Teresa Quintel

The Impact of Interoperability on the processing of (Biometric) Data of Third Country Nationals by Europol*

Zusammenfassung

Am 12. Dezember 2017 legte die EU-Kommission einen Vorschlag zur Interoperabilität von EU-Informationssystemen vor. Den vorgeschlagenen Maßnahmen zufolge sollen alle zentralisierten EU-Datenbanken in den Bereichen Sicherheit, Grenzschutz und Migrationssteuerung bis 2020 miteinander verknüpft werden. In den zugrundeliegenden IT-Systemen werden personenbezogene Daten von Drittstaatsangehörigen wie Reisenden und Asylbewerbern, Informationen zu Visumsanträgen oder Daten über vermisste Personen und Kriminelle gespeichert.

Im Zuge der Interoperabilität würden Daten, die sich zuvor in getrennten Systemen befanden, in drei neuen zentralisierten Datenbanken gespeichert und leichter zugänglich sein, auch zum Zweck der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten. Während die Suche personenbezogener Daten bei strafrechtlichen Ermittlungen zurzeit noch eine vorangegangene Abfrage in separaten Datenbanken erfordert, soll diese abstufende Sicherheitsmaßnahme schrittweise aufgegeben werden, um sicherzustellen, dass Grenzschutz, Polizeibeamte und Europol Zugang zu allen relevanten Informationen erhalten. Neben vereinfachten Zugangsbedingungen würde dies neue Verarbeitungsvorgänge schaffen, für welche die vorgeschlagenen Maßnahmen keine adäquate Rechtsgrundlage bieten.

Dem Vorschlag zufolge würde die Verknüpfung der relevanten Datenbanken die Genauigkeit alphanumerischer Daten verbessern, soweit diese systematisch mit biometrischen Daten abgeglichen würden. Die Verarbeitung biometrischer Daten birgt jedoch besondere Risiken, da diese zur eindeutigen Identifizierung einer Person beitragen und generell unveränderbar sind. Dementsprechend kann die Erfassung und Analyse biometrischer Daten weitreichende Konsequenzen für die betroffene Person zur Folge haben.

Die relevanten EU-Datenschutzgesetze definieren biometrische Daten als besondere Kategorien personenbezogener Daten, deren Verarbeitung geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen erfordert. Folglich ist es bemerkenswert, dass biometrische Daten unter der Europol Verordnung nicht als besondere Kategorien personenbezogener Daten gelten: Im Rahmen der Europol Verordnung können alle personenbezogenen Daten zur Ermittlung etwaiger Zusammenhänge oder anderer relevanter Verbindungen zwischen Informationen in Bezug auf Personen, die einer Straftat oder der Beteiligung an einer Straftat verdächtigt werden oder die wegen einer solchen Straftat verurteilt worden sind, gleichermaßen verarbeitet werden.

---

* Teresa Quintel, LL.M. is an FNR-funded Ph.D. student at the University of Luxembourg and Uppsala University under co-supervision of Prof. Mark D. Cole and Assistant Prof. Maria Bergström.

KritV 4/2018, DOI: 10.5771/2193-7869-2018-4-332

Dieser Artikel erörtert zwei Defizite, die bei der Verknüpfung von EU Datenbanken berücksichtigt werden sollten. Zum einen entstehen durch die Schaffung von drei neuen Datenbanken, die große Mengen an biometrischen Daten speichern und zusätzliche Arten von Verarbeitungsvorgängen ermöglichen, erhebliche Bedenken, da eine adäquate Rechtsgrundlage fehlt. Zum anderen wären die zusätzlichen Verarbeitungsmöglichkeiten von biometrischen Daten durch Europol datenschutzrechtlich problematisch, da die Europol Verordnung einen unzureichenden Schutz für besondere Kategorien personenbezogener Daten gewährt.

Résumé

Le 12 décembre 2017 la Commission de l'Union Européenne déposait une proposition relative à l'interopérabilité des systèmes d'information de l'Union Européenne. La proposition prévoit que tous les systèmes d'information centralisés de l'Union Européenne concernant la sécurité, la protection des frontières et le contrôle de l'immigration soient d'ici 2020 connectés entre eux. Dans les systèmes informatiques sous-jacents, seront sauvegardées des informations relatives à des personnes venant d'États tiers comme les voyageurs et les demandeurs d'asile, des informations concernant des demandes de visas, des personnes disparues ou des criminels.

Dans le sillon de la mise en place de l'interopérabilité, des données qui se trouvaient jusque là dans des systèmes étanches, seront engrangées dans trois nouvelles bases de données centralisées, devenant ainsi accessibles, y compris dans le cadre de la prévention des crimes et délits, des enquêtes et des poursuites les concernant. La recherche de données personnelles en matière d'enquêtes pénales exige actuellement des demandes préalables auprès de différentes bases de données. Cette mesure de protection organisée en échelons doit être progressivement abandonnée afin d'assurer à la protection des frontières, aux fonctionnaires de police et à Europol l'accès à tous les informations d'importance. Ainsi seraient simplifiées les conditions d'accès mais cela engendrerait de nouveaux procédés de traitement pour lesquels les mesures proposées ne prévoient pas de fondement juridique convenable.

Selon la nouvelle proposition la connexion entre les bases de données ferait progresser l'exactitude des données alphanumériques, dès que celles-ci seraient comparées à des données biométriques. Cependant le traitement de données biométriques recèle un danger spécifique, celui de contribuer à une identification sans équivoque d'une personne particulière; de plus elles sont en général immuables.

La règlementation européenne sur la protection des données définit les données biométriques comme une catégorie particulière de données personnelles, données dont le traitement exige une garantie appropriée des droits et libertés de la personne en question. A ce niveau il convient de relever que le règlement relatif à Europol ne considère pas les données biométriques comme une catégorie particulière de données personnelles: il permet l'utilisation des données personnelles d'une manière égale pour les besoins relatifs à une quelconque enquête, ou une recherche de liens entre des informations concernant des personnes soupçonnées d'avoir commis un crime ou délit ou d'y avoir participé, ou encore des personnes condamnées pour crime ou délit.

La contribution suivante s'attache à deux insuffisances dont la prise en considération dans la connexion des bases de données européennes s'impose. D'une part la création de trois nouvelles bases de données qui sauvergardent une grande quantité de données biométriques et rendent possible des formes supplémentaires de moyens de traitement, engendrent de sérieuses inquiétudes du fait de l'absence d'une base juridique adéquate. D'autre part l'utilisation par Europol des moyens de traitement supplémentaires des données biométriques poserait un problème du point de vue du droit de la protection des données, puisque le règlement Europol n'offre qu'une protection insuffisante quant aux catégories particulières de données personnelles.

Introduction

On 12 December 2017, the EU Commission presented two proposals on the interoperability of EU large-scale Information Systems. The proposals seek to enable all centralised EU databases for security, border and migration management to be fully interconnected by 2023.

The underlying IT-systems mainly 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 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 national law enforcement authorities (LEAs) and Europol. Despite simplified access conditions, this would require new types of processing operations for which the interoperability proposals do not provide a legal basis.

According to the proposals, interoperability would improve the accuracy of alphanumeric data where these are systematically matched against biometric data. However, the processing of biometric data always bears particular risks for data subjects, as they uniquely identify a natural person. Consequently, any bulk collection and analysis of TCNs' biometric data may lead to adverse effects that might be in violation of the EU Charter of Fundamental Rights (EU Charter).

The relevant EU data protection instruments define biometric data as *special categories of data*, which merit particularly strong protection and additional procedural safeguards. Yet, it is noteworthy that, in contrast to these instruments, the Europol Regulation does not treat biometric data as special categories of data: Under that Regulation, all personal data may be processed for the purpose of identifying links between information related to persons who are suspected of having committed a crime, or regarding whom there are factual indications to believe that they may commit criminal offences.

This article addresses two major deficiencies that should be taken into account when implementing interoperability. On the one hand, the concerns that will arise with the creation of two entirely new databases that will store biometric data in bulk and allow for additional types of processing operations for which a legal basis is lacking. On the other hand, the new possibilities for Europol to process such data that

will become problematic from a data protection point of view due to the insufficient protection of special categories of data under the Europol Regulation.

Following a general overview of the situation concerning data management on EU level (section I.) and a brief description of the different interoperability components under section II. and II.1., the article will address the concerns arising with an interoperable system (section II.2.) and the processing of biometric data under the proposed framework (section II.3.). Sections III, III.1, III.2 and III.3. focus on Europol, the agency's possibilities to process data under Regulation (EU) 2016/794[1] and the shortcomings of the Europol Regulation with regard to the protection of biometric data. Sections IV. and IV.1. deal with Europol access to EU databases and the proposed interoperability framework.

