in *Schrems* that "*The right to respect for private life, guaranteed by Article 7 of the Charter* […] *would be rendered meaningless if State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification* […]".[93]

[86] Cf.: Dennis Broeders et al., "Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data", in: Computer Law & Security Review Volume 33, Issue 3, June 2017, Pages 309-323.
[87] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ, L 119/1, 4.5.2016.
[88] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ, L 119/89, 4.5.2016.
[89] This analysis will refer to Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238*;* Case C-362/14, *Schrems* ECLI:EU:C:2015:650*;* Joined Cases C-203/15 and C-698/15, *Tele2/Watson*, ECLI:EU:C:2016:970 and *Opinion 1/15* on the Draft agreement between Canada and the European Union, ECLI:EU:C:2017:592.
[90] Mark D. Cole and Teresa Quintel, "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 for the Greens / European Free Alliance in the European Parliament. Brussels, October 2017, p. 13. https://www.greens-efa.eu/files/doc/docs/c1dc866168f947309cc1f26835a07c14.PDF.
[91] On the ground-breaking 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.
[92] 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, 13.4.2006.
[93] Case C-362/14 *Schrems* para 34.

On the basis of the *Digital Rights Ireland* judgment and the invalidated Data Retention Directive, the CJEU held, in *Tele2/Watson*, that EU law, and, in particular, the EU Charter, precludes the general and indiscriminate retention of metadata from all subscribers of telecommunications services.

Furthermore, the CJEU found that access to retained data by competent national authorities would require prior authorization by either a court or an independent authority[94] and that competent authorities to whom access to retained data had been granted, were obliged to notify the data subjects concerned of the interference with their rights as soon as such notification would no longer jeopardize ongoing investigations.[95]

In addition, the Court required the processing of personal data to be reviewed by an independent authority to ensure compliance with the level of protection guaranteed by EU data protection law and emphasised the possibility for individuals to lodge a complaint with the national supervisory authorities.[96]

In *Opinion 1/15*, the Court relied on these judgments to determine the requirements that must be fulfilled when introducing mass data retention schemes, which 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 access to retained data by LE authorities, and the existence of objective evidence when granting such access for the purpose of the prevention, detection, investigation and prosecution of serious crime.[97] Thus, these requirements for the establishment of data retention schemes are reoccurring in all of the abovementioned judgments and should be regarded as general principles.

The fact that the Court consistently reaffirmed these principles in all relevant judgments should be taken into account with regard to databases set up at EU level that store information on a large-scale and for rather long periods of time.[98] Consequently, the requirements established by the CJEU should be followed for both existing and proposed databases.

This would presumably entail a review of the SIS II, the VIS and the Eurodac databases along the conditions of the Court, as, most importantly, neither of them requires judicial authorization for LE-access. Secondly, it is crucial that these conditions will be incorporated in any anticipated database, and will be applicable to an interoperable system. Thirdly, thorough supervision[99] by the European Data Protection Supervisor (EDPS) for the processing of personal data by EU bodies within the scope of Regulation 45/2001[100], and by the national supervisory authorities for processing carried out on national level in accordance with Article 8(3) Charter and Chapter VI of either GDPR or the LE-Directive, as well as effective corrective powers of the supervisory authorities are essential.

[94] Case C-203/15 and C-698/15 *Tele2/Watson* para 114.
[95] Case C-203/15 and C-698/15 *Tele2/Watson* para 121. Cf.: Teresa Quintel,"Hello! Is It Me You're Looking for? Not after Tele2 Anymore…," *RSIEAblog* (blog), August 2, 2017, http://RSIblog.blogactiv.eu/2017/08/02/hello-is-it-me-youre-looking-for-not-after-tele2-anymore/./. Cf. forthcoming book chapter: 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.
[96] *Tele2/Watson* para 123, *Digital Rights Ireland* para 68 and *Schrems* para 41 and 58.
[97] Mark D. Cole and Teresa Quintel, "*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 for the Greens / European Free Alliance in the European Parliament. Brussels, October 2017, p. 8.
[98] Ibid, p. 13.
[99] For the role of Data Protection Authorities in Supervising LE authorities cf.: Paul De Hert and Juraj Sajfert, "The role of the data protection authorities in supervising police and criminal justice authorities processing personal data" in Chloé Brière and Anne Weyembergh (eds), The needed balances in EU Criminal Law: past present and future, Hart Publishing, 2017, 243-255.
[100] Regulation (EC) 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ, L 8/1, p. 1–22. 12.1.2001. This Regulation is currently being revised.

