Europol's International Exchanges of Data and Interoperability of AFSJ Databases

Florin Coman-Kund*

Data sharing and interoperability aspects of Europol's information systems outside the EU are particularly problematic because of the difficulty of ensuring that adequate legal safeguards are complied with in partner third countries and international organizations. At the same time, the way in which the ongoing interoperability initiatives regarding the Area of Freedom, Security and Justice (AFSJ) databases may influence Europol's international cooperation raises arguably a set of new legal and practical questions that require urgent consideration. This article examines these issues by connecting the Europol-specific legal framework and international practice to the recently adopted AFSJ interoperability regulations as well as to the EU broader data protection framework. It looks more specifically at the balance between data protection/fundamental rights and operational effectiveness throughout Europol's legal framework and practice of international cooperation and examines the implications of interoperability of AFSJ databases on this. On the one hand, interoperability of AFSJ databases is likely to boost Europol as an information hub through extended personal data collection and data processing possibilities, thereby making the Agency more attractive to international partners. On the other hand, the possibility to transfer such data outside the EU requires strong and effective safeguards from a data protection perspective. The article tentatively concludes that Europol's current legal and practical framework for international cooperation seems to tilt the balance on the side of operational effectiveness to the detriment of data protection and fundamental rights, and that the new possibilities offered by the interoperability of AFSJ databases will further enhance this trend.

Keywords: Europol, international cooperation, interoperability, AFSJ databases, data protection, fundamental rights, effective police cooperation

1 INTRODUCTION

Europol is the typical example of an EU agency whose main job and added value consist mostly of its tasks and capacity to analyse and share information. Data processing within Europol's area of competence in the sensitive Justice and Home Affairs (JHA) field already entails intricate interactions with the competent authorities of the Member States and other EU institutions and bodies, such as the Commission, the European Anti-Fraud Office (OLAF) and other EU agencies, in particular Frontex and Eurojust. The sharing of personal data with third countries/

* Erasmus School of Law, Erasmus University Rotterdam. Email: comankund@law.eur.nl.

Coman-Kund, Florin. 'Europol's International Exchanges of Data and Interoperability of AFSJ Databases'. *European Public Law* 26, no. 1 (2020): 181–204.

international organizations adds yet another layer of complexity. It also raises particular concerns as regards data protection and individual rights, whilst potentially increasing the effectiveness of the Agency as an information hub in the field of police cooperation on cross-border crime.

Europol's international cooperation dimension has been substantively redesigned by the recent Europol Regulation in order to align the Agency's legal regime with the Lisbon Treaty and with the Common Approach on EU agencies. Yet just like the previous Europol Council Decision of 2009, the new legal framework designs a special data processing and data protection regime for Europol. This entails tailored technical-operational parameters, obligations and related procedures regarding information processing and exchange in order to ensure that the Agency delivers in a particularly sensitive area. At the same time, data sharing and interoperability aspects of Europol's information systems outside the EU are particularly problematic in view of the difficulty to ensure that adequate legal safeguards are complied with in partner third countries and international organizations.[1]

The two recent interoperability regulations in the Area of Freedom, Security and Justice (AFSJ) add a new dimension to the already complex legal-operational landscape of Europol's international exchanges of data.[2] The new interoperability legal framework promises unprecedented direct access and processing possibilities by Europol of personal data stored in AFSJ databases, including non-law enforcement databases.[3] This will likely enhance significantly Europol's role as the 'EU criminal information hub' and make cooperation with the agency more appealing to international partners. However, the intricate framework governing the partly unified-partly compartmentalized interoperability system also begs important questions regarding governance and supervision, as well as compliance with data protection principles and fundamental rights.[4] This becomes more crucial if Europol transfers personal data processed within the interoperability framework outside the EU.

Against this background, this article reveals salient legal and practical issues illustrating the difficulty to strike a balance between data protection/fundamental

---

1 *See* Case C-362/14, Maximillian Schrems *v.* Data Protection Commissioner, EU:C:2015:650 and Opinion 1/15, Canada-EU PNR Draft Agreement EU:C:2017:592.

2 Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135, 27–84 (22 May 2019), and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 85–135 (22 May 2019) (the Interoperability Regulations).

3 *See* EDPS Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems of 16 Apr. 2018.

4 *See ibid.*, at 9–10.

rights considerations and effective police cooperation in Europol's international cooperation. It also raises a set of topical questions resulting from the interplay between Europol's international exchanges of data and the interoperability of AFSJ databases.

The article begins by expounding some of the peculiarities regarding data sharing and interoperability in the field of police cooperation, with an emphasis on international cooperation aspects (section 1). This is followed by a brief overview of the AFSJ interoperability framework and what it means for Europol (section 2). Next, the broader patchwork EU legal regime concerning international exchanges of personal data is sketched to understand the general principles and elements of Union's approach to data sharing with third countries and international organizations as part of the broader picture relevant for assessing Europol's international exchanges of data (section 3). Against this background, the core elements of Europol's specific data processing/protection framework are examined (section 4). This is followed by a 'zoom in' analysis into Europol's legal framework and practice regarding international exchanges of personal data based on Agency's former and current founding acts (section 5). In a final step, Europol's international exchanges of personal data and the impact of the AFSJ interoperability framework thereupon are assessed from the perspective of the central idea of balancing data protection/fundamental rights and effectiveness in Agency's activities (section 6).

2 DATA SHARING AND INTEROPERABILITY IN THE FIELD OF POLICE COOPERATION

The very nature of police work entailing specific (undisclosed) activities pertaining to criminal investigations and often the use of sensitive data requires special conditions and safeguards with regard to data processing, including data exchanges. At the same time, the potential of police data to interfere intrusively with fundamental rights demands a commensurate data protection regime. This translated traditionally into closed police databases and restrictive conditions regarding data access and data processing.[5] At the same time, crimes are committed across borders and criminal organizations commonly operate across national jurisdictions. This requires swift and efficient cooperation between law enforcement authorities. In this context, enabling cross-border data exchanges between law enforcement authorities is essential to prevent and combat crime effectively. Part of this, interoperability broadly defined as 'the ability of information systems to

[5] Paul de Hert & Serge Gutwirth, *Interoperability of Police Databases Within the EU: An Accountable Political Choice?*, 20(1–2) Int'l Rev. L. Computers & Tech. 25 (2006).

communicate, exchange data and use the information that has been exchanged'[6] seems a suitable technical tool to boost data availability and data sharing for increasing inter alia efficiency in preventing and combating crime.[7] Yet, data sharing and interoperability are not merely technical solutions aiming at increased efficiency in the fight against crime, but they are also entrenched with important political and legal dimensions.[8]

While data sharing and interoperability in the field of law enforcement cooperation within the EU is already a thorny issue,[9] international cooperation adds yet another layer of complexity. Thus, data exchanges with third countries and international organizations raise specific problems. These pertain to the data protection system of the international partners, effective control over data transferred outside the Union, protection of fundamental rights and legal remedies available in other jurisdictions. Therefore, non-interoperability is rather the rule, personal data exchanges with international partners being enabled under strict conditions and based on reciprocity, usually in the framework of bilateral agreements.[10]

3 THE INTEROPERABILITY OF AFSJ DATABASES

The two interoperability regulations have been adopted in response to the perceived need to improve EU border management and combatting of cross-border crime and, more generally, to enhance the internal security of the Union.[11] They aim essentially at ensuring quick, seamless and systematic access to large-scale EU databases in the AFSJ by law enforcement authorities with a view to increase the effectiveness of their operations.[12] The two regulations mainly cover six databases[13] and to a limited extent they also address the possibility to query

---

6 EDPS, *Reflection Paper on the Interoperabilty of Information Systems in the Area of Freedom, Security and Justice* 6 (17 Nov. 2017).