I. Background: Data for migration management

Being able to generate in-depth knowledge of migration routes and improving the identification of individuals enhances the control over TCNs coming to the EU and unfolds possibilities to better monitor immigration.[2] Competent authorities collect, analyse and share personal data of visa required and visa exempted travellers, asylum seekers, *irregular* migrants,[3] or information on persons illegally staying within the territory of the EU. These data are stored in EU databases that grant access to staff of competent authorities such as border guards, or visa and asylum authorities in accordance with the particular purposes for which the databases were established. In addition, national LEAs and Europol may request access to retained data for the purposes of the prevention, detection and investigation of terrorist offences or other serious crime.

Thus, the management of the EU's external border control, visa, asylum and immigration related security measures strongly relies on large-scale IT systems whenever decisions concerning persons coming to the EU are taken. Systems that were developed with a view to monitor migration and asylum, to facilitate the implementation of the European visa policy, or to improve the exchange of personal data between LEAs exist since over a decade. However, in the past years, and particularly during the aftermath of the so-called *migration crisis* in 2015, the Commission has presented legislative amendments on the revision of existing databases and proposed new systems. These proposals introduce new purposes for processing, add more categories of data to be retained and progressively widen provisions on access to data by LEAs and Europol.

1 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/ JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L 135/53. (Hereafter: Europol Regulation).

2 Dennis Broeders, "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants" International Sociology 2007; 22; 71, p. 89.

3 The EU Commission defines irregular migration as 'movement of persons to a new place of residence or transit that takes place outside the regulatory norms of the sending, transit and receiving countries', https://ec.europa.eu/home-affairs/content/irregular-migration-0_en.

I.1. EU databases

At the moment, the operative EU databases are the *Schengen Information System* (SIS II),[4] which comprises two Regulations[5] and one Council Decision[6] concerning border control, cooperation on vehicle registration and law enforcement cooperation,[7] the *Visa Information System* (VIS),[8] a large-scale IT-system seeking to facilitate the administration, issuance and checks of short-stay visas to the Schengen area, and *Eurodac*,[9] which assists the implementation of the Dublin system by determining the Member State responsible for processing an asylum application. The VIS[10] and Eurodac[11] are currently under revision: an updated Eurodac Regulation was published in 2016, the proposal for the revision of the VIS issued in May 2018 and on 19 November 2018, the Council adopted three new SIS Regulations, strengthening the use of the Schengen Information System for police cooperation, borders checks and return purposes.[12]

4 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.

5 Regulation (EC) No 1987/2006 **(**Border control cooperation), Regulation (EC) No 1986/2006 **(**Cooperation on vehicle registration**).**

6 Council Decision 2007/533/JHA (law enforcement cooperation).

7 European Commission, "Schengen Information System," Migration and Home Affairs – European Commission, December 6, 2016, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en.

8 Regulation (EC) No 767/2008 of the European Parliament and of the Council 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 P. 120 – 141.

9 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 (recast), OJ L 180/1.

10 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM(2018) 302 final, Brussels, 16.5.2018.

11 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, 4.5.2016.

12 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)

In the future, the *Entry/Exit System* (EES),[13] which was adopted in October 2017,[14] shall contribute to an enhanced management of the external Schengen borders, prevent irregular immigration and facilitate the management of migration flows.[15] The EES will apply to visa-exempted TCNs as well as those persons who are admitted for a short stay of maximum 90 days within any 180-day period in the EU and allows for the tracking of entries and exits to and from the Schengen Area.

In addition, the Commission proposal for a *European Travel Information and Authorization System* (ETIAS)[16] was adopted in September 2018. Like the EES, ETIAS is supposed to improve the management of the external Schengen borders, avert irregular immigration and ease the management of migration flows.[17] ETIAS formally entered into force in October 2018, but will not become operational before 2021.[18]

The *European Criminal Records Information System for Third Country Nationals and stateless persons* (ECRIS-TCN),[19] which is a centralized system for the exchange of criminal records on convicted TCNs was proposed in June 2017.[20] In September 2018, the Council proposed to include information of both third country nationals

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.

13 Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 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 and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, OJ L 327.

14 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.

15 European Commission, "Security Union: Commission welcomes adoption of Entry/Exit system for stronger and smarter EU borders", Brussels 25 October 2017.

16 Regulation (EU) 2018/1240 of the of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, L 236, 19 September 2018.

17 European Commission, "Security Union: Commission welcomes adoption of Entry/Exit system for stronger and smarter EU borders", Brussels 25 October 2017.

18 European Parliamentary Research Service (EPRS), European Travel Information and Authorisation System (ETIAS)', 18 October 2018, PE 599.298, p. 1.

19 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.

20 Cf.: 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.

(TCN) and dual nationals.[21] In December 2018, Council and EP negotiators agreed on the inclusion on the ECRIS-TCN into the existing ECRIS.[22]

I.2. The developments towards Interoperability

Against the background of reinforcing the EU's internal security and due to the insufficient capability of EU databases to exchange information between each other, the Commission presented, in April 2016, a *Communication on Stronger and smarter information systems for borders and security*[23] to address a number of structural shortcomings[24] related to the functioning of EU databases.[25] As one of the long-term objectives, the communication named the need to improve the interoperability of EU large-scale information systems.[26] Interoperability is commonly referred to as the ability of different information systems to communicate, exchange data and use the information that has been exchanged.[27] Others describe it as the possibility to analyse data sets without an additional procedural burden.[28] With interoperability, the Commission sought to tackle deficiencies and gaps caused by the fragmented regime of information systems at EU level.[29]

In June 2016, a Commission Decision[30] established the high-level expert group on information systems and interoperability, which, in May 2017, published its final report putting forward recommendations concerning the interoperability of EU information systems.[31]

---

21 Union citizens that also have the nationality of a third country, see: Council Document 11310/18 of 6 September 2018.

22 Cf.: Teresa Quintel and Juraj Sajfert on the applicability of Article 10 GDPR for the processing of personal data stored in the European Criminal Records System (ECRIS) and ECRIS-TCN, in a Commentary on the General Data Protection Regulation, Edward Elgar Publishing (forthcoming 2019).

23 Communication from the European Commission to the European Parliament and the Council, 'Stronger and Smarter Information Systems for Borders and Security', COM(2016) 205 of 6 April 2016.

24 (1) Sub-optimal functionalities in some of the existing information systems; (2) information gaps in the EU's architecture of data management; (3) a complex landscape of differently governed information systems; and (4) a fragmented architecture of data management for borders and security where information is stored separately in unconnected systems, leading to blind spots.

25 COM(2017) 793 and 794 final, Brussels, 12.12.2017.

26 Ibid, p. 2.

27 European Data Protection Supervisor (EDPS), "Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice", 17 November 2017. P. 6.

28 Daniel Drewer, Vesela Miladinova: 'The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation', computer law & security review 33 (2017) 298–308, p. 305.

29 COM(2016) 205 of 6 April 2016, p. 15.

30 Commission Decision of 17 June 2016 setting up the High Level Expert Group on Information Systems and Interoperability, 2016/C 257/03, 15 July 2016.

31 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

In December 2017, the Commission eventually presented two proposals[32] on the interoperability of EU large-scale Information Systems.

The proposals include two Regulations, one concerning the *Schengen Acquis*, which will cover the EES, the VIS, the ETIAS and those parts of the SIS II that deal with border control cooperation. The scope of the second Regulation applies to Eurodac, the so-called 'police Schengen' and the 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.[33]

The underlying IT-systems predominantly retain data of TCNs, namely travellers, applicants for international protection, information relating to visa applications or data on missing persons and criminals. However, connected to the SIS II, the interoperable system would also make data of EU citizens related to whom SIS II-alerts exist searchable. Moreover, the Council proposed to insert a provision that would include dual nationals in the ECRIS-TCN,[34] and the VIS shall be expanded to contain information on long-stay visas and residence permits under the revised regulation.[35]

With interoperability, data, once held within the silos structure of disconnected databases, would be retained in a new centralized database and would become more easily accessible, also for the prevention, investigation and prosecution of crime. Two additional central databases would be established to facilitate the querying of individuals via biometric identifiers for the detection of multiple identities and identity fraud. Where criminal investigations previously required multiple searches in separate databases, this cascading safeguard would progressively be abandoned to streamline access to personal data by LEAs and Europol.

Hence, all existing and adopted systems (Eurodac, SIS II, VIS, EES and ETIAS) as well as the proposed ones (Eurodac, VIS and ECRIS-TCN) grant Europol access to personal data for the purposes of the prevention, detection or investigation of terrorist offences or other serious crime.

