21. FROM TAMPERE OVER STOCKHOLM TO LUXEMBOURG AND BRUSSELS: WHERE ARE WE NOW? THE EVOLUTION OF AFSJ DATABASES – MEANDERING BETWEEN SECURITY AND DATA PROTECTION

Teresa Quintel

1. Introduction: General Concerns Related to the Interoperability of EU Databases

At times, the different objectives that the European Union's (EU) Area of Freedom, Security and Justice (AFSJ)[1] should achieve are difficult to reconcile. The removal of the EU internal borders certainly brought more freedom and propelled the cooperation between Member States in both security and justice affairs. Nevertheless, the views on how to achieve security while offering the highest standards of justice diverge. Consequently, the means of cooperation between competent authorities in the EU Member States differ as well, both in the area of border control, migration and asylum, but also in the field of police and judicial cooperation.

1 The objectives for the AFSJ are laid down in Article 67 TFEU.

To compensate for the abolition of internal border controls in the Schengen Area, large-scale databases were set up at EU level to facilitate the information exchange between law enforcement authorities on the one hand and to improve the administration of visas, facilitate border checks and to better manage asylum applications on the other. Over time, the founding acts of those databases, initially established for specific purposes and with strict access requirements, were revised in order to serve more purposes, retain additional categories of data and provide broader access to more authorities.

A number of immigration databases allow law enforcement authorities access for the purposes of the prevention, detection, and investigation of crime. This type of access is often met with critical acclaim, as such access risks to associate two undoubtedly different objectives - managing migration and combating crime (Vavoula, 2020). Particularly during recent years, migration has become a fiercely debated element in the internal security discourse within the EU. In many EU Member States, the security-versus-privacy debate reached new dimensions during the aftermath of the arrival of great numbers of individuals seeking asylum in the EU in 2015.

In order to close the remaining information gap between EU databases, the EU Commission proposed, in December 2017[2], the Interoperability of EU large-scale IT-systems, which was adopted in April 2019.[3] The Interoperability framework is supposed to connect six EU databases, half of which are currently operational,

2 Proposal for a Regulation on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and Proposal for a Regulation on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, COM(2017)793 and 794.

3 Regulation (EU) 2019/817 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 and Council Decisions 2004/512/EC and 2008/633/JHA [2019] OJ L 135/27 and Regulation (EU) 2019/818 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 [2019] OJ L 135/85 (hereafter 'Interoperability Regulations').

the other half foreseen to be established by 2023 (Luyten and Voronova, 2019).[4]

Three general concerns may arise with the Interoperability regime: Firstly, the complexity of the anticipated system makes it increasingly difficult for individuals to grasp the processing operations, which may prevent them from exercising their data subject rights: understanding the interoperable system requires understanding the underlying databases as well as the different actors that are responsible for replying to access and rectification requests.

Secondly, beyond their primary purposes of border control, asylum, migration and the management of short-term visas, all underlying databases, including the Interoperability components, are supposed to contribute to the fight against serious crime, the detection of identity fraud and the identification of (unknown) suspects.[5] In that vein, the Interoperability Regulations shall streamline law enforcement access to non-law enforcement databases that hold information concerning third country nationals (TCNs). This means that not only the initial purpose of the underlying databases was changed from an immigration-related to a law enforcement purpose. That change of purpose also has an impact on the data protection regime that applies to the processing of personal data retrieved from the systems.

Thirdly, besides broadened access rights for national competent authorities, EU Agencies that play an increasingly prominent role in the area of border control and migration management were attributed more access possibilities to the databases. Hence, the number of authorities accessing and further processing the personal data from the different systems multiplied, which might not only affect the willingness of different authorities to share information via the databases, but also impinge on the trust among those authorities.