7 *See* Commission, Impact assessment accompanying the proposals for the two interoperability regulations SWD(2017) 473 final, Part 1, 6 and 15–16.

8 *See* Hert & Gutwirth, *supra* n. 5, at 31–32.

9 *See* T. Bunyan, *The 'Point of No Return' Interoperability Morphs into the Creation of a Big Brother Centralised EU State Database Including All Existing and Future Justice and Home Affairs Databases* (Statewatch Analysis), updated July 2018, http://www.statewatch.org/analyses/no-332-eu-interop-morphs-into-central-database-revised.pdf.

10 Hert & Gutwirth, *supra* n. 5, at 25–26.

11 Commission, Impact assessment accompanying the proposals for the two interoperability regulations SWD(2017) 473 final, Part I, at 3; *see also* Recital (9) of the Preamble of the two regulations.

12 *See* Commission, Impact assessment accompanying the proposals for the two interoperability regulations SWD(2017) 473 final, Part I, at 15; *see also* Art. 6 of the two regulations. Law enforcement authorities encompass both Member State authorities and relevant EU agencies (e.g. eu-Lisa, Europol, Eurojust, Frontex, the European Public Prosecutor's Office (EPPO)).

13 Eurodac, the Schengen Information System (SIS), the European Criminal Records Information for Third-Country Nationals (ECRIS-TCN), the Entry-Exit System (EES), the Visa Information System (VIS) and the European Travel Information and Authorization System (ETIAS).

Europol data as well as Interpol databases.[14] They represent yet another symptom of the trend in the AFSJ to increasingly mix migration and security purposes.[15] Far from merely providing technical solutions for better law enforcement, the scope and the interoperability architecture[16] established under the two regulations has far-reaching consequences for the future of data processing and data protection in the AFSJ. It marks a fundamental shift from the principle of a closed environment upon which EU databases have been premised so far to that of a shared environment entailing increased connectivity between databases.[17] This has important implications for the purpose limitation principle as data from different databases established for specific purposes can now be used for rather broad law enforcement purposes.[18] Moreover, the establishment of the Common Identity Repository (CIR) as a centralized super database storing personal data of millions of third country nationals registered in various AFSJ databases creates the possibility of abusive data processing through extended access to personal data, beyond the specific aims of each AFSJ database.[19] Furthermore, the access of law enforcement authorities (LEA) to non-law enforcement personal data for reasons as broad as identifying persons, combating identify fraud as well as preventing and investigating serious crime may easily amount to disproportionate restrictions on the fundamental rights provided by Articles 7–8 of the EU Charter of Fundamental Rights (EUCFR).[20] Yet importantly, the interoperability architecture seems overly complex.[21] This will likely result in significant difficulties regarding the functioning of the system, ensuring a high level of data protection and data security, enabling the traceability of data processing operations, supervision and the accountability of the actors involved. One may conclude that AFSJ interoperability framework set up by the two regulations is mainly motivated by an operational effectiveness-driven philosophy with data protection and fundamental rights concerns being rather second-level concerns.

As far as Europol is concerned, the Interoperability Regulations enable the agency as a 'law enforcement authority' to query the AFSJ databases through the use of a European search portal (ESP), a shared biometric matching service (BMS), a common identity repository (CIR) and a multiple-identity detector (MID). While Europol is bound to use

---

14 *See* Arts 3, 6–7 and 9 of Regulation 2019/818 and 6–7 and 9 of Regulation 2019/817.
15 *See* EDPS Opinion 4/2018 of 16 Apr. 2018, at 9.
16 Consisting of the ESP, BMS, CIR and MID.
17 EDPS, Statement on the Concept of Interoperability in the Field of Migration, Asylum and Security 2–3 (15 May 2017), https://edps.europa.eu/sites/edp/files/publication/17-05-08_statement_on_interoperability_en.pdf.
18 *See* EDPS Opinion 4/2018 of 16 Apr. 2018, at 12.
19 *See ibid.*, at 11–12; *see also* Arts 18–23 of the Interoperability Regulations.
20 *See* EDPS Opinion 4/2018 of 16 Apr. 2018, at 11–18.
21 *See ibid.*, at 9–10.

the interoperability components in the performance of its tasks and in accordance with its access rights to each AFSJ database, the rather vague wording of its mandate in combination with the use of the 'hit/no hit' system will likely result in extended personal data collection by the Agency. Conversely, law enforcement authorities may query Europol data. Yet the possibility to query Europol data is limited to queries that are corroborated with the query of Eurodac, SIS and ECRIS-TCN, while effective access has to take place according to Europol Regulation.[22] Finally, Article 50 of the Interoperability Regulations prohibits in principle the international transfers of personal data processed or accessed by interoperability components. However, this article also includes a non-affection clause covering among others the provisions on international personal data transfers in the Europol Regulation. This essentially entails that international transfers of personal data processed by Europol based on the Interoperability Regulations will be ultimately governed by the Europol Regulation.

4 THE EU APPROACH TO INTERNATIONAL EXCHANGES OF PERSONAL DATA

The wider legal framework relevant for Europol's exchanges of personal data comprises a patchwork of EU primary law provisions, international instruments[23] and EU secondary legislation. Article 16 TFEU enshrines the individuals' right to protection of personal data. It also compels the EU legislator to enact rules regarding data protection and processing by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities within the scope of Union law. Additionally, Article 8 EUCFR enshrines basic data protection principles, such as fair processing, purpose limitation and data subject's rights.

The EU system of reference on personal data protection and processing is the General Data Protection Regulation (GDPR),[24] aimed at setting up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data. Among others, it sets basic principles[25] and limits on the collection and use of personal data, lays down a set of rights for the data subject, and requires the Member States to have independent national bodies in place, responsible for the supervision of any activity linked to the processing of personal data.

---

22 Article 3(2) of Regulation 2019/818.

23 Most importantly, Convention 108/1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

24 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 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, 1–88 (4 May 2016).