I.3. Processing Biometric Data by Europol

As so-called information hub, Europol supports the exchange of information and personal data between national police authorities via its Secure Information Exchange Network Application (SIENA).[36] The Europol Information System (EIS)[37] is the

32 European Commission Fact Sheet, 'Frequently asked questions – Interoperability of EU information systems for security, border and migration management', Strasbourg, 12 December 2017; http://europa.eu/rapid/press-release_MEMO-17-5241_en.htm.

33 Teresa Quintel, 'Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention' (March 1, 2018). University of Luxembourg Law Working Paper No. 002-2018. Available at SSRN: https://ssrn.com/abstract=3132506 or http://dx.doi.org/10.2139/ssrn.3132506.

34 See Article 2(2) and Article 7(2 a) of Council Document 11310/18 of 6 September 2018.

35 Meaning that information regarding possible relationships to EU citizens will be stored in the systems. See: Vis Proposal, COM(2018) 302 final, Brussels, 16.5.2018, p. 6.

36 COM(2016) 205 of 6 April 2016, p. 6.

37 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing

agency's central criminal information and intelligence database, allowing Member States to retain and consult data concerning serious crime and terrorism. Europol, however, remains the sole data controller of the EIS, thus determining the purposes of the processing. The interoperability proposals foresee to include the EIS as one of the databases to be queried where a search would be launched via the interoperable components.

Having permission to consult all underlying databases, Europol would be granted access to the interoperable system, to process both alphanumeric and biometric personal data within its mandate.

The different components established under the interoperability proposals and the underlying databases feeding these components are increasingly based on biometric data, the latter being considered a very reliable source to establish the identity of a person. In an interoperable system, alphanumeric data could be matched against biometric data in order to correct the former and render incorrect data retained in the systems more accurate. However, where systems contain a large amount of incorrect data, this could lead to wrong matches and the misidentification of TCNs.

Because of their sensitive nature and their potential to uniquely identify a natural person, biometric data are being defined as special categories of data under relevant EU legislation.[38] These instruments generally prohibit the processing of such data or require certain limitations and strict safeguards where such data are being processed.

This is not the case under the Europol Regulation, which does not define biometric data as special categories of data. Thus, the processing of biometric data by Europol staff does not require specific safeguards for the protection of such data. This may pose major concerns where Europol has access to biometric data that are being retained in the EU databases as well as in the interoperability components, as the agency would be permitted to process biometric data without the establishment of additional safeguards and specific procedural measures. Consequently, the protection of such data is insufficient under the Europol Regulation and therefore goes against the objectives of the EU Data Protection Reform, which entered into force in May 2018.[39]

II. Interoperability of EU databases

During recent years, the European Union has been faced with migratory challenges due to the increase of irregular border crossings into the Union. At the same time, the internal security of the EU has been threatened by a series of terrorist attacks in several Member States. These events reinforced the discussion on a strategy to strengthen the EU's information tools for border management, migration and security in order to make information exchange in the EU more effective and to enhance the pro-

and repealing Council Decisions 2009/371/ JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L 135/53, Art. 20 (2).

38 Most importantly Regulation (EU) 2016/679 and Directive (EU) 2016/680.

39 "2018 Reform of EU Data Protection Rules," Text, European Commission – European Commission, accessed May 9, 2018, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

tection of the Union's external borders.[40] Thus, the interoperability proposals were presented at a time when both national and European decision-makers were faced with enormous pressure to react to these challenges.

II.1. Components to be established under the Proposed Interoperability

The four main components that are supposed to be established under the interoperability proposals are a *European Search Portal* (ESP), a shared *Biometric Matching Service* (BMS), a *Common Identity Repository* (CIR), and a *Multiple Identity Detector* (MID).[41]

The ESP would be a single search interface that would enable end users to conduct parallel searches in all underlying information systems as well as certain Europol and Interpol data via a central infrastructure.[42] The searches in the ESP would be conducted systematically within all systems using both biographical and biometric data, and the combined results would be displayed on one single screen to the querying user(s). Thereby, the ESP would solely indicate the information held in the underlying systems to which the user would normally have access. Thus, the proposed access regime for the ESP builds on the existing access rights of the underlying databases.[43]

The BMS would establish a common platform that would use data from the Central-SIS, Eurodac, the EES, the VIS and the proposed ECRIS-TCN[44] to generate and store so-called biometric templates. Contrary to the Commission's assertion that the biometric templates that are to be stored in the BMS do not constitute sensitive data but merely a mathematical representation of the biometric samples,[45] both the former Article 29 Data Protection Working Party (WP29, now European Data Protection Board, EDPB) as well as the European Data Protection Supervisor (EDPS) maintained that the BMS establishes a common platform of biometric data.[46] According to the interoperability proposals, the BMS aims at increasing the reliability of data for

40 COM(2017) 794 final, Brussels, 12.12.2017, p. 1.

41 Interoperability proposals, Articles 6, 12, 17 and 25, COM(2017) 793 and 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.

42 Article 29 Data Protection Working Party opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration, Adopted on 11 April 2018 (WP29 Opinion), p. 3.

43 Teresa Quintel, Connecting Personal Data of Third Country Nationals in the Light of the CJEU's Case Law on Data Retention: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention (March 1, 2018). University of Luxembourg Law Working Paper No. 002-2018. Available at SSRN: https://ssrn.com/abstract=3132506 or http://dx.doi.org/10.2139/ssrn.3132506, p. 14.

44 The ETIAS will not store biometric data and will, therefore, not be linked to the shared BMS.

45 COM(2017) 793 final, P. 7.

46 WP29 opinion on Commission proposals on establishing a framework for interoperability between EU information systems, p. 6 and 7. EDPS opinion on the Proposals for two Regulations establishing a framework for interoperability, 19 (point 77).

the purpose of identifying TCNs by automatically comparing the biometric data stored in the connected systems with the biometric templates held in the BMS.

The MID would enable the CIR, the BMS and the SIS II to compare stored data and link different identities in order to detect identity fraud. The multiple identity detection would automatically be launched whenever data within the underlying systems would be added or updated, and the links between the identities would be stored in the MID.[47] Where identical data would exist in more than one systems and would be associable to the same person, the MID would create white, green, yellow and red links that would indicate whether the different identities are likely to be lawfully referring to the same person, or whether there is suspicion of identity fraud.[48]

The main objectives of the CIR are to facilitate the correct identification of TCNs and supporting the detection of false identities,[49] as well as simplifying and streamlining law enforcement access and Europol access to non-law enforcement databases for the prevention, investigation, detection or prosecution of serious crime.[50] The CIR would create an individual file for each person registered in the five underlying databases and would store both biometric and alphanumeric identity data extracted from these systems.[51]

The CIR would be connected to the other interoperability components, as well as to the central systems of the EES, Eurodac, the VIS, the ETIAS, and the ECRIS-TCN. Pursuant to Article 17 of the proposed Regulations, the CIR would retain certain data from the central systems of the underlying databases by replacing parts of the latter, which could lead to issues regarding the duplication of personal data.[52]

Data stored in the CIR would be searched by LEAs along a two-step approach where, in a first step, the system(s) holding data that correspond to the input information would be displayed to the querying user and, in a second step, access to each system that indicated a match would be requested individually.[53]

47 WP29 opinion on Commission proposals on establishing a framework for interoperability between EU information systems, p.8.

48 FRA Opinion 1/2018, 'Interoperability and fundamental rights implications. Opinion of the European Union Agency for Fundamental Rights', Vienna, 11 April 2018, p. 8.

49 COM(2017) 794 final, p. 7.

50 Article 17(1) of the interoperability proposal, COM(2017) 794 final.

51 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.

52 Teresa Quintel, 'comment on the EDPS and Article 29 WP opinions about the Commission proposals on interoperability of databases', EDPL (forthcoming), p. 8.

53 COM(2017) 794 final, p. 8. In June 2018, the Commission published two amended versions of the proposed interoperability Regulations. The amendments take into account the agreements reached on the SIS II and the ETIAS, and add, under Chapter IX of the original interoperability proposals from December 2017, changes to the SIS II Regulations and the ETIAS Regulation. In May 2018, the European Parliament and in June 2018, the Council issued their amendments to the proposals. In October 2018, the LIBE Committee voted on the amendments and the texts went into trilogue negotiations.