Furthermore, the advice and guidelines issued by the future European Data Protection Board (EDPB)[101], which will be in charge of the authoritative interpretation of both the GDPR and the LE-Directive, will play an important role.[102]

Beyond the criteria established by the CJEU, it is important that competent authorities, whenever they access and subsequently process data stored in the relevant systems comply with the data protection standards laid down in secondary legislation. As mentioned above, once accessed, data will be processed either under the GDPR, or, whenever data is processed by competent authorities for LE purposes, within the scope of the LE-Directive.[103] However, ambiguities regarding the scope of the two legal instruments exists and may, particularly in the area of migration and asylum, lead to limitations of data subject rights[104], less strict obligations for controllers[105], or restricted capacities for supervisory authorities to exercise their investigatory and corrective powers whenever controllers apply the Directive instead of the Regulation.[106]

5. From Silos to Interoperability

In a world of Big Data, the question of whether or not information from different sources is being connected to create individual profiles is a matter of legal constraints rather than technological ones, as the latter progressively lose their relevance.[107] With improved technological means, steps towards connecting the abovementioned databases became more tangible during the recent years.[108]

The anticipated interoperability[109] of EU databases shall enable competent authorities with fast, seamless, systematic and controlled access to information, provide a solution to detect multiple identities, facilitate identity checks of TCNs and streamline access by LE authorities to non-LE information systems.[110] In the asylum, borders and security context, a competent authority, when consulting the interoperable system, could obtain information about a person's past travel behaviour and visa applications, existing re-entry bans, or asylum requests in one search and would be notified where multiple identities are linked to the same person. LE

[101] With the transposition of the EU Data Protection Reform, the Article 29 Working Party will be replaced by the European Data Protection Board (EDPB) from May 2018 under Article 68 GDPR. The Board will be composed of one supervisory authority of each Member State, the EDPS and, if required or deemed necessary, representatives from the Commission.
[102] Paul De Hert and Juraj Sajfert, "The role of the data protection authorities in supervising police and criminal justice authorities processing personal data", p. 254.
[103] Cf. Statement of the Article 29 Working Party, "Data protection and privacy aspects of cross-border access to electronic evidence", Brussels, 29 November 2017, p. 2.
[104] Right of access to personal data, right of rectification and right to deletion of personal data enshrined in Articles 15, 16 and 17 of Regulation (EU) 2016/679; Articles 14 and 16 of Directive (EU) 2016/680 respectively.
[105] For instance, when carrying out impact assessments for profiling operations pursuant to Article 35 of Regulation 2016/679.
[106] Paul De Hert and Juraj Sajfert, "The role of the data protection authorities in supervising police and criminal justice authorities processing personal data", p. 254.
[107] Dennis Broeders, "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants" International Sociology, Vol. 22, Issue 1, 2007, p. 77; Paul De Hert and Serge Gutwirth, "Interoperability of Police Databases within the EU: An Accountable Political Choice?", in: International Review of Law, Computers & Technology, Volume 20, Nos. 1 and 2, pages 21-35, March-July 2006, p. 25.
[108] Cf.: European public services, COM(2010) 744 final, Brussels, 16 December 2010; European Commission, A digital Single Market Strategy for Europe, COM(2015) 192 final, Brussels, 6 May 2015; Decision No. 922/2009/EC of the European Parliament and of the Council of September 2009 on interoperability solutions for European public administrations (ISA); Decision (EU) 2015/2240 of the European Parliament and of the Council, of 25 November 2015, establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA² programme) as a means of modernising the public sector; European Commission (2017), European Interoperability Framework Implementation Strategy, COM(2017) 134 final, Brussels, 23 March 2017.
[109] On the proposal on interoperability, cf. European Commission Press Release, "Security Union: Commission closes information gaps to better protect EU citizens", Strasbourg, 12 December 2017.
[110] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems, COM(2017) 793 final and COM(2017) 794 final, Strasbourg and Brussels, 12 December 2017, p. 3. For issues that arise with LE-access to non-LE databases, cf.: Paul De Hert and Serge Gutwirth, "Interoperability of Police Databases within the EU: An Accountable Political Choice?", in: International Review of Law, Computers & Technology, Volume 20, Nos. 1 and 2, pages 21-35, March-July 2006, p. 27 ff.