25 *See* Art. 5 GDPR.

However, in the field of police and judicial cooperation in criminal matters, it is Directive 2016/680 which governs, as *lex specialis*, the processing of personal data and related personal data protection.[26] The rationale of Directive 2016/680 has to be linked back to Declaration 21 attached to the Founding Treaties supporting the adoption of 'specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation'.[27] Overall, Directive 2016/680 is aimed at ensuring a high level of data protection, whilst also enabling efficient and effective information exchanges between police and criminal justice authorities for the purpose of combating cross-border crime.[28] As such, it also serves as *lex generali* for the more specific legal regimes of law enforcement authorities, being particularly relevant for Europol's personal data processing activities.[29]

In respect of the EU institutions, bodies and agencies, the principles and detailed rules regarding data processing and data protection are laid down in the recent Regulation 2018/1725[30] replacing the partly 'outdated' Regulation 45/2001.[31] Regulation 2018/1725 brings the data protection/processing regime of EU institutions and bodies in line with the new data protection framework applicable to the Member States.[32] It lays down inter alia basic principles regarding quality and processing of personal data,[33] empowers the European Data Protection Supervisor (EDPS) to monitor the application of the data protection rules,[34] and

---

[26] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 Apr. 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, 89–131, 4 May 2016).

[27] Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation. *See also* recital 19 of the Preamble to GDPR.

[28] *See* recitals 4 and 7 of the Directive.

[29] *See* recital (40) of the Preamble of Europol Regulation; *see* for an application, EDPS Opinion 2/18 on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries at 9 (14 Mar. 2018).

[30] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 Oct. 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 39–98, 21 Nov. 2018).

[31] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 Dec. 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ L 8, 1–22 (12 Jan. 2001).

[32] The legal regime under the EU level Data Protection Regulation is considered as 'equivalent' to the GDPR and consistent with Directive 2016/680, *see* Recitals (5) and (10) of the Preamble to Regulation 2018/1725.

[33] According to Art. 4 of Regulation 2018/1725, mirroring Art. 5 GDPR, personal data must be processed in accordance with the following principles: (1) lawfulness, fairness and transparency; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; (7) accountability.

[34] Chapters 6–7 of Regulation 2018/1725. The Regulation also ensures that each EU institution and body appoints at least one data protection officer (DPO) with the task of cooperating with the EDPS,

confers extended enforceable rights[35] and remedies to individuals.[36] Similarly to the data processing/protection regime applicable to Member States, the EU Level Data Protection Regulation reflects the distinction between ordinary personal data processing and processing of personal data for criminal law purposes. Thus, Chapter IX of the Regulation lays down specific provisions regarding the processing of operational data by EU institutions and bodies within the scope of Chapters 4–5, Title V, Part 3 TFEU.[37] Similarly to Directive 2016/680, Chapter IX represents *lex generali* in relation to specific provisions on data processing for criminal law purposes applicable to various EU institutions and bodies. At the same time, the *lex specialis* applicable to EU agencies and bodies should be consistent with the *lex generali*.[38]

All above mentioned legal instruments contain provisions regarding transfers of personal data to third countries and international organizations.[39] There are some differences between the GDPR, Directive 2016/680 and Regulation 2018/1725 in the concrete design of the legal framework for international exchanges of data, but the principled approach to such transfers is quite similar. Thus according to what has been termed as the 'EU data protection model' international exchanges of personal data are subject to a special filter – i.e. an *adequate level of data protection* in the third country/international organization concerned.[40] According to the recent case law of the Court of Justice of the European Union (CJEU) this entails that the level of data protection in the third country/international organization must be 'essentially equivalent' to that guaranteed within the EU.[41] The adequacy of the data protection offered by a third country or international organization should normally be determined by a Commission 'adequacy decision'[42] or, in the absence thereof, demonstrated through adequate safeguards (provided for instance in a legally binding instrument, such as an international agreement, or based on an

---

and ensuring that the rights and freedoms of data subjects are not compromised through data processing (Arts 43–45 of Regulation 2018/1725).

35 For example, the right to access, rectify, block or erase personal data, the right to data portability, the right not to be subject to a decision based solely on automated processing (*see* Ch. 3 of Regulation 2018/1725).

36 Right to file complaints to the EDPS, right to a judicial remedy, right to obtain compensation for damages incurred as a result of unlawful processing of personal data, right of representation by a relevant organization or association (Ch. 8 of Regulation 2018/1725).

37 The provisions of Ch. IX are to be seen as *lex specialis* by reference to the other provisions of Regulation 2018/1725.

38 Recital (11) of the Preamble to Regulation 2018/1725.

39 Chapter 5 (Arts 44–50) of GDPR, Ch. 5 (Arts 35–40) of Directive 2016/680, and Ch. 5 (Arts 45–51) of Regulation 2018/1725.

40 Paul de Hert & Vagelis Papakonstantinou, *The New Police and Criminal Justice Data Protection Directive. A First Analysis*, 7(1) New J. Eur. Crim. L. 14 (2016).

41 *See* Case C-362/14, Maximillian Schrems *v.* Data Protection Commissioner, EU:C:2015:650 para. 73; Opinion 1/15, Canada-EU PNR Draft Agreement EU:C:2017:592, para. 93.

42 Article 45 GDPR, Art. 36 of Directive 2016/680 and Art. 47 of Regulation 2018/1725.

assessment of the data controller).[43] In the absence of a Commission adequacy decision or of adequate safeguards, it is still possible to transfer personal data to third countries/international organizations in derogatory situations. In such cases, the transfer must be necessary for attaining public or individual related-objectives, and subject to specific conditions and safeguards.[44] Another essential element regarding international exchanges of personal data concerns the conditions on onward transfers to authorities in the same third country or to other third countries and international organizations.[45] Importantly, a guiding principle for the application of the provisions regarding international transfers of personal data is that they should not undermine the level of protection offered by GDPR, Directive 2016/680 and Regulation 2018/1725.[46]

As regards transfers of personal data processed for criminal law purposes, the issue of adequate safeguards is particularly important as the use of such data may have massive impact on the fundamental rights of individuals.[47] In this context, compliance with the purpose limitation principle entails special attention for data ownership entailing the prerogative to determine the processing purposes and to impose restrictions on access, use and onward transfers. In this respect, Directive 2016/680 explicitly lays down the principle of data owner prior authorization for international transfers and determines specific requirements in case of onward transfers.[48] Conversely, the specific rules on international transfers of operational data within the scope of Chapter IX of Regulation 2018/1725 remain rather vague on these issues.[49]

5 EUROPOL'S SPECIAL DATA PROCESSING/PROTECTION FRAMEWORK

Swift and efficient processing and exchanges of good quality personal data is essential for Europol to fulfil its core role to assist Member States with preventing and combating serious crime within its mandate. Reflecting the logic expressed in Declaration 21, Europol has been subject since its inception to a specific and autonomous regime on personal data protection and processing.[50] This has also been the

---

43 Article 46 GDPR, Art. 37(1) of Directive 2016/680 and Art. 48 of Regulation 2018/1725.

44 Article 49 GDPR, Art. 38 of Directive 2016/680, and Art. 50 of Regulation 2018/1725; a specific safeguard under Regulation 2018/1725 includes a duty to inform the EDPS.