4 As stated in the proposals, the Commission aims to achieve interoperability by the end of 2023.

5 See Article 2 of the Interoperability Regulations.

Furthermore, the new processing operations and the additional actors that will process the data in the complex systems will render supervision more difficult and require close cooperation between supervisory authorities. The work of national data protection authorities (DPAs) and the European Data Protection Supervisor (EDPS) will be decisive not only for scrutinizing and, where necessary, sanctioning data controllers, but also to ensure that individuals will be able to enjoy their right to effective administrative and judicial review.

2. From Immigration to Law Enforcement Databases and Interoperability

The operational databases - Eurodac[6], the Schengen Information System (SIS)[7] and the Visa Information System (VIS)[8], were established at different times, for different purposes and to be used by different actors. Whereas the Eurodac shall facilitate the determination of the first country of entry of asylum seekers, the VIS is supposed to support the issuance of short-term visas and

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

7 Regulation (EU) 2018/1860 of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals [2018] OJ L 312/1; Regulation (EU) 2018/1861 of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 [2018] OJ L 312/14 and Regulation (EU) 2018/1862 of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 and Commission Decision 2010/261/EU [2018] OJ L 312/56.

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

the SIS is a law enforcement database, which enables competent authorities to communicate and exchange information via secure channels. However, during the past years, all three databases have been revised, with the latest changes to the Eurodac[9] and the VIS[10] currently pending, and three new SIS Regulations having been adopted in November 2018. All revisions are based on additional legal bases, adding new purposes to the existing ones. Beyond those new purposes, further categories of data shall be added, and the systems shall be rendered interoperable, together with three new databases for which legislation has recently been adopted.[11] In total, five (primarily) immigration systems and the SIS shall form the underlying databases that will build the Interoperability framework.

In a nutshell, Interoperability will connect the underlying systems by creating three new centralized databases[12] and a search tool that will enable simultaneous queries in all databases. This will create new layers of complexity and thus, make it more difficult for individuals to understand who is processing their personal data and whom to contact to exercise their rights. Interoperability will also create new access possibilities for competent authorities and will obscure the steps in which data that were connected led to a final result.

9 Proposal for a Regulation 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) [2016] COM(2016) 272 final.

10 Proposal for a Regulation 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 [2018] COM(2018) 302 final.

11 The Entry-Exit System (EES), The European Travel Information and Authorization System (ETIAS) and the European Criminal Records Information System (ECRIS-TCN).

12 A Common Identity Repository (CIR), a Biometric Matching Service (BMS) and a Multiple Identity Detector (MID) will store biometric and biographical data centrally. A European Search Portal (ESP) will enable competent authorities to search all systems simultaneously and to be granted access in accordance with the access rights under each individual system.

What is remarkable is that, while the original setup of the operational databases did not grant access to law enforcement authorities, such access was added during the early revisions of their founding acts. Later on, law enforcement access became a default function for the recently adopted systems and the Interoperability components. Hence, the databases were transformed from serving exclusively immigration-related purposes to systems that may all be accessed by competent law enforcement authorities for the prevention, detection and investigation of serious crime. Interoperability pushes such repurposing of personal data even further, by abolishing the cascading system of prior checks in national databases.

The consequences of such transformation are manifold and will not only lead to unnecessary processing operations but might encourage false suspicions against persons whose data are stored in the databases, to the detriment of data subject rights and an increased workload for competent authorities.

On the one hand, the abolition of mandatory checks in national databases prior to accessing the EU systems seems illogical with respect to criminal investigations: the question here would be why a national law enforcement authority should check an EU database such as Eurodac *before* checking a national police database for fingerprints of a potential suspect or perpetrator? It seems likely that this *reverse* procedure would simply lead to additional processing operations, where competent authorities would have to search national databases after an unsuccessful query in the EU systems.

What is more, a hit during a search in the EU databases could lead to an inference that could have been clarified with a prior check in the national systems. Such inference may lead to an unnecessary suspicion against a person and could motivate a police officer to process personal data of that person within a data protection regime that would make it easier to limit the person's rights.