authorities could be granted access to data for the prevention, investigation, detection or prosecution of serious crime and terrorism, without passing the current process of prior verification of national databases.

The interoperability proposal includes two Regulations, one[111] concerning the Schengen Acquis, which will cover the EES, the VIS, ETIAS and those parts of SIS II that deal with border control cooperation. The scope of the second Regulation[112] applies to Eurodac, the so-called 'police Schengen'[113] and ECRIS-TCN. Apart from their scope, the Regulations may be regarded as more or less identical 'sister Regulations' that achieve full interoperability of all underlying systems when being read together.

The four main components that are supposed to be established under the interoperability are a **European Search Portal (ESP)**, a shared **Biometric Matching Service (BMS),** a **Common Identity Repository (CIR)**, and a **Multiple Identity Detector (MID)**.[114]

The **ESP**, as a central infrastructure shall enable competent authorities the simultaneous querying of the underlying systems.[115] Instead of queries being carried out in eight different databases separately, searches via the ESP will be systematically conducted within all systems in parallel using both biographical and biometric data, and the combined results will be displayed on one single screen.[116] The results shown shall solely contain the data to which the end-user has access according to his or her access rights under the provisions of the underlying databases.

The **BMS** will create a common platform that uses data from the Central-SIS, Eurodac, the EES, VIS and the proposed ECRIS-TCN[117] to generate and store biometric templates.[118] The BMS seeks to make the identification of TCNs more reliable by automatically comparing biometric data in all connected systems with the biometric templates, thereby substituting the checking of each underlying database in five separate searches.

Connected to the ESP, the BMS and the MID, as well as to the central systems of the EES, Eurodac, the VIS, the proposed ETIAS, and the proposed ECRIS-TCN[119], the **CIR** will create an individual file for each person registered in the five databases and store their data in a central repository.[120] The individual files shall contain both biometric and biographical data as well as a reference indicating the system from which the data were retrieved.

[111] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, COM(2017) 793 final, Strasbourg, 12 December 2017.

[112] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), COM(2017) 794 final, Brussels, 12 December 2017.

[113] Council Decision 2007/533/JHA on LE cooperation and, in the future, the proposed SIS II Regulation on Police Cooperation, COM(2016) 883 final.

[114] Interoperability proposal, Articles 6, 12, 17 and 25, COM(2017) 794 final. Cf. European Commission Factsheet, "Security Union-Interoperability of EU Information Systems", October 2017. Cf.: High-Level Expert Group on Information systems and interoperability. Final Report May 2017, p. 28-30.

[115] The EES, VIS, Eurodac, SIS II, the proposed ETIAS, the proposed ECRIS-TCN, the Common Identity Repository as well as Europol data and the Interpol database on Stolen and Lost Travel Documents (SLTD).

[116] European Commission Fact Sheet "Frequently asked questions: Interoperability of EU information systems for security, border and migration management", Strasbourg, 12 December 2017.

[117] The proposed ETIAS will not store biometric data and will, therefore, not be linked to the shared BMS.

[118] The biometric data (fingerprint and facial images) are exclusively retained by the underlying systems. The shared BMS would create and retain a mathematical representation of the biometric samples (a template) but would discard the actual data. According to the proposal, these data are not personal data.