45 The duty to provide and observe conditions for onward transfers as a requirement for personal data exchanges is stipulated in Art. 44 GDPR, Art. 35 of Directive 2016/680, and Art. 46 of Regulation 2018/1725.

46 Article 44 GDPR, Art. 35(3) of Directive 2016/680 and Art. 46 of Regulation 2018/1725.

47 *See* Recital 26 of the Preamble to Europol Regulation.

48 Article 35 of Directive 2016/680.

49 *See* Art. 94 of Regulation 2018/1725, partly mirroring Art. 25 of the Europol Regulation.

50 Convention based on Art. K 3 of the Treaty on the European Union, on the establishment of a European Police Office (Europol Convention) [1995] OJ C 316/1.

case under the Europol Council Decision of 2009 (ECD),[51] transforming Europol into an EU agency, and further under the Europol Regulation of 2016, upgrading the Agency in light of the EU constitutional framework based on the Lisbon Treaty.[52] Europol Regulation draws a distinction between processing of operational personal data (for the purpose of attaining Agency's core objectives) and non-operational or administrative personal data. Europol's special legal regime covers only the first category whereas for the second category,[53] the general data protection and processing regime under Regulation 2018/1725 is applicable.[54] However, Europol's special data processing and protection framework should take into account the principles upon which Regulation 2018/1725 is based[55] and be consistent with other relevant legal instruments applicable in the area of police cooperation.[56] Yet it is difficult to understand what these rather vague statements entail precisely and how they could be legally enforced provided that the prescriptive part of Regulation 2018/1725 clearly stipulates that it does not apply to Europol.[57]

A bird's-eye view of Europol's special data processing and protection regime reveals overall adherence to the general principles and safeguards applicable within the EU.[58] It also features sector specific provisions justified arguably by the peculiarities of police work. Such are, for instance:

- the competence of Europol to process personal data to identify links between multiple crime areas and investigations covering persons suspected of having committed crimes and even persons who might commit crimes in the future, as well as to determine the relevance of the respective data[59];
- the wide ranging possibility of the Agency to gain computerized access to EU, national or international information systems[60] in order to

---

51 Council Decision 2009/371/JHA of 6 Apr. 2009 establishing the European Police Office (Europol) [2009] OJ L 131/37.

52 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, [2016] OJ L 135/53.

53 Yet based on Recitals (12)–(13) and Art. 98 of Regulation 2018/1725, the Commission shall review by 30 Apr. 2022 the Europol Regulation with a view to applying Ch. IX on processing of operational data to the Agency.

54 Recital 53 and Art. 46 of Europol Regulation.

55 Recital 40 of Europol Regulation.

56 *Ibid*. (in particular Directive 2016/680 and Convention 108/1980).

57 Article 2(3) of Regulation 2018/1725.

58 For example, the general data protection principles, subject's rights to access, rectification, erasure and restriction of data, individual redress and oversight by the EDPS.

59 Recital 25 and Art. 18 of Europol Regulation.

60 For example, Interpol databases or, highly relevant for the purpose of this paper, the EU centralized databases covered by the Interoperability Regulations.

retrieve and process data that is deemed necessary for the performance of its tasks[61];
- specific data retention periods and review[62];
- restricted access of the data subject to own personal data,[63] limited availability of information and transparency regarding Europol's data processing activities.[64]

Some of these provisions are likely to entail more restrictive effects on the fundamental rights of the individuals as compared to the ordinary legal regime under Regulation 2018/1725.[65] This raises particular concerns regarding the justification, necessity and proportionality of these peculiarities, as well as their compliance with basic data protection principles such as lawfulness, fairness and transparency, purpose limitation or data minimization. Utmost attention should be paid to the application of such provisions so that compliance with Europol's data protection framework and observance of individual rights are ensured. In this respect, Europol is required to apply the data protection by design principle by implementing appropriate technical and organizational measures and procedures to ensure that data processing complies with the Regulation and observe the protection of data subjects.[66] Yet unlike Regulation 2018/1725[67] there is no explicit provision imposing on Europol data protection by default.

Under the Europol Council Decision, the Agency put in place separate information systems allowing input, access and analysis of data, namely the Europol Information System (EIS) and the Analysis Work Files (AWF).[68] The EIS was a database that enabled the Agency and the Member States to cross-check personal data regarding persons suspected or convicted for committing crimes within Europol's remit, as well as concerning persons who might commit such crimes in the future.[69] Only the categories of data explicitly listed in the Europol Council Decision could be stored in the EIS[70] and that data could be accessed and used in accordance with clearly defined rules.[71] The AWFs,

---

61 Article 17(3) of Europol Regulation.
62 Article 31 of Europol Regulation.
63 *See* Art. 36 of Europol Regulation.
64 For example, Arts 28(2) and 30(6) of Europol Regulation.
65 Just to give a simple illustration under Arts 14(5) and 78(4) of Regulation 2018/1725 individual's right of access to personal data is free of charge, whereas Art. 36(3) of the Europol Regulation merely provides that in exercising his/her right of access to personal data, the individual should not incur excessive costs.
66 Article 33 of Europol Regulation.
67 *See* Art. 27 of Regulation 2018/1725.
68 Alexandra de Moor & Gert Vermeulen, *The Europol Council Decision: Transforming Europol into an Agency of the European Union*, 47 CML Rev. 1100 (2010).
69 Articles 11–12 ECD.
70 *See* Art. 12 ECD.
71 *See* Art. 13 ECD.

currently relabelled as Analysis Projects (APs) allowed for collecting broader information for specific purposes enabling Europol to provide operational analysis for investigations carried out by the Member States or more general analysis of a strategic nature.[72] An index function enabled performing searches in the AWFs.[73] AWFs were established for specific crime areas, included wider categories of persons[74] and data,[75] and were subject to special and detailed data protection and processing rules.[76] The Agency also created and maintained a secure information exchange network application (SIENA), with the aim of facilitating the secure exchange of information between Member States, Europol, other Union bodies, third countries and international organizations.[77] This information exchange platform interfaces with EIS and is an essential element enabling Europol to become an EU information hub on cross-border crime. An essential feature of Europol's information architecture was that EIS and AWFs were legally separated. This meant that they pursued different purposes, were subject to specific rules regarding access and use, and the Agency could not link or cross-examine data from the different databases.[78]