II.2. Issues arising with the proposed Interoperability Regulations

According to the proposals, interoperability could improve decision-making processes and increase the accuracy of alphanumeric data[54] where the latter are systematically matched against biometric data.[55] Consequently, the use of the biometric data held in all underlying databases (except for the ETIAS) to identify TCNs could render identification more reliable and lead to more accurate results.[56] 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, would reduce waiting times at border crossing points and help to distinguish 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 accelerated detection of missing children, confirm the accuracy of an asylum claim and detect victims of human trafficking.[57]

Yet, with the cross-checking and comparison of data in the interoperable system, the proposals would create new uses of personal data, without having established the proportionality and necessity of such processing operations. In addition, the requirement to put forward clearly defined purposes for new processing operations seems to be lacking in certain provisions and the generally vague purposes are not sufficiently justified in the Commission's impact assessment.[58] For instance, it has been put forward that the purposes of combating irregular migration and contributing to a high level of security are too broad and do not fulfil the requirements of being 'strictly re-

54 Inaccuracies of alphanumeric data are common due to spelling errors; lack of documents provided by a person; insufficient language skills by the officer; 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 skills and training; or situations where the common format for data transmissions is not followed. 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-2018 Report, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights'. European Union Agency for Fundamental Rights. March 2018, p. 31. Cf.: Mirja Gutheil *et al.,* 'Interoperability of Justice and Home Affairs Information Systems', Study for the LIBE committee, PE 604.947- April 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf.

55 Alphanumerical data can be unreliable for establishing the identity of a person, due to many so-called aliases, cases of identity fraud, entry and spelling mistakes and might lead to matches connected to the wrong person. FRA Report, p. 20.

56 Teresa Quintel, 'Connecting Personal Data of Third Country Nationals', (March 1, 2018), pp. 13-14.

57 EDPS Opinion 4/2018 opinion on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 16 April 2018, p. 13 (point 42).

58 SWD (2017) 473 final and SWD (2017) 474 final.

stricted' and 'precisely defined' in order to justify access to the CIR for the sole purposes of identification.[59]

In addition, it has been demonstrated that most of the operational systems contain significant amounts of erroneous data,[60] which might complicate the detection of multiple identities,[61] and lead to large numbers of wrong matches that could potentially hamper the work of competent authorities instead of facilitating the correction of erroneous data.

For instance, the EU Agency for Fundamental Rights (FRA) in its Report on biometrics and EU IT-systems from March 2018 acknowledges that the EU databases hold inaccurate alphanumeric data such as names, nationality, age or date of birth.[62] In addition, biometric data would partially be of low quality due to injuries, intentional destruction, poor fingerprinting devices or so-called spoofing.[63] According to FRA research, inaccurate data in the VIS and the SIS II databases led to considerable amounts of wrong matches where these systems were queried by the competent authorities.[64]

In an interoperable system, the storage of erroneous data in the underlying databases would not only go against the principle of data accuracy,[65] it would presumably multiply wrong matches where data would be cross-checked against additional systems and would maximise the hits that would be shown to the querying user. Consequently, a higher probability for wrong matches would increase the likelihood of an individual being erroneously linked to a false profile and exacerbate the risk of privacy infringements where a person would, for instance, have to undergo subsequent security checks due to a wrong match. Hence, the assertion under Recital 22 of the proposed interoperability Regulations that the central storage of personal data in the CIR and the automated matching of such data would lead to an increased accuracy of identification might not be entirely valid. Even if wrong data would be easier recognizable, it might not improve the work of competent authorities where these would be confronted with thousands of wrong matched when inserting new data in the systems.

However, most striking about the interoperability proposals is that, with the CIR, the BMS and the MID, the anticipated Regulations would establish three new databases that would retain personal data on a central level. While the MID would solely

59 Fra-2018 Report 'Under watchful eyes: biometrics, EU IT systems and fundamental rights', March 2018, p. 96. FRA mainly refers to data stored in the VIS and the SIS databases, but also refers to Eurodac.

60 EDPS Opinion 4/2018 opinion on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 16 April 2018. Point 36.

61 Fra-2018 Report, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights', March 2018, p. 15.

62 Which refers to the falsification of an identity by manipulating the fingerprint using silicone, see FRA-2018 Report on biometrics, p. 50.

63 Falsifying of fingerprint data for instance by destroying the fingertip, see: Fra-2018 Report, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights', March 2018. P. 82.

64 EDPS Opinion 07/2016 on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations), p. 8.

65 Article 5(1)(d) of Regulation 2016/679 (see below).

store links and references to those information systems that created those links, the CIR and the BMS would actually retain both biographical and biometric data. The creation of two new databases that would store biometric data on a central level and that would grant streamlined law enforcement and Europol access to data initially collected for non-law enforcement purposes, poses serious threats to the protection of personal data and data subject rights.

The risks related to the inclusion of additional biometric datasets and the interference arising with streamlined law enforcement access to data under the proposed Regulations will be further discussed in sub-section II.3. and section III.

II.3. Processing of Biometric Data under the Interoperability Proposals

Pursuant to Article 9 of Regulation (EU) 2016/679[66] and Article 10 of Directive (EU) 2016/680,[67] biometric data are special categories of data, which are, by nature, particularly sensitive and merit higher protection.[68] Thus, biometric data should not be processed, unless processing is allowed in specific cases, for instance, for the compliance with a legal obligation or for the performance of a task carried out in the public interest.[69] Moreover, processing of special categories of data should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons, thus, requiring additional safeguards.[70]

Biometric data uniquely identify a person and, unlike other personal data, are neither given by a third party nor chosen by the individual. As they are inherent to the data subject's body, they permanently refer to that person[71] and can in general neither be deleted or altered.[72] Thus, the processing of biometric data presents a more serious interference with data subject rights than the processing of 'normal' data and must be subject to a higher level of data protection standards.[73]

66 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. (Hereafter 'GDPR').

67 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.

68 Recital (53) of the GDPR.

69 Recital (51) of the GDPR.

70 Recital (54) of the GDPR.

71 EDPS Opinion 4/2018 opinion on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 16 April 2018, p. 11 (point 31).

72 Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, adopted on 27th April 2012.

73 EDPS Opinion 06/2016 on the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System, p. 8.

Because of their peculiar nature, the collection and storage of biometric data requires a thorough analysis and strong security measures. Such analysis is all the more necessary where biometric data are stored in large amounts and in central databases.[74] Thus, any system storing biometric data should be accompanied by sufficient guarantees and safeguards in order to ensure that the data are protected against risks of unauthorized access, misuse, deletion, alteration or misappropriation.[75] Moreover, compliance with the purpose limitation principle, the data minimization principle as well as with the accuracy and storage limitation principles is a prerequisite for the processing of biometric data.[76] Thus, data must be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes, it must be limited to what is necessary, must be accurate, kept up to data and be stored for no longer than required for the purposes for which the data are processed.[77]

With an exception of the ETIAS, all of the current databases, anticipated EU IT-systems and legislative revisions to be included in the interoperability framework store biometric data.[78] At the moment, Eurodac and the VIS store fingerprints, both proposals for legislative revisions additionally foresee to retain facial images, once this is technically possible with accurate results.[79]

The EES and the ECRIS-TCN will store both fingerprints and facial images once operational. The SIS Regulation in the field of border checks[80] and SIS Regulation for the return of illegally staying TCNs[81] include fingerprint data, facial images and even palm prints. The SIS Regulation on police cooperation and judicial cooperation in criminal matters[82] would additionally store DNA data of missing or wanted persons.[83]

Thus, the individual files stored in the CIR, which would compile data from the underlying systems would include biometric data such as fingerprints and facial images (the SIS II would, due to its complexity not be included in the CIR).[84] For the purpose of identity checks, biometric data could be matched against alphanumerical data and

74 EDPS Opinion 07/2016 on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations), p. 8.

75 EDPS Opinion 06/2016 EDPS on the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System, p. 12.

76 Article 29 Data Protection Working Party Opinion 3/2012 on developments in biometric technologies, Adopted on 27th April 2012, p. 7.

77 Article 5 of the GDPR and Article 4 of Directive (EU) 2016/680, principles relating to processing of personal data.

78 Article 5(b) and (c) of the VIS proposal, Article 42(4) of the Eurodac proposal, Article 42(4)of the SIS II police proposal, Article28(4) of the SIS II borders proposal; Article 13 of the SIS II return proposal, Article 36(b) of the EES Regulation, Article 6(2) of the ECRIS-TCN proposal.

79 Fra-2018 Report, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights', March 2018, p. 25.

80 COM(2016) 882 final (SIS II borders proposal).

81 COM(2016) 881 final (SIS II return proposal).

82 COM(2016) 883 final.

83 Fra-2018 Report, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights', March 2018, p. 23.

84 COM(2017) 793 and 794 final, p. 7.

be connected to a person stored in the CIR. The quality of the biometric identifiers is, therefore, of paramount importance in order to avoid wrong matches.[85]

According to Article 12 of the interoperability proposals, the purpose of the BMS is to support the CIR and the MID and to fulfil the objectives of the underlying databases.