[119] The CIR would not contain data from the SIS II system, as the architecture of the SIS is too complex and not technically feasible to be included within the CIR, COM(2017) 794 final, p. 7.

[120] Article 17 (2)(a) of the interoperability proposal, COM(2017) 794 final.

The main purposes of the CIR are to facilitate the correct identification of TCNs and supporting the detection of false identities.[121] Moreover, the CIR shall contribute to simplifying and streamlining LE-access to non-LE databases for the prevention, investigation, detection or prosecution of serious crime.[122]

Data stored in the CIR will be searched along a two-step approach where, in a first step, the system(s) holding data that correspond to the input information will be indicated to the querying user. In a second step, the user may request access to each individual system that contains the matching data. Access would remain subject to prior authorization by a verifying authority, along the access provisions of the underlying systems.[123] According to the proposals, the two-step approach would be particularly valuable in situations where criminals or victims are unknown, and would make the current cascade of checking national databases prior to searching the EU systems superfluous. [124]

An extension to the BMS, the **MID** uses the alphanumeric data stored in the CIR and the SIS in order to detect multiple identities.[125] Where identical data exist in more than one system and can be associated to the same person, the MID creates white, green, yellow and red links that indicate whether the different identities are likely to be lawfully referring to the same person, or whether there is suspicion of identity fraud.[126] Pursuant to Article 30 of the interoperability proposal, yellow links are to be verified manually[127] in order to ascertain whether a person was registered either lawfully or unlawfully under multiple identities. A yellow link forces the verifying authority to improve the accuracy of the data and change the colour into either white, green or red. While a change to a green or a white link would signify that the person was registered lawfully under multiple identities, a red link would require further action concerning identity fraud in accordance with Union or national law.[128]

5.1 General issues of the interoperability proposal

According to the proposal, interoperability would improve decision-making processes and increase the accuracy of alphanumeric data[129] where the latter are systematically matched against biometric data.[130] The extended use of biometric data to identify TCNs would render identification more reliable and lead to more accurate results.[131] This would not only be beneficial for the authorities processing personal data of TCNs, but would accelerate the average time to process travel or visa applications, reduce waiting times at border crossing points and distinguish

[121] COM(2017) 794 final, p. 7.
[122] Article 17(1) of the interoperability proposal, COM(2017) 794 final.
[123] COM(2017) 794 final, p. 8.
[124] COM(2017) 794 final, p. 9.
[125] A multiple identity detection shall be launched where an application for international protection had been created in Eurodac, an alert in the SIS is created or updated, or where data is recorded or updated in the ECRIS-TCN. Where these systems under the CIR or the SIS II contain biometric data, the multiple identity detection will be carried out by the BMS.
[126] In accordance to Article 30, 31, 32 and 33 of the interoperability proposal, the links are yellow, green, red or white. Both red and yellow links shall be verified manually in order to ascertain whether a person uses different identities unlawfully. The links are stored in the CIR.
[127] By the authorities competent to assess a request for international protection (Eurodac), the Sirene Bureaux of the Member States (SIS II on police cooperation) and the central authorities of the convicting Member State (ECRIS-TCN) pursuant to Article 26 of the Interoperability proposal on police cooperation. The border authority creating or updating a file in the EES, competent authorities creating or updating a file in the VIS, ETIAS Units where hits on alerts occur and Sirene Bureaux (SIS II on border checks) in accordance with Article 29 of the interoperability proposal concerning borders and visas.
[128] Article 32(2) of the interoperability proposals, COM(2017) 793 final and COM(2017) 794 final.
[129] Inaccuracies of alphanumeric data are common due to spelling errors, lack of documents provided, insufficient language skills, technical deficiencies, incorrect transcription of names into the Latin alphabet, cultural norms determining the usage of first and second names, recording of birth dates when the precise date is unknown, lack of training, or in situations where the common format for data transmissions is not followed. In: FRA 2017 Report, "Fundamental rights and the interoperability of EU information systems: borders and security", July 2017, p. 30.
[130] Alphanumerical data can be unreliable for establishing the identity of a person, due to so-called aliases, cases of identity fraud, or entry and spelling mistakes and might lead to matches connected to the wrong person. FRA 2017 Report, p. 20. Although biometric data are considered very reliable, many factors may influence the quality of e.g. finger print data, for instance, age, manual work, humidity, dry, wet and untidy fingertips, unintentional as well as deliberate injuries to the fingertips, lack of training and technical difficulties, cf. FRA 2017 Report, p. 31.
[131] Paul De Hert and Serge Gutwirth, "Interoperability of Police Databases within the EU: An Accountable Political Choice?", in: International Review of Law, Computers & Technology, Volume 20, Nos. 1 and 2, pages 21-35, March-July 2006, p. 26, 27.