The Europol Regulation brought a fundamental change in approach as regards data processing by replacing the provisions on pre-defined data processing systems in the Europol Council Decision with a new information structure focusing on the purposes for which data is being processed.[79] Thus, Article 18 of the Europol Regulation enables the Agency to process personal data for the following purposes: (1) cross-checking aimed at identifying connections between information related to crimes within Europol's mandate; (2) strategic or thematic analyses; (3) operational analyses; (4) facilitating exchanges of information between Member States, Europol and other EU bodies, as well as third countries and international organizations. This new data processing approach obviously offers more flexibility and increased information-related powers to Europol potentially enhancing Agency's operational effectiveness.[80]

---

72 Articles 14 and 16 of ECD, also de Moor & Vermeulen, *supra* n. 68, at 1101.
73 Article 15 ECD; *see also* de Moor & Vermeulen, *supra* n. 68, at 1101.
74 For example, witnesses, victims, informants and other relevant persons.
75 For example, language skills, financial and property data, behavioural data, *see* Art. 6 of Council Decision 2009/936/JHA of 30 Nov. 2009 adopting the implementing rules for Europol analysis work files [2009] OJ L 325/14.
76 *See* Arts 7–18 of Council Decision 2009/936/JHA.
77 *See* Recital 24 of the Europol Regulation.
78 *See* EDPS Opinion 31/13 on the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA (31 May 2013) 8–9.
79 *Ibid*.
80 EDPS Opinion 31/13, at 10–11.

Yet this approach also raises concerns as regards the principle of purpose limitation and data minimization and requires effective safeguards and controls.[81] In particular the possibility for Europol to cross-match data collected for different purposes and across different databases and the extended access to Europol data provided to Member States[82] seem problematic from a data protection perspective.[83] The emphasis on operational effectiveness is further amplified by the requirement that the Agency uses new technologies for data processing and most efficient IT-structures for its databases 'to swiftly detect links between investigations and common *modi operandi* across different criminal groups, to check cross-matches of data and to have a clear overview of trends'.[84] The potential intrusive effects of such technologies over essential data protection principles and fundamental rights render the need for adequate safeguards crucial. This trend is also reinforced by the extended possibilities for Europol to access and retrieve information from various EU, international and national databases.-[85] Especially for databases established for other purposes than law enforcement, such as in the case of the Regulation 2019/817, problems arise in terms of purpose limitation, necessity and proportionality as well as the principle of ownership of data.[86] Additionally, much legal uncertainty is created by the conflict rule in Article 17(3) of Europol Regulation establishing the application of the 'stricter legal framework' criterion as regards the access and processing by the Agency of data from various databases. While the new legal framework also lays down a number of countering safeguards, the general impression is that creating fertile ground for effective law enforcement was the main priority behind Europol's reform. In our view, the Interoperability Regulations will further enhance Europol's operational role at the expense of data protection and fundamental rights.

6 EUROPOL'S INTERNATIONAL EXCHANGES OF DATA[87]

This section provides an overview and assessment of Europol's legal framework (6.1) and practice (6.2) regarding exchanges of personal data with third countries and international organizations. In order to provide a system of reference for comparing

---

81 *Ibid*., at 11–13; in my view, the danger that the new information architecture represents for fundamental rights and data protection principles is exacerbated in light of Europol's extended and vaguely defined objectives based on Art. 3 of Europol Regulation.

82 *See* Art. 20 of the Europol Regulation.

83 In this context observance of the principles of necessity and proportionality require utmost attention.

84 Recital 24 of the Preamble to the Europol Regulation.

85 *See* Art. 17 of Europol Regulation.

86 *See* EDPS Opinion 31/13, at 24.

87 This section is partly based on Florin Coman-Kund, *Europol's International Cooperation Between 'Past Present' and 'Present Future': Reshaping the External Dimension of EU Police Cooperation*, 1(1) Eur. & the World: A L. Rev. 1–37 (2018). For a monographic study regarding more generally the international dimension of EU agencies and examining Europol as a case study, *see* Florin Coman-Kund, *European Union Agencies as Global Actors. A Legal Study of the European Aviation Safety Agency, Frontex and Europol* (Routledge 2018).

and better understanding Europol's recent international cooperation framework, a retrospective look is taken at Agency's international exchanges of personal data based on the previous Europol Council Decision. Looking at the former legal framework is pertinent as most of Europol's international cooperation based on the Europol Council Decision has survived for the time being under the new regulation. This overlook allows 'measuring' with a certain degree of precision the balance between data protection and effective data sharing in Europol's international cooperation.

6.1 The legal framework for Europol's international exchanges of data between 'past present' and 'present future'

The legal framework for Europol's international cooperation activities was provided primarily by Article 23 of the *ECD* complemented by Council Decision 2009/934/JHA.[88] Article 23(1) ECD stipulated that Europol's international cooperation activities were instrumental to the core mandate and tasks of the Agency. It permitted the conclusion of cooperation agreements as the main vehicle to formalize Europol's relationship with non-EU partners. Additionally, in line with the core function of Europol, it conveyed that information exchange was the main concern of such instruments.[89] Subject to special conditions, personal data could be exchanged by Europol with third countries/international organizations also before the entry into force of a formal cooperation agreement or even in the absence of such an agreement.[90]

Depending on the types of information that could be exchanged, Europol's previous legal framework operated a distinction between operational (also personal data) and strategic agreements (only non-personal data).[91] The ECD provided two important limitations on Europol's international cooperation: (1) agreements could be concluded only with third countries and international organizations put on a

---

88 Council Decision 2009/934/JHA of 30 Nov. 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information [2009] OJ L 325/6.

89 Article 23(3)–(9) ECD.

90 Article 23(3)–(6) and (8)–(9) ECD. Art. 23(6) and (8)–(9) of the ECD allowed the Executive Director to transfer personal data to third countries and international organizations in the absence of a cooperation agreement only in two situations: (1) when this was 'necessary in individual cases for the purposes of preventing or combating criminal offences' within Europol's competence and (2) when it was considered that the transmission of the data was 'absolutely necessary to safeguard the essential interests of the Member States concerned within the scope of Europol's objectives or in the interests of preventing imminent danger associated with crime or terrorist offences', and after assessing the adequacy of the level of data protection afforded by the entities concerned. However, Europol could not transmit personal data and confidential information to entities which were not included on the 'Council's list' of third countries and international organizations with which the Agency could conclude agreements – Art. 23(5) ECD.