With the BMS, the proposed Regulations on interoperability would retain 'all biometric templates in one single location to facilitate cross-system comparisons using biometric data in order to detect multiple identities'.[86] Both the EDPS and the WP29 held that the biometric templates stored in the BMS are, contrary to the Commission's assertion that the templates would not constitute sensitive data,[87] indeed special categories of data.[88] By providing a common platform for the storage of biometric templates,[89] the BMS would therefore establish a central biometric database, which would enable the CIR and the SIS II to automatically query and compare the biometric data (fingerprints, facial images and, with the connection to the future SIS II Regulations, palm prints and DNA data) from several central systems simultaneously.[90]

II.4. Interim 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(2) 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 permitted to consult the underlying systems.[91] Disregarding the purposes limitation principle might eventually lead to information gaps, as national LEAs may be reluctant to provide data where they cannot be certain who will be granted access or for which purposes the information will be processed in other Member States.

The necessity and proportionality requirements under Article 52(1) of the EU Charter, stipulating that 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, have not sufficiently been taken into account in the Commission's impact assessment, which neither demonstrates the necessity of establishing new conso-

85 Ibid, p. 15.
86 EDPS Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 16 April 2018, p. 19 (point 77).
87 COM(2017) 793 and 794 final, P. 7.
88 WP29 opinion on Commission proposals on establishing a framework for interoperability between EU information systems, p. 6 and 7 and EDPS opinion on the Proposals for two Regulations establishing a framework for interoperability, p. 19 (point 77).
89 WP29 opinion on Commission proposals on establishing a framework for interoperability between EU information systems, p. 6.
90 COM(2017) 793 and 794 final, Brussels, 12.12.2017, p.6.
91 EDPS Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017, p. 12.

lidated databases, nor adequately considers the possibility of alternative solutions that could achieve the same objectives by less intrusive means.[92]

In addition, abandoning the current silo structure of EU databases and circumventing the cascading safeguards would pose major data protection concerns: 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 (biometric) data would be stored on a centralized basis.[93]

The establishment of new, interconnected large-scale databases that would store biometric data centrally requires a sufficiently justified explanation regarding the necessity and proportionality of such a framework, and additional safeguards due to the sensitivity of biometric data. Any central storage of biometric data heightens the risks for data subjects in case of unlawful access and use and therefore requires an increased level of security.[94]

The collection, cross-matching and querying of personal data would pose additional interferences to privacy and data protection rights, in particular, where data within the interoperability components would be processed for different purposes than the ones of the underlying databases.[95] Furthermore, the purposes of combating irregular migration and contributing to a high level of security are very broad and not 'strictly restricted' and 'precisely defined', as required by the CJEU.[96]

III. Europol

The European Police Office, Europol, is an international police organisation that was established to promote and strengthen cooperation among the LEAs of the EU Member States.[97] Since its establishment with the adoption of the Europol Convention[98] in 1995, Europol has been subject to several developments and undergone dynamic legislative changes.[99]

In 1999, Europol became fully operational and since then experienced massive modifications in terms of its status, mandate and competences.[100]

92 Ibid, p. 5.
93 Teresa Quintel, 'Connecting Personal Data of Third Country Nationals', p. 17.
94 WP29 opinion on Commission proposals on establishing a framework for interoperability between EU information systems, p. 19.
95 Ibid, p. 21.
96 EDPS opinion on the Proposals for two Regulations establishing a framework for interoperability, p. 13 (point 42).
97 Emma Disley et al.: 'Rand Report – Evaluation of the implementation of the Europol Council Decision and of Europol's activities' (2012), p. XV.
98 Convention on the Establishment of a European Police Office, based on Article K3 of the Treaty on European Union (TEU Maastricht) ('Europol Convention'), [1995] OJ C316/2.
99 Agathe Piquet, 'Supranational Activism as an Assertion Process? The Case of Europol', Journal of Contemporary European Research, [S.l.], v. 13, n. 2, May 2017. ISSN 1815-347X. Available at: http://jcer.net/index.php/jcer/article/view/773.
100 Europol's predecessor, the European Drugs Unit (EDU) had already become operational in the early 1990 s. For further information see: F R Monaco, 'Europol: The Culmination

With the entry into force of the Lisbon Treaty in 2009, the EU's activities in criminal matters, which had been established in 1993 on a purely intergovernmental basis as part of the Third Pillar,[101] were attributed more importance with the abolishment of the pillar structure.

Great sections of EU criminal law became subject to the community method and Europol's mandate was re-defined in EU primary law under Article 88 of the Lisbon Treaty.[102] Under the latter, Europol was transformed into a full EU Agency[103] and, henceforth, had to comply with general rules and procedures applicable to EU agencies.[104] These procedures included certain judicial overview by the CJEU, budgeting and auditing rules and changes to the review of Europol's legal basis.[105]

Under the Europol Council Decision 2009/371/JHA,[106] Europol's declared objective was now to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States.[107] Thus, from 1 January 2010, Europol's mandate included terrorism, and organised transnational crimes such as drug trafficking, terrorism, illegal immigration, human trafficking, cybercrime, financial crime and counterfeiting.[108]

Only two years later, negotiations on a Europol Regulation were initiated to extend the agency's competence towards newly emerging types of criminal activity, particularly in cyberspace.[109]

While Europol was originally intended to act as an enormous hub for the exchange of information, the agency progressively developed into a data-driven 'intelligence analyst', competent to exchange information with the LEAs of the Member States and other EU agencies,[110] as well as with certain third countries and international orga-

---

of the European Union's International Police Cooperation Efforts' (1995) 19 Fordham International Law Journal 247, 282.

101 Police and Judicial Cooperation in Criminal Matters (PJCCM).

102 Europol and Eurojust are the only AFSJ agencies whose mandates are defined under EU primary law, Chloé Brière, 'Cooperation of Europol and Eurojust with external partners in the fight against crime: what are the challenges ahead?', Brexit Institute, Working Paper No. 1 (2018), p. 1.

103 "Europol's New Regulation," Europol, accessed May 7, 2018, https://www.europol.europa.eu/newsroom/news/europols-new-regulation.

104 See, for instance, M. Tebaldi and M. Calaresu, 'Level of Europeanization and Policy outcomes: The Common Security Policy and the Case of Europol' (June 2013) SAGE Open, p. 7.

105 Sabine Gless, ‚Europol' in: Valsamis Mitsilegas et al. (eds.) Reseach Handbook on EU Criminal Law, (Edward Elgar, 2016), p. 464.

106 Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), [2009] OJ L121/37.

107 Article 3 of Council Decision 2009/371/JHA.

108 102 Emma Disley et al.: 'Rand Report – Evaluation of the implementation of the Europol Council Decision and of Europol's activities' (2012), p. XV.

109 Sabine Gless and Thomas Wahl, 'A Comparison of the Evolution and Pace of Police and Judicial Cooperation in Criminal Matters: A Race Between Europol and Eurojust?' In: The Needed Balances in EU Criminal Law. Oxford (2014), pp. 339-354.

110 Such as Eurojust, Frontex or the European Anti-Fraud Office, OLAF.

nizations such as Interpol.[111] As 'mega search engine'[112] Europol supports operational activities of national LEAs, provides real-time analysis of information, coordinates law enforcement action and assists with forensic tools.[113]

However, even under the new Regulation, Europol was not granted executive powers and continues to operate through its relationships with the Member States. Thus, Europol's mandate solely permits the agency to act as 'service provider' and to assist national LEAs upon request without powers to carry out investigative measures or operational commands. Put differently, Europol relies on national LEAs, third countries or international organizations to receive information and is generally not the owner of the data stored in its own databases.[114]

Yet, the new Regulation not only attributed Europol a more powerful role in terms of agency, it also introduced a time-limit for Member States' authorities to justify the non-compliance with Europol requests for information and thereby strengthened Europol's capacity to launch criminal investigations via the national authorities.[115] Moreover, the new Regulation endorsed Europol's capacity to analyse data more flexibly by shifting data protection rules that were attached to specific databases to certain processing operations carried out by Europol.

The following section will address some of the changes that have been introduced by the new Europol Regulation with regard to data processing operations and point to the concerns that these changes might generate in terms of data protection standards (sections III.1. and III.2.). Thereafter, section III.3. will deal with the non-existent rules on additional safeguards that apply to Europol when processing biometric data, particularly focussing on biometric data of TCNs. Sections IV and IV.1. will illustrate the current procedures for granting Europol access to EU databases and point to the risks of facilitating and streamlining such access under the proposed interoperability regulations.