between *bona fide* and unauthorized travellers. The cross-checking of databases could facilitate the detection of false identities and forged documents, or be used to prevent the re-entry of criminals and rejected asylum seekers. It could contribute to an enhanced detection of missing children, confirm the accuracy of asylum claims and discover victims of human trafficking.

However, if the underlying systems hold inaccurate data, which currently is the case,[132] combining these data will lead to irregularities, wrongful matches and a significant amount of false hits instead of facilitating decision-making and improving data quality.

The current silo system of EU databases was not intended to be interoperable, as each database, besides being set up for a specific purpose, has its own data protection framework with appropriate retention periods:[133] The purposes of each database are defined in a corresponding legal instrument that provides for specific safeguards concerning data security, access and supervision. The purpose limitation principle, which stipulates that personal data must be collected for 'specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes'[134], might be undermined where the boundaries between migration management and the *fight against terrorism* are increasingly being blurred.[135]

The **ESP** as the main tool to consult all underlying IT-systems at once is not problematic as such, provided that access rights are strictly adhered to and that its future use in connection with the BMS, the CIR and the MID complies with the purpose limitation principle.

Quite alarming, however, is the fact that with the CIR, the BMS and the MID, the interoperability proposal establishes three entirely new centralized large-scale databases, without having carried out a thorough impact assessment for each single component at the time the proposal was published.[136]

The generation of biometric templates that are to be stored in the **BMS** constitutes a new data processing operation, for which the interoperability proposal does not provide a legal basis. Furthermore, and despite the assertion that the biometric templates stored in the BMS are not (sensitive) personal data[137], the risk of re-identification of individuals cannot be completely eliminated.

The **CIR** stores both biographical and biometric data, the processing of the latter being generally prohibited unless sufficiently justified and strictly necessary. Moreover, the CIR will replace the central systems of the underlying databases and instead create a centralized system, which will be more prone to security breaches. With an abolition of the prior checking of national databases before accessing the CIR, the proposal will eliminate an important data protection safeguard. Necessity and proportionality to curtail the cascading system would, however, only be justifiable if the latter procedure was proven to be too burdensome and to undermine the work of LE authorities.

The **MID** will not allow the retention of personal data *per se*, but store so-called identity confirmation files that contain the links between data stored in the CIR and the SIS. Further, the MID-identity confirmation files include a reference to the databases holding the matching data and an identification number with which that data may be retrieved.[138]

Pursuant to Article 26 of the interoperability proposal, Member State authorities and EU bodies having access to at least one EU information system included in the CIR or to the SIS shall have access to MID-identity confirmation files where there is suspicion that different biographical identities are unlawfully used by the same

[132] Eu*observer*, "Inaccurate data in Schengen system 'threatens rights'", 8 January 2018. https://euobserver.com/tickers/140468.
[133] While the retention period of data in Eurodac is currently ten years, retention periods for data in SIS II differ from the types of alerts and the national rules in the MS, in the Visa Information System data is to be stored for a maximum period of five years.
[134] More details on this, cf. Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, p. 3.
[135] EDPS Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017, p. 9.
[136] Refer to point 5.2 and 5.3. of the Impact Assessment for the interoperability proposal, SWD(2017) 473 final, Strasbourg, 12 December 2017, p. 23.
[137] COM(2017) 794 final P. 7.
[138] Article 34 of both interoperability proposals, COM(2017) 793 final and COM(2017) 794 final.