On the other hand, the checking of immigration databases for purposes of criminal investigations might be futile and lead to

additional work for competent authorities. Comparing the access requests by law enforcement authorities to the SIS and Eurodac, the different ratio is striking. While the SIS was accessed a total of 6.185.199.597 times by the sum of all Member States in 2018,[13] searches in Eurodac carried out by law enforcement authorities amounted to 296 by 10 Member States.[14] Certainly, it should be taken into account that while Eurodac's main purpose is related to asylum, the SIS is a law enforcement database that, obviously, is mainly searched by competent authorities. However, the above numbers demonstrate that law enforcement authorities do not make use of the access possibilities granted to them regarding Eurodac. Consequently, necessity and proportionality of such access rights are not attained.

Beyond standardizing law enforcement access to the underlying databases and streamlining it for the new interoperable system, the Interoperability Regulations shall authorize national police authorities to access one of the interoperability components, the Common Identity Repository (CIR), for the purpose of identifying a person.

Under Article 20 of the Interoperability Regulations, national police authorities may search the CIR during identity checks with biometric data of TCNs. For each person whose data are stored in the CIR, the system shall create an individual file that separates the data according to the information system from which they originated.[15] Moreover, the individual files shall include a reference to the actual record in the underlying databases to which the data belong[16] and retain links that were generated during a so-called

13 SIS II – 2018 annual statistics, 5; https://www.eulisa.europa.eu/Publications/Reports/SIS%202018%20statistics.pdf (accessed on 30 October 2019).

14 Europol performed 10 category 5 searches, see: Eurodac – 2018 annual report, 14; https://www.eulisa.europa.eu/Publications/Reports/2018%20Eurodac%20Annual%20Report.pdf. (accessed on 30 October 2019).

15 Article 18(1) of the Interoperability Regulations.

16 Article 18(4) of the Interoperability Regulations. Moreover, links from the multiple identity detection, to be carried out in another interoperability component, will be included in each individual file in the CIR.

multiple identity detection.[17] Theoretically, a police officer could stop a person on the street to carry out a random identity check, querying the component with biometric data of that person. While the data stored in the CIR are essentially the same as on a conventional passport and hence, do not reveal more information than a travel or ID document, the reference to the underlying databases and the links on multiple identities could prompt the querying officer to draw certain conclusions about a person.

In addition, a police officer (and Europol staff) may, under Article 22 of the Interoperability Regulations, access the CIR for the prevention, detection and investigation of serious criminal offences, where there are reasonable grounds to believe that consultation of the databases would sustain a suspicion that personal data of a suspect or perpetrator are stored in the underlying systems.[18]

While random police checks in the Schengen Area are in line with the case law of both the Court of Justice of the European Union (CJEU) and the European Court on Human Rights (Quintel, 2018), Article 20 identity checks are by far more intrusive from a privacy point of view and may lead to unjustified suspicions against individuals.

3. Access to EU Databases by EU Agencies

Beyond the broadened access to the databases by national (law enforcement) authorities, access has also been widened for those EU Agencies that are involved in the management of migration at the external Schengen Borders, for instance during secondary security checks in the so-called hotspots.[19]

Europol, an EU Agency originally responsible to support

17 Article 19(2) of the Interoperability Regulations. One of the interoperability components, the Multiple Identity Detector, will store links that indicate whether a person used fraudulent identities to enter the Schengen Area.

18 Article 22(1) of the interoperability Regulations.

19 European Commission, Hotspot Approach, https://ec.europa.eu/home-affairs/content/hotspot-approach_en. (accessed 19 October 2019).

national law enforcement authorities in the fight against organized crime and terrorism, became increasingly involved in migration related investigations such as migrant smuggling or document fraud. All EU databases feature provisions granting Europol access to retained data for the purposes of fighting serious crime and terrorism. Requirements for access by Europol staff are, inter alia, the existence of reasonable grounds to consider that the consultation of data in the systems may substantially contribute to the prevention, detection or investigation of criminal offences, or, if consultation is necessary to support and strengthen action by Member States within