III.1. The new Europol Regulation

The process on the revision of Europol's legal basis started in 2012 with the goal to transform the Europol Decision into a Regulation. The objective of the reform was to increase the EU's internal security by making Europol a stronger hub for information exchange between the LEAs in the Member States.

111 Sabine Gless, 'Europol' in : Valsamis Mitsilegas et al. (eds.) Reseach Handbook on EU Criminal Law, (Edward Elgar, 2016), p.465.

112 A. Weyemberg et al., 'The inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area', Study realized for the LIBE Committee of the European Parliament, November 2014, pp. 11-14.

113 Europol, 2013 Europol Review, p. 14.

114 Chloé Brière, 'Cooperation of Europol and Eurojust with external partners in the fight against crime: what are the challenges ahead?', Brexit Institute, Working Paper No. 1 (2018), pp. 11-12.

115 Sabine Gless and Thomas Wahl, 'A Comparison of the Evolution and Pace of Police and Judicial Cooperation in Criminal Matters: A Race Between Europol and Eurojust?' In: The Needed Balances in EU Criminal Law. Oxford (2014), p. 244.

As a response to new trends of crime and to facilitate information sharing, the volume and quality of information transmitted to Europol by the Member States should increase and discrepancies regarding the level of information provided by Member States be reduced. In addition, Europol staff should obtain the capacities to fully assist Member States in order to decrease delays in the handling of operational analysis on the one hand and to avoid duplication of data on the other.[116] The new legal instrument further de-pillarized Europol's functioning and granted more tools to the agency in order to increase its support for cross-border cooperation in criminal matters, for instance in counter-terrorism and combatting the smuggling of migrants.[117]

In the age of Big Data analytics, the Regulation sought to create stronger incentives for Member States to transfer additional data to Europol by strengthening the obligation to provide such information to the agency.[118] The Regulation should adapt Europol's modus operandi to new forms of serious organised crime in the digital age. Thus, Europol was granted further capacities to effectively gather, cross-match, analyse, store and link information.

On 1 May 2017, the new Europol Regulation, which had been adopted on 11 May 2016, entered into force and took effect in all 28 Member States.[119] The Regulation was part of the EU Data Protection Reform in the field of Justice and Police and introduced a number of changes to the structure of the agency, also with regard to its data protection rules. The provisions on data protection under the Europol Regulation followed the rules of the GDPR and Directive (EU) 2016/680.[120] However, despite the alignment with those two legal instruments, Europol nevertheless was granted a *sui generis* data protection framework, tailored to the specific data processing needs of the agency.[121]

Under the new Regulation, Europol operates as forum that connects and analyses information and personal data that it receives from the Member States and via additional channels, by applying the power of data analytics.[122] Europol as information hub currently provides for a technology-enabled and data-driven platform that connects over 500 LEAs within the EU Member States and beyond.[123]

116 SWD(2013) 99 final [part 1], Brussels, 27.3.2013, p. 4.

117 See for instance, Council Conclusions on EU External Action on Counter-terrorism, 19 June 2017. Cf.: Chloé Brière, 'Cooperation of Europol and Eurojust with external partners in the fight against crime: what are the challenges ahead?', Brexit Institute, Working Paper No. 1 (2018), p. 2.

118 Ibid, p. 8.

119 "Europol's New Regulation," Europol, accessed May 7, 2018, https://www.europol.europa.eu/newsroom/news/europols-new-regulation.

120 Chloé Brière, 'Cooperation of Europol and Eurojust with external partners in the fight against crime: what are the challenges ahead?', Brexit Institute, Working Paper No. 1 (2018), p. 9.

121 Ibid.

122 Rob Wainwright, 'The 'Uberisation' of international police work', published on January 23, 2016.

123 Daniel Drewer, Vesela Miladinova: 'The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation', computer law & security review 33 (2017) 298–308, p. 300.

Europol's strengthened mandate was supposed to modernize the agency's capacity to exchange information, increase the flexibility of integrated data management systems and to utilise new technological advancements in criminal investigations.[124] Put differently, the processing architecture under the Regulation was re-designed as to enable the agency to use large quantities of information to provide, by means of Big Data analytics, both strategic and preventive insights.[125] Thus, with the Regulation, Europol was basically transformed from a police-oriented agency into an intelligence producing information hub.

As EU Agency, Europol must comply with the Union's principles that are enshrined in the Charter and the Treaties, inter alia, with the provisions regarding the right to data protection under Article 16 of the TFEU.[126] Europol's activities in carrying out its tasks may directly interfere with individuals' fundamental rights to privacy and data protection, as the agency may, particularly under the new Regulation, collect, store, cross-check, analyse and exchange personal data in so far as is necessary for the achievement of the objectives under Article 3 of the Europol Regulation.[127]

In contrast to other EU institutions and bodies, which apply Regulation [(EU)2018/1725][128] for the processing of personal data, Europol processes personal data within the framework of the stand-alone data protection regime under its own Regulation. The latter particularly takes Europol's specific needs as law enforcement authority into account, by aligning the data protection rules with those under Directive (EU) 2016/680 that applies to national LEAs. Thus, while the Regulation changed the way in which Europol may process personal data, it also introduced additional rules on data protection. The Regulation adopted the provisions on general principles related to the processing of personal data, those on retention periods and the standards on data subject rights in a similar manner as under Directive (EU) 2016/680.[129]

With its widened mandate, Europol's data processing framework was redefined and now particularly emphasises the 'data protection by design' approach under Article 33 of the Europol Regulation. The proper implementation of this principle shall be ensured by Europol's Data Protection Officer, the EDPS and the national supervisory authorities.[130]

124 Ibid.
125 Ibid, p. 307.
126 Chloé Brière, 'Cooperation of Europol and Eurojust with external partners in the fight against crime: what are the challenges ahead?', Brexit Institute, Working Paper No. 1 (2018), pp. 17-18.
127 Article 18 of the Europol Regulation.
128 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/ECText with EEA relevance. OJ, L 295/39, p.39-98.
129 Chloé Brière, 'Cooperation of Europol and Eurojust with external partners in the fight against crime: what are the challenges ahead?', Brexit Institute, Working Paper No. 1 (2018), p. 19.
130 Fanny Coudert, 'The Europol Regulation and purpose limitation: from the "silo-based approach" to…what exactly? (Part II), 20 April 2017.

III.2. Processing of Personal Data under the Europol Regulation

In a world of Big Data in which intelligence and data mining have become vital tools for the prevention, detection, investigation and prosecution of crime, the Europol Regulation introduced a technology neutral approach towards data processing. The Regulation shifts the purpose limitation away from databases and attaches specific purposes to separate data processing activities by the agency.[131] This enables Europol to process information more flexibly, allowing to cross-check, link and classify personal data.[132] Under the Europol Regulation, the purposes for processing are defined broadly and permit Europol to use Big Data analytics.[133]

Pursuant to Article 18 2(a), Europol may engage in data mining, by 'cross-checking aimed at identifying connections or other relevant links between information' regarding persons who are suspected of having committed, or who were convicted for a crime. Moreover, the agency may process personal data for the purposes of strategic[134] and operational analyses.[135]

Under Article 19(1), Europol shall process information received by the Member States in order to determine the purpose(s) for which the data is further processed, where the provider of the information did not determine a purpose. Thus, Europol may, by means of data mining assess whether data received might be relevant for the performance of its tasks.

Data mining and cross-checking of data based on a suspicion against a person inevitably includes the processing of personal data without a clearly pre-defined purpose and does not require the determination of a hypothesis before querying a database.[136] Moreover, Europol may, pursuant to Article 18(6) temporarily process data for the purpose of determining whether such data are relevant to its tasks. In theory, Europol could carry out intelligence-led data mining in order to discover unexpected correlations, as crime prediction method, or to reconstruct past events.[137]

Moreover, in the law enforcement area, personal data may be processed for subsequent purposes where processing is not incompatible with the initial purposes for pro-

131 Daniel Drewer, Vesela Miladinova, 'The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation', computer law & security review 33 (2017), p. 301.

132 Tomasz Safjánski and Adrian James, 'Europol's Crime Analysis System – Practical Determinants of Its Success, in: Policing (Oxford University Press, 2018), pp. 1-10.

133 Fanny Coudert, 'The Europol Regulation and purpose limitation: from the "silo-based approach" to…what exactly? (Part II), 20 April 2017. Available at: https://www.law.kuleuven.be/citip/blog/the-europol-regulation-and-purpose-limitation-from-the-silo-based-approach-to-what-exactly-part-ii/.