person.[139] The manual verification of whether multiple identities are used unlawfully shall be carried out by the authority creating or updating files, applications or alerts in the underlying systems.[140]

This means that where a LE authority, creating an alert in the SIS, receives a match with data in Eurodac via the MID, it would be authorized to inspect the identity confirmation files stored in the MID and further access the Eurodac for verification purposes. This would entail similar issues as those arising with the two-step approach under the CIR regarding LE-access to non-LE databases. Although in the case of the MID LE-access would be justified for the detection of identity fraud, it is likely that comparisons of alphanumeric data will detect a great number of MID-links that need to be verified manually and eventually lead to disproportionate processing of personal data.

5.2. Issues of the interoperability proposal related to LE-access

One of the objectives of the interoperability proposal is to facilitate and streamline access by LE authorities to EU IT-systems that are not exclusively established for the purpose of the prevention, investigation, detection or prosecution of serious crime.[141] In addition, the obligatory launch of prior searches in national databases shall progressively be abolished once the two-step-approach through the CIR has become operational.[142]

The purpose limitation principle has particular relevance in the context of LE-access to the individual IT-systems, as their primary purpose, except for the SIS II, are of non-LE nature. Although the access rights of the respective underlying databases continue to be applicable in an interoperable framework, the two-step approach for the CIR, showing hits for matching data in all systems, might provide LE staff with information that they may not have the right to access within their competences. Though such information is not personal data, a flagged hit would reveal information that may prompt an officer to draw certain conclusions concerning a TCN. This might not represent a direct interference with the right to the protection of personal data, but certainly limit the right to privacy under Article 7 of the EU Charter without a valid justification.

It is crucial that access rights are verified thoroughly and that the conditions for logging and supervision under the interoperability proposal are strictly complied with in order to effectively protect personal data against unauthorized access and the risk of abuse.[143]

The verification of access is *already* commonly disregarded, and unauthorized personnel easily obtain personal data indirectly.[144] Where strict access requirements are circumvented by officers who request indirect access via colleagues who have wider access permissions and forward information that should not be accessible to the requesting officer, severe sanctions should be imposed.[145] This should specifically be the case for interoperable systems, as even more information would be available to share.

In addition, a police officer, checking data for immigration purposes, could discover links to a person in LE databases and easily end up in a situation where it is not clear which legal instrument applies for accessing the data. While for data processing operations relating to immigration and asylum the GDPR would be applicable, data processed for LE purposes would fall within the scope of the LE-Directive. The unclear delineation between the Regulation and the Directive could easily lead to the application of the wrong instrument and a lowering of data protection rights for individuals where a police officer applies the rules under the Directive instead of the Regulation.[146]

---

[139] Thus, these authorities should, according to Recital (41), solely have access to so-called red links, where the linked data shares the same biometric, but different identity data.
[140] Article 29 of the interoperability proposal, COM(2017) 794 final.
[141] Recital (24) of the interoperability proposal, COM(2017) 794 final.
[142] Recital (34) of the interoperability proposal. Also see page 9 of the same, COM(2017) 794 final.
[143] Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd and Seitlinger and Others* and para. 54 with further references.
[144] FRA 2017 Report on Interoperability, p. 25.
[145] Ibid, p. 26.
[146] Cf. in other contexts, Thomas Marquenie, "The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework", in: Computer Law & Security Review Volume 33, Issue 3, June 2017, Pages 324-340.

In a different scenario, a police officer could check TCNs' personal data in a LE database without evidence that the individual concerned may present a risk for public security. The officer could base the processing operation on a 'probable cause' and process data under the Directive. This may cause issues in the light of the purpose limitation principle and traditional police investigations via criminal records, set up for very strict purposes, would be substituted or even replaced by intelligence-based searches within different databases.