91 Article 1(g) and (h) of Council Decision 2009/934/JHA.

'list' drawn up by the Council[92]; (2) each Europol's agreement was subject to prior approval by the Council.[93]

Regarding specifically the operational agreements, before initiating negotiations, Europol had to carry out 'an assessment of the existence of an adequate level of data protection ensured by the third party'.[94] This assessment was sent to the Joint Supervisory Body (JSB)[95] for an opinion based on which the Management Board decided whether to authorize the Executive Director to start negotiations.[96] After the negotiations, the Management Board asked again the opinion of the JSB on the draft agreement.[97]

Within the framework of cooperation agreements or in derogatory situations, exchanges of information between Europol and international partners were subject to several conditions and restrictions. This entailed among others (1) special provisions limiting data exchanges to Europol's mandate and in light of the principle of data minimization,[98] (2) specification of the purpose and reasons for which data was requested by the third party,[99] (3) exchanging data only via designated contact points specified in cooperation agreements,[100] (4) prior consent of the data owner (Member States),[101] (5) specific conditions and restrictions on onward transfers of data transmitted by Europol to third parties,[102] (6) special safeguards in case of derogatory situations.[103]

Similarly to the former Europol Council Decision, *Europol Regulation* makes transfers of personal data to international partners subject to the conditions that they are necessary for tackling crimes within the scope of Europol's objectives, and that the recipient gives an undertaking that data will be processed for the transmission purpose.[104] It also maintains the prior authorization requirement on onward transfers by third countries/international organizations.[105] The Regulation also

---

92 Article 26(1)(a) ECD; the 'list' took the form of Council Decision 2009/935/JHA of 30 Nov. 2009 determining the list of third States and organizations with which Europol shall conclude agreements [2009] OJ L 325/12.

93 Article 23(2) ECD.

94 Article 5(4) of Council Decision 2009/934/JHA.

95 Until 1 May 2017, JSB was Europol's personal data protection control authority.

96 Article 6(1) of Council Decision 2009/934/JHA.

97 Article 6(3) of Council Decision 2009/934/JHA.

98 For example, Art. 23(1),(3),(6) ECD.

99 Article 15 of Council Decision 2009/934/JHA.

100 Article 23(2) ECD.

101 Article 24(1) ECD.

102 Articles 17–18 of Council Decision 2009/934/JHA.

103 That is, the duty of Europol's Director to inform as soon as possible the Management Board and the JSB about the decision to transfer and the basis for the data protection adequacy assessment – *see* Art. 23(8) ECD.

104 Article 23(6) of Europol Regulation. Yet the phrase 'crime falling within the scope of Europol's objectives' is very broad as the crimes within Europol's remit are not defined and the Regulation has further expanded the scope of Agency's mandate by adding for instance, the vague category of crimes that 'affect a common interest covered by a Union policy'.

105 Article 23(6) of Europol Regulation.

keeps and extends the scope of the rather questionable prohibition to process data 'clearly (…) obtained in obvious violation of fundamental rights'[106]

The Regulation also brings important substantive changes to Europol's international dimension with a view, which is claimed to align it with the Lisbon Treaty and to the recent EU general data protection/processing framework. To begin with, there will no longer be Europol cooperation agreements. While Europol's agreements concluded until 1 May 2017 are preserved, future international agreements concerning the Agency must be concluded according to Article 218 TFEU.[107] Europol is still allowed to conclude working arrangements and administrative arrangements. The working arrangements are designed to cover cooperative relations, except for exchanges of personal data, and are explicitly characterized as not being binding for the EU and the Member States.[108] Europol's administrative arrangements are intended to implement 'Article 218 TFEU' agreements or the Commission's adequacy decisions regarding the transfer of personal data. Yet, unlike the working arrangements, nothing is mentioned about their legal nature.[109] In contrast with Europol's agreements under the ECD, the Regulation does not provide details regarding the procedure for the negotiation and conclusion of Agency's working and administrative arrangements.[110]

Next, the Europol Regulation enhances Commission's role with regard to Europol's international dimension. Most obviously, this is exhibited by formalizing Commission's 'adequacy decisions'[111] as one of the legal bases allowing the Agency to exchange personal data.[112] The implementation of such decisions may require the Agency to conclude specific administrative arrangements with competent authorities of third countries and international organizations.[113] Moreover, Europol's Executive Director has a duty to report to the Management Board on the implementation of Commission's 'adequacy decisions'.[114] The Regulation also bolsters the Commission's position by granting it the power to review Europol's

---

106 Article 23 (9) of Europol Regulation; cf. Art. 20 (4) of Council Decision 2009/934/JHA.

107 Article 25(1) of Europol Regulation. Such international agreements must 'adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of the individuals'.

108 Article 23(4) of Europol Regulation.

109 Article 25(1) of Europol Regulation.

110 Except that the Management Board decides on the conclusion of such instruments, and that the Executive Director must inform the Management Board on the intention to initial such arrangements – Arts 11(1)(r) and 23(3) of Europol Regulation.

111 Based on Directive (EU) 2016/680. According to Art. 36 in combination with Recital 67 of the Preamble of this directive, an 'adequacy decision' is a Commission decision determining that the third country or the international organization in question 'ensures an adequate level of protection', which is 'essentially equivalent to that ensured within the Union'.

112 This entails in theory a broadening of the category of 'international partners' with whom Europol may exchange extensively personal data.

113 Article 25(1) of Europol Regulation.

114 Article 25(2) of Europol Regulation.

'surviving' cooperation agreements with a view to maintain or replace them with 'Article 218' agreements.[115]

In line with Article 88(2) TFEU, parliamentary scrutiny of Europol's international cooperation appears to be formally enhanced through the Joint Parliamentary Scrutiny Group (JPSG) bringing together members of the EP and of national parliaments.[116] Also, the supervision over Europol's processing of personal data seems reinforced by replacing the JSB with a European Data Protection Supervisor (EDPS) with far-reaching tasks and powers.[117] The EDPS may inter alia warn or admonish Europol, compel the Agency to rectify, restrict, erase or destroy incorrectly processed personal data, ban Europol's processing operations, or refer a matter to the EP, the Council, the Commission or the CJEU.[118]

Similarly to the ECD, the New Regulation provides for derogations, enabling Europol to transmit personal data without having to rely on a Commission adequacy decision, an 'Article 218 TFEU' agreement, or a Europol cooperation agreement. Yet the new legal framework expands the list of reasons for case-by-case transfers,[119] some of these reasons being quite broadly formulated.[120] It also formally opens up, for the same reasons, the possibility for the Agency to transfer sets of personal data for renewable periods of maximum one year.[121] The safeguards designed by the New Regulation with regard to these derogatory situations entail essentially a fundamental rights balancing exercise[122] and a duty of the Executive Director to inform *ex post* the Management Board and the EDPS, in case of individual transfers,[123] respectively a duty of the Management Board to act in agreement with the EDPS for sets of transfers.[124] While Europol has now extended possibilities to transmit personal data through derogations, the safeguards designed by the new legal framework seem meager as compared to the detailed data protection adequacy assessment imposed by the ECD.[125]

A final point, also relevant in the context of the interoperability of AFSJ databases, pertains to the conditions and safeguards regarding Europol's computerized access to international and third country information systems. The main requirements for Europol's processing of data from such sources entail at least (1)