134 Article 18(2)(b) of the Europol Regulation.

135 Article 18(2)(c) of the Europol Regulation.

136 Fanny Coudert, 'The Europol Regulation and purpose limitation: from the "silo-based approach" to…what exactly? (Part II), 20 April 2017.

137 Broeders et al. (2017) 'Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data', Computer Law & Security Review, Vol. 33 (3): 309-323.

cessing.[138] Processing is thereby based on the presumption of compatibility in the law enforcement context, consequently relying on secondary uses of data, which is further encouraged by the use of data-driven technologies.

In addition, the Europol Regulation does not contain provisions on automated decision-making and profiling that offer similar data protection standards as the ones under the GDPR or Directive (EU) 2016/680.[139]

III.3. Processing of TCN's Biometric Data by Europol

One of the shortcomings under the Europol Regulation is the insufficient protection of biometric data, which are not defined as special categories of data under Article 30. That provision was not aligned with the data protection standards concerning special categories of data under the GDPR and Directive (EU) 2016/680. The only limitation on the processing of biometric data may be found in Annex II of the Europol Regulation, which stipulates that personal data that may be subject to processing for the purpose of cross-checking shall only include personal data that are 'not subject to change such as dactyloscopic data', *where necessary*. Thus, the processing of fingerprint data should, theoretically, comply with a necessity requirement.

Because biometric data are not defined as special categories of data under the Europol Regulation, prior consultation carried out by the EDPS in accordance with Article 39(1)(a) is not required where fingerprints, DNA data or other biometric identifiers are being processed by Europol. In addition, Article 39(1)(b) solely requires prior consultation for particular types of processing that present specific risks for data subject rights without taking into account the types of data. Thus, where Member States authorities do not attach specific restrictions to the use of biometric data, Europol may theoretically treat these data in the same way as any other type of personal data.

In the context of migration, Europol progressively appeared as one of the main JHA actors in the field of border management and asylum. Due to the expansion of the types of crime that fall within Europol's mandate, migrant smuggling, as one of the top priorities of the *European Agenda on Migration*,[140] was, together with counterterrorism, included within the agency's responsibilities.[141]

In accordance with the hotspot approach,[142] Europol was granted operational tasks at border sites in Greece and other countries, where the agency assisted intelligence

138 Article 4(2) of Directive (EU) 2016/680 introduces the notion of subsequent processing (processing by the same or another controller for purposes other than the ones for which the data was collected, if falling within the scope of Article 1(1)) and thus, does not refer to further processing, which, under the GDPR may not take place if processing is incompatible with the initial purposes.

139 Fanny Coudert, 'The Europol Regulation and purpose limitation: from the "silo-based approach" to…what exactly? (Part II), 20 April 2017.

140 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A European Agenda on migration', COM(2015) 240 final, Brussels, 13.5.2015.

141 Satoko Horii, 'Accountability, Dependency, and EU Agencies: The Hotspot Approach in the Refugee Crisis', Refugee Survey Quarterly, 2018, 0, 1-27, p. 15.

142 Cf.: https://ec.europa.eu/home-affairs/content/hotspot-approach_en.

investigations during so-called secondary security checks in order to identify movements of suspected terrorists[143] and to detect organized crime networks of migrant smugglers.[144] During these security checks, Europol's mission was to assist national LEAs with the cross-checking of personal data of TCNs against the Europol databases. During the secondary security inspection in Greece, around 1.490 TCNs were checked against the Europol Information System (EIS) by Europol officers.[145]

During recent years, the operations[146] in which Europol may collect (biometric) data from TCNs for the purpose of cross-checking the information against the EIS were further extended, involving several third countries and, thus, going beyond the checks in the hotspots on the territory of the EU.[147]

In the context of data protection and processing of personal data by Europol staff, one must differentiate between Europol officers who carry out processing within the framework of joint investigation teams or other arrangements where processing falls within the scope of national legislation, and processing of personal data by Europol staff falling within the scope of the Europol Regulation. Thus, where Europol officers participate in joint investigation teams under Article 5 of the Europol Regulation, they should apply the national laws transposing Directive (EU) 2016/680 whenever they process personal data for the purposes of the prevention, detection, investigation or prosecution of criminal offences, whereas general Europol staff would have to comply with the rules under the Europol Regulation.

Consequently, a Europol officer who must apply Directive (EU) 2016/680, is obliged to process biometric data in accordance with Article 10 of the Directive and thus, only where strictly necessary and providing additional safeguards. Moreover, profiling that would result in discrimination on the basis of special categories of data would be prohibited under Article 11 of Directive (EU) 2016/680.

Where the processing and cross-checking carried out by Europol staff would fall within the scope of the Europol Regulation, the respective officer(s) would not have to comply with the specific rules applicable to biometric data under Directive (EU) 2016/680, as those data would not be treated as special categories of data. Thus, a Europol officer processing biometric data within the scope of the Europol Regulation would have more flexibility in terms of processing activities.

143 Europol press release, 'Europol setting up team of 200 investigators to deploy to Migration Hotspots', https://www.europol.europa.eu/newsroom/news/europol-setting-team-of-200-investigators-to-deploy-to-migration-hotspots.

144 Satoko Horii, 'Accountability, Dependency, and EU Agencies: The Hotspot Approach in the Refugee Crisis', Refugee Survey Quarterly, 2018, 0, 1-27, p. 18.

145 Council of the EU, Implementation of the Counter-Terrorism Agenda Set by the European Council, 13627/16 Brussels, 4 November 2016, p.4.

146 In February 2016, Europol established the European Migrant Smuggling Centre (EMSC) to support Member States in cross-border anti-smuggling operations. Within the framework of the EMSC, Europol's activities in the Joint Operational Team Mare (JOT-MARE), which had been launched in 2015, were expanded to include the gathering of intelligence information to combat migrant smuggling by boat across the Mediterranean Sea and to provide access to its databases to national LEAs and intelligence agencies.

147 Satoko Horii, 'Accountability, Dependency, and EU Agencies: The Hotspot Approach in the Refugee Crisis', Refugee Survey Quarterly, 2018, 0, 1-27, p. 6.

In the context of databases, Europol may, pursuant to Article 17(3) of the Europol Regulation and insofar as it is entitled to do so under Union, international or national law, gain access to data from Union, international or national information systems in order to retrieve and process personal data if necessary for the performance of its tasks. Accordingly, once data would be retrieved from these information systems by Europol, the agency could process such data in accordance with Article 18(2) for cross-checking and linking purposes (after having obtained the consent of the Member State owning the data). The results of such processing by Europol could then be queried by the national LEAs via their access to the EIS.[148] Europol could thus, analyse biometric data in bulk and national LEAs, circumventing the constraints regarding the processing of biometric data under Directive (EU) 2016/680, could use the final product provided by Europol.

As mentioned above, all operational databases and those that are to be established in the future (with the exception of the ETIAS) hold biometric data. Where the latter would be processed by national competent authorities for border control, visa, or immigration purposes, processing would fall within the scope of the GDPR and would thus, have to comply with the strict rules applicable to the processing of biometric data. Similarly, processing carried out by national LEAs for the purposes of the prevention, detection, investigation or prosecution of crime within the scope of Directive (EU) 2016/680, would require the application of the rules under the Directive whenever biometric data would be processed. Only where Europol staff would retrieve and subsequently process biometric data for the purpose of the performance of the agency's tasks, additional safeguards would not have to be provided, which puts at risk special categories of personal data, particularly where these would be retained centrally in the EIS.

III.4. Interim Conclusion

On the one hand, the Europol Regulation adapts to the challenges of a changing crime environment, inter alia related to migration, thereby enabling the agency to engage in Big Data analytics of large quantities of data. On the other hand, the Regulation provides Europol with a remarkably broad scope and flexibility to process personal data, which bears risks to data protection standards.

In the area of migrants smuggling and related organized crime, Europol may assist Member States by providing both strategical and operational insights of cross-border security threats. Thereby it is important that Europol complies with data protection standards, following a purpose-based processing approach. Yet, the broad scope of Article 18 and the somewhat wider interpretation of the purpose limitation principle in the law enforcement context reflect the extensive possibilities for Europol to process personal data. Moreover, the Regulation does not define biometric data as special categories of personal data, thus, not requiring a Data Protection Impact Assessment (DPIA) or a prior consultation with the EDPS whenever Europol processes such data.

148 Heiner Busch and Matthias Monroy, 'Counter-terrorism and the inflation of EU databases', Analysis for Statewatch, May 2017, http://statewatch.org/analyses/no-316-ct-and-inflation-eu-databases.pdf.