With interoperable databases the risk of a 'function creep' rises where systems that were originally intended to perform narrowly specified functions are extended to combine different steps of data analysis at once. Furthermore, interoperability would presumably widen the circle of actors with authorized access to databases and would streamline LE-access. This could be detrimental to effective LE-cooperation, as the reluctance of some authorities to share information could increase if they know that the data may be made available to more actors in other Member States.[147] Therefore, interoperable databases push the limits of the EU legal framework that was set up to protect personal data and privacy rights.[148]

6. Conclusion

The fundamental concern that emerges with the proposed system of interoperable databases is the circumvention of the purpose limitation principle, stipulated in Article 8(1) of the EU Charter. Interoperability creates new processing operations that are not covered by existing legal bases and provides information to authorities that would normally not be allowed to access the underlying system storing certain data.[149] The right to the protection of personal data is not an absolute right. However, new processing operations must be sufficiently justified and need to have undergone a necessity and proportionality assessment.[150]

Interoperability will fundamentally change the current architecture of EU large-scale IT-systems and introduce a shift from separated silos to an interconnected framework, where personal data would be stored on a centralized basis. While offering huge benefits for competent authorities, streamlined access rights and new processing operations might lead to a risk of function creep through the widening of the purpose of the system or the purpose for which data processing is carried out.

There is a need to balance between the ability of LE authorities to effectively carry out their work and the interests of individuals not to become subject to unfair processing. Despite the current terrorist threat in many Member States and increased security challenges due to migration flows to the EU, it is important to respect the fundamental rights granted to everyone in the Union.

While it is true that the fight against crime and threats to public security is an objective of general interest of the EU and capable to justify even serious interferences with fundamental rights[151], processing must be carried out in a proportionate manner and be strictly necessary in order to avoid inadequate and unfair processing of personal data.

Moreover, risks of discriminatory profiling have to be mitigated in order to avoid the creation of different data protection standards for EU citizens and TCNs, unless such different treatment is solidly justified. Non-discrimination standards, the security and integrity of personal data, oversight mechanisms, transparency requirements and rights for data subjects must be complied with to make existing and proposed databases, as well as interoperability compliant with the legal framework.

---

[147] Sergio Carrera, Elspeth Guild and Valsamis Mitsilegas, "Reflections on the Terrorist Attacks in Barcelona Constructing a principled and trust-based EU approach to countering terrorism", No 2017-32 / August 2017, p. 8.
[148] Dennis Broeders, "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants" International Sociology, Vol. 22, Issue 1, 2007, p. 81.
[149] EDPS Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017, p. 12.
[150] Interferences may be justified if they are proportionate, provided for by law, genuinely meet the objectives of a general interest or the need to protect the rights and freedoms of others, Article 52(1) EU Charter.
[151] C-293/12 and C-594/12, *Digital Rights Ireland and Others*, paras 42 and 44; C-601/15, *PPU*, EU:C:2016:84, para 53 and *Opinion 1/15*, para 149.

The need to adopt the least intrusive measures to achieve the wider objectives of border control, immigration and effective police cooperation, while trying to find a way to make these measures compatible with fundamental rights[152], is indispensable for interoperable databases to be compliant with both EU data protection standards and the requirements of the CJEU. This includes the definition of a specific purpose and the implementation of adequate safeguards, all of the latter in combination with a necessity and proportionality test.

In this context, it would be worthwhile considering the possibilities that already exist in terms of data analysis, to fully exhaust the existing databases and to reduce incorrect data that impede the work of competent authorities, before investing into new systems that do not keep up with the standards set by the CJEU.[153]

[152] Not only data protection and privacy rights, but also the right to a fair trial, presumption of innocence, or the right to good administration enshrined in Articles 8, 47, 48 and 41 of the EU Charter respectively.

[153] A problem per se is combining all databases through interoperability because abuses then have a much higher dimension. The same goes for potential security breaches which again have a greater impact. Incorrect data and mistakes in one database will impact all other databases and ultimately the individual. On the other hand, the Commission argues that the combination of data leads to the correction of errors, which is a valid argument.