---

115 Article 25(4) of Europol Regulation.
116 Article 51(1) of Europol Regulation.
117 *See* Art. 43 of Europol Regulation.
118 Article 43(3) of Europol Regulation.
119 Article 25(5) of Europol Regulation.
120 Such as the grounds mentioned under Art. 25(5)(d) and (e).
121 Article 25(5)–(7) of Europol Regulation. *See also* Europol JSB, Opinion 13/56, at 33.
122 This is slightly different for individual transfers as compared to massive transfers – *see* Art. 25(5) and (6).
123 Article 25(7) of Europol Regulation.
124 Article 25(6) of Europol Regulation.
125 Cf. Arts 23(8)-(9) ECD.

the existence of an international, EU or national instrument governing access conditions and the use of information; (2) access granted to duly authorized Europol staff and (3) only as far as necessary and proportionate for the performance of their tasks.[126]

6.2 Europol's international dimension in practice

Europol has currently twenty-six agreements: eighteen operational agreements – seventeen with third countries[127] and one with Interpol – and eight strategic agreements – six with third countries[128] and the remaining two with United Nations Office on Drugs and Crime (UNODC) and World Customs Organization (WCO).[129] Under the New Europol Regulation, the Commission has initialled in 2017 the process for the negotiation of further eight 'Article 218 TFEU' agreements with third countries.[130]

The core part of the agreements deals mainly with information exchanges including confidentiality duties. Importantly, the agreements provide for the possibility to assign liaison officers (LOs) with a view to operationalize contacts and facilitate information exchanges between the parties. The final provisions of the agreements usually cover dispute settlement, amendment procedures, entry into force, termination of the agreement, and the relationship with other international instruments. The operational agreements in particular include detailed provisions on the procedures and obligations of the parties concerning the exchange, processing and handling of personal data. Generally, the agreements include provisions mirroring Europol's legal framework concerning purpose limitation and data minimization, restrictions on processing, prior authorization in case of further processing and onward transmission, storage conditions, association at Europol's analysis projects, confidentiality and security conditions. They also lay down a right for the individuals and private entities to have access to personal data concerning them. Additionally, these agreements comprise provisions on the

[126] Article 17(3) of Europol Regulation; as mentioned previously, the provision according to which access and use of information from foreign information systems is governed by the relevant instrument to the extent it contains stricter rules then Europol Regulation may create legal uncertainty as to the legal regime applicable and may be misleading insofar it suggests that access by Europol to foreign databases would routinely be subject to the Europol Regulation.

[127] Albania, Australia, Bosnia and Herzegovina, Canada, Colombia, Former Yugoslav Republic of Macedonia (FYROM), Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Serbia, Switzerland, Ukraine, USA (2002).

[128] Brazil, China, Russian Federation, Turkey, United Arab Emirates, USA (2001).

[129] A list of cooperation agreements can be found at https://www.europol.europa.eu/partners-agreements.

[130] COM(2017) 798 final (Jordan); COM(2017) 799 final (Turkey); COM(2017) 805 final (Lebanon); COM(2017) 806 final (Israel); COM(2017) 807 final (Tunisia); COM(2017) 808 final (Morocco); COM(2017) 809 final (Egypt); COM(2017) 811 final (Algeria).

liability of the contracting parties for damages caused to individuals resulting from errors in the exchange and processing of personal data.

Whilst the clauses of Europol's cooperation agreements are presumably consistent overall with Agency's former and current legal framework, they also raise a number of issues from a data protection perspective. First, the scope of data transfers remains potentially very broad and insufficiently defined because of the elusive list of crimes within Europol's mandate. Second, the term of third country competent authority is given a broad meaning potentially encompassing all authorities entrusted with law enforcement tasks, though the more recent agreements also provide a list of authorities with whom Europol can exchange data. This bears the risk that information transmitted by Europol to third countries might be used by various law enforcement authorities with potentially intrusive effects on individual rights.[131] Third, and closely related to the previous point, specifying clearly and precisely the purpose of transmission is key to ensuring full compliance with EU data protection framework. Yet Europol's agreements simply provide that the purpose of transmission must be indicated together with the reason for transmission. Fourth, processing of Europol transmitted data beyond the initial purpose needs to be duly justified and allowed only if necessary and proportionate.[132] However, Europol's agreements just stipulate that further processing must be authorized by the transmitting party. Fifth, onward transfers to other third parties should be subject to strict conditions and safeguards, but Europol's agreements merely provide that such transfers are subject to Europol's consent. Sixth, one may wonder whether the condition that parties can exchange sensitive personal data only 'if strictly necessary' is sufficient to ensure the high level of protection required by this type of data. Finally, while Europol's agreements include some individual guarantees such as the prohibition to process data manifestly obtained in violation of fundamental rights, rights to access, check, correct or delete personal data and liability, they largely lack safeguards regarding the enforcement of these rights.[133] Europol's international data exchanges practice so far raises thus questions regarding the observance and rigorous application of fundamental rights and data protection standards as devised by the CJEU in its case law.

In practice, based on the existence of a cooperation agreement, third countries and international organizations may access, usually through LOs posted at Europol's headquarters, the EIS and make use of SIENA. In the case of EIS,

[131] A prime example is the 2002 Supplemental Agreement between Europol and USA, granting access to personal data transmitted by Europol to a broad range of competent US federal, state and local authorities (Art. 7).

[132] *See* EDPS Opinion 2/18 on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries, at 10–11 (14 Mar. 2018).

[133] Cf. EDPS Opinion 2/18 on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries, at 13 (14 Mar. 2018).

third parties may query and store data in the system only through Europol authorized staff.[134] Access to SIENA requires the conclusion of a memorandum of understanding (MoU) between Europol and the partner country or organization based on an existing cooperation agreement.[135] Another practical issue pertains to the fact that so far the implementation of Agency's cooperation agreements has remained largely a matter of in-house work with little monitoring and oversight from outside. Europol has concluded recently the first working arrangements under Article 23(4) of the Europol Regulation.[136] The provisions of these instruments mirror to a great extent the structure, content and wording of Europol's strategic and operational agreements, suggesting that such instruments may qualify as legally binding agreements in disguise. They also largely duplicate the data protection concerns discussed earlier with regard to Europol's agreements. Additionally and quite interestingly, although the working arrangements provide explicitly that they do not represent a legal basis for exchanges of personal data, they cover nevertheless transmissions of personal data based on the derogations in the Europol Regulation or allowed under the national legislation of the respective third country.[137] In this respect, the working arrangement with New Zealand is more clear specifying that it covers exchanges of non-personal data between Europol and New Zealand police as well as transfers of personal data by the New Zealand Police to Europol.[138] Europol's international cooperation practice based on the 2016 Regulation is still at a nascent stage and therefore difficult to assess. Yet these early developments already point to problematic areas of friction with the relevant EU data protection framework. Moreover, only time will tell how Europol's extended derogations regime regarding transmission of personal data abroad will work in practice.