Therefore, it is all the more important that prior consultation will be carried out where biometric data will be processed in bulk, foreseen under Article 39(2)(b) of the Europol Regulation for types of processing that present specific risks to data subject rights.

Law enforcement and Europol access to EU databases as well as the changes that would be introduced with regard to such access under the proposed interoperability will be addressed in to following two sections (sections IV. and IV.1.).

IV. Europol access to EU databases

All large-scale EU IT-systems feature provisions granting Europol access to retained data for the purpose of fighting serious crime and terrorism. Requirements for access to the databases by Europol are, inter alia, that reasonable grounds exist to consider that the consultation of data in the systems may substantially contribute to the prevention, detection or investigation of criminal offences, or if the consultation is necessary to support and strengthen action by Member States within the mandate of Europol.

Processing of data retrieved from the databases is subject to prior consent by the Member State owning the data and Europol may only make single enquiries for specific data. Yet, the recently adopted SIS II Regulations grant Europol access to further datasets in order to retrieve and process those data within the scope of the Europol Regulation and under Article 22 p(3) of the proposed VIS Regulation, Europol's designated authority may submit a "reasoned electronic request" for the consultation of all data or a specific set of data stored in the VIS.[149]

As mentioned above, all underlying systems that will be included in the interoperable framework increasingly rely on biometric data, currently fingerprints and facial images, and will, in the future, also include palm prints and DNA data for the purpose of better identifying a person.

Moreover, all systems (except for SIS II and ECRIS-TCN) contain data on persons not suspected of having committed any crimes, but nevertheless grant law enforcement access for the purposes of the prevention, detection, or investigation of serious crime. Thus, LEAs are allowed to access data stored in Eurodac, the VIS, the EES and the ETIAS for these purposes, provided that they adhere to the safeguards specified in the corresponding legal instruments.[150]

IV.1. Access to personal data by Europol under the Interoperability Proposals

One of the objectives of the interoperability proposals is to facilitate and streamline access by LEAs and Europol to EU IT-systems that are not exclusively established for

149 Heiner Busch and Matthias Monroy, 'Counter-terrorism and the inflation of EU databases', Analysis for Statewatch, May 2017, http://statewatch.org/analyses/no-316-ct-and-inflation-eu-databases.pdf.

150 Fra-2018 Report, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights', March 2018, p. 9.

the purposes of the prevention, investigation, detection or prosecution of serious crime.[151]

Under the interoperability proposals Europol as processor would be granted access to all underlying databases as well as to the CIR, the MID and the ESP for processing personal data within its mandate. As mentioned above, under Article 17(3) of the Europol Regulation, the agency may retrieve personal data from the EU information systems in order to cross-match these data against its own database (generally with the requirement to obtaining prior consent by the relevant Member State).

Consequently, data acquired during the query in the ESP could subsequently be used for data mining by Europol staff, even where the data was retrieved from a non-law enforcement database.

The purpose limitation principle has particular relevance in the context of law enforcement access to the individual IT-systems, as their primary purposes, except for the SIS II, are of non-law enforcement 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 Europol staff with information that they otherwise may not have the right to access within their competences. Though such information is not personal data *per se*, 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.[152]

V. Conclusion

In a world of Big Data, where more and more information is available and used to generate un-precedented insights of human behaviour, LEAs and Europol progressively seek to exploit personal data not only for security purposes, but, in the context of border management, also for counter-terrorism and for cross-border anti-migrant (smuggling) operations.

To achieve the most accurate results, large datasets are needed to find (reliable) correlations and to increase the probability of a prognosis. Accordingly, any data-driven analysis by its very nature raises concerns regarding its compliance with core EU data protection principles.

With interoperability, information exchanges between authorities on both national and EU level would be facilitated and data concerning terrorists and serious crime be easier accessible, as all information relating to a specific person would be accumulated in one search.[153] However, streamlined access conditions for national LEAs and Europol would also grant access to additional types of data.

151 Recital (24) of the interoperability proposal, COM(2017) 794 final. Cf.: Teresa Quintel, ‘interoperability of EU databases’, p. 16.

152 Teresa Quintel, ‘interoperability of EU databases’, p. 16.

153 See: Final report of the High-level expert group on information systems and interoperability, May 2017. Ref. Ares(2017)2412067; 11/05/2017.

Under the Europol Regulation, the agency is able to process large datasets in order to provide better insights into specific crime dynamics and to engage in the use of bulk data analysis, to allow for more flexibility and to create a better understanding of crime patterns. This not only bears risks with regard to the purpose limitation principle, it also allows Europol to process biometric data in bulk, as the Regulation does not treat these data as special categories of data.

While it is true that the fight against crime and threats to public security are objectives of general interest of the EU and capable to justify even serious interferences with fundamental rights,[154] 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,[155] is indispensable for interoperable databases to be compliant with both EU data protection standards and the requirements of the CJEU.[156] This should also include strict necessity and the provision of additional safeguards whenever special categories of personal data are being processed, as those data are of particularly sensitive nature.

In the future, more actors will be involved in the processing of personal data of TCNs. Currently, a pilot project, the so-called crime information cell, hosted by the EEAS service[157] within EUNAVFOR MED Operation Sophia[158] as a mechanism under which current cooperation and information sharing between CSDP[159] missions and JHA agencies shall be further enhanced[160] to facilitate the information exchange for both analytical and operational use by Europol and the European Border and Coast Guard Agency (EBCGA), is on its way.[161] Not only would this lead to a blurring of lines between processing of data by law enforcement and the military, the EBCGA, Europol and the national LEAs would each apply their respective data protection frameworks.[162] In addition, personal data gathered by military staff would be directly transferred to the EU agencies as well as the national LEAs, although the CSDP missions generally do not have a mandate to process personal data in cooperation

154 See for instance *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.

155 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.

156 Teresa Quintel, connecting personal data of Third Country nationals', p. 18.

157 http://statewatch.org/news/2017/nov/eu-civ-mil-intel-coop.htm and euobserver, 'Pilot project blurs military and police lines on migration', Brussels, 9 March 2018, https://euobserver.com/migration/141258.

158 https://www.operationsophia.eu/.

159 Common Security and Defence Policy.

160 151 14265/17, LIMITE, 20 November 2017, p. 3.

161 euobserver, 'Pilot project blurs military and police lines on migration', Brussels, 9 March 2018, https://euobserver.com/migration/141258.

162 The EBCGA would apply the 'new' Regulation (EC)45/2001, Europol would process personal data within the scope of the Europol Regulation and national LEAs would apply either the GDPR or Directive (EU)2016/680.

with JHA agencies.[163] This creates problems regarding potential gaps between data protection standards, as three[164] different entities would process the same data but under separate data protection regimes.

To that end, the support of the EBCGA, aka Frontex, in contributing 'to preventing and detecting serious crime with a cross-border dimension' shall be reinforced and coordination of the EBCGA's activities with Europol (and Eurojust) shall be improved[165] through the exchange of information[166] and the involvement of both EU agencies in migration management support teams.[167] In line with the new role that the agency was granted under its revised Regulation[168] as well as a recently issued EBCGA proposal,[169] Frontex will be permitted to process personal data more *actively*. In addition, the EBCGA will obtain a more prominent role in the context of interoperability,[170] the revised VIS[171] and as controller of the ETIAS.[172]

163 14265/17, LIMITE, 20 November 2017, p. 3.
164 CSDP staff, EU Agencies and national competent authorities.
165 Article 10(1)(19), Article 69(1)(b) and (e) and Recital (34) of the 2018 EBCGA proposal, COM(2018) 631 final, Brussels, 12.9.2018.
166 Article 88(1)(c) and Recital (74) of the 2018 EBCGA proposal, COM(2018) 631 final, Brussels, 12.9.2018.
167 Article 41(1), Article 89 and Recital (46) of the 2018 EBCGA proposal, COM(2018) 631 final, Brussels, 12.9.2018.
168 Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).
169 Proposal for a Regulation of the European Parliament and of the Council on the European Border and Coast Guard and repealing Council Joint Action no 98/700/JHA, Regulation (EU) no 1052/2013 of the European Parliament and of the Council and Regulation (EU) n ° 2016/1624 of the European Parliament and of the Council, COM(2018) 631 final, Brussels, 12.9.2018.
170 According to Article 40(3)(a) of the interoperability proposals, the EBCGA shall be the controller of the MID and, under Article 56(4) shall have access to certain data related to the ESP for the purposes of reporting and statistics (without enabling individual identification).
171 See for instance Recital (35) of the VIS proposal.
172 Article 50 of the ETIAS proposal.