7 TIPPING THE BALANCE BETWEEN DATA PROTECTION AND EFFECTIVE POLICE COOPERATION?

In line with the EU data protection model, Regulation 2016/794 maintains the system based on an adequate level of data protection requirement and restricted interoperability in Europol's international exchanges of data. At the same time it enlarges the possibilities

134 *See* Europol Consolidated Annual Activity Report 2018, at 22.

135 For example, Georgia recently concluded a SIENA connection MoU with Europol based on the Agreement on strategic and operational cooperation between the two parties of 2017 – *see* Europol Consolidated Annual Activity Report 2018, at 28.

136 With Israeli, Japanese and New Zeeland law enforcement authorities; no agreements have been concluded with these countries under the previous Europol framework.

137 For example, Arts 10–11 of the Working arrangement with the law enforcement authorities of Israel.

138 Article 1 of the Working arrangement with the New Zealand Police. Yet one may wonder why the New Zealand Police would be willing to transfer personal data to Europol in the absence of a corresponding obligation on behalf of the Agency.

for the Agency to cooperate with third countries and international organizations by supplementing the legal bases enabling regular exchanges of personal data and through redesigning Agency's derogations system. In this respect, the purpose-based data processing introduced by the new legal framework covers the aim of 'facilitating the exchange of information between Member States, Europol (…) third countries and international organisations'[139] entailing essentially the operation and upgrading of SIENA. Also the addition to the Agency's core mandate of the vaguely defined category of 'forms of crime which affect a common interest covered by a Union policy' entails extended data processing powers for Europol, including with regard to international exchanges of data. Additionally, Europol's data processing capacity is enhanced as the Agency is urged to use advanced information technologies and most efficient IT structures, as well as to access and process information from various databases as a way to improve effectiveness of law enforcement. The latter covers, for instance, the possibility to access the AFSJ databases under the Interoperability Regulations, which is particularly problematic considering that some of these databases have been established for other purposes than law enforcement. All this bears the promise to transform Europol into a genuine EU criminal information hub providing vast and valuable datasets and information sharing capabilities. As such the Agency will likely become an increasingly attractive partner for third countries and international organizations.

In turn these developments require commensurate fundamental rights and data protection safeguards. In this regard, the derogatory regime regarding the transfer of personal data to third states and international organizations has a broader scope under the Europol Regulation as compared to the ECD, covering both case-by-case transfers and sets of transfers of personal data, and features open-textured provisions. It also suggests a lower threshold on effecting such international transfers. The safeguards designed by the New Regulation with regard to these derogatory situations entail a duty of Europol's Executive Director to inform ex post the Management Board and the EDPS, in case of individual transfers, and the duty of the Management Board to act in agreement with the EDPS when authorizing a set of transfers. Additionally, in the case of individual transfers the Executive Director is required to assess whether 'fundamental rights and freedoms of the data subject concerned override the public interest in the transfer',[140] whilst sets of transfers require taking into account 'the existence of adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals'.[141] Still this seems less strict than the requirement imposed on Europol

[139] Article 18(2)(d) of Europol Regulation.
[140] Article 25(5).
[141] Article 25(6).

under ECD to thoroughly assess the adequacy of the level of data protection of the third country/international organization concerned.[142]

Next, one may wonder whether some of the safeguards designed specifically for international exchanges of data are adequately addressing data protection considerations.

Thus, for derogations in individual cases it is rather unclear what are the criteria on the basis of which the Executive Director will assess whether the public interest justifying the transfer of personal data is overridden by the fundamental rights of the data subject. One may also wonder whether, for the purpose of determining whether information can be processed or not, the threshold of having 'clearly been obtained in obvious violation of human rights' unduly priorities operational considerations over data protection and individual rights aspects.[143]

One remaining problem under the New Europol Regulation is reconciling Europol's international cooperation practice based on 'problematic' cooperation agreements with the EU data protection legal framework. In this respect, the New Regulation sets a deadline for the Commission in 2021 to evaluate existing Europol agreements and to propose eventually their replacement with Article 218 TFEU agreements, which may take another few years to negotiate and conclude. Another issue which has not been addressed by the New Europol Regulation relates to the use of the SIENA enabling third countries and international organizations to potentially exchange without Europol's involvement personal data over crimes not linked to Europol's mandate.[144] As to the nascent international practice under the new legal framework, it remains to be seen how the new projected international agreements based on Article 218 TFEU will ensure 'adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals'.[145] The working arrangements concluded so far by Europol under the new regulation already raise some questions regarding their consistency with the EU legal framework.

Whilst, the new legal regime is likely to boost Agency's operational effectiveness in international exchanges of data, it seems prima facie to fall short on the data protection/fundamental rights side, at least as compared to Europol's previous legal framework. In our view, the Interoperability Regulations will further amplify this trend through the new extended possibilities granted to Europol to collect and

---

142 According to the CJEU, the level of data protection abroad should be 'essentially equivalent' to that offerred by EU law – *see* Schrems and Opinion 1/15.

143 Article 23(9).

144 *See* Europol JSB, Opinion 13/31, at 7–8.

145 Such safeguards should ensure that the level of protection resulting from these agreements is essentially equivalent to the EU level of protection, *see* EDPS Opinion 2/18 on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries, at 15 (14 Mar. 2018).

process personal data from multiple AFSJ large-scale information systems. The broadly defined Europol's objectives and crime areas are likely to enable to Agency to extensively access personal data, including from non-law enforcement databases under the Interoperability Regulations especially through the use of CIR. Based on Article 50 of the Interoperability Regulations such data could then be transmitted to third countries and international organizations according to Europol Regulation. In view of the rather encompassing and flexible derogations regime according to the Europol Regulation, the transfer abroad of personal data originating in interoperability components would be relatively easy while potentially entailing significant intrusive effects on fundamental rights.

8 CONCLUSION

Overall, the present analysis suggests that under the Europol Regulation the relationship between data protection/fundamental rights and effectiveness of operational police cooperation, including interoperability aspects, remains a thorny issue. In particular, it appears that more than ever before, the emphasis lies on the operational side of the coin both in the law and practice of Europol's international exchanges of personal data at the expense data protection and fundamental rights. The recent AFSJ Interoperability Regulations seem to reinforce this trend by promising unprecedented direct access and processing possibilities by Europol of personal data stored in AFSJ databases, including non-law enforcement databases.[146] This will likely enhance significantly Europol's role as the 'EU criminal information hub' and make cooperation with the agency more appealing to international partners. Given the potentially significant intrusive effects on individuals of transferring personal data abroad, the main challenge will be how to maintain a decent level of respect for EU data protection and fundamental rights standards.

[146] *See* EDPS Opinion 4/2018 of 16 Apr. 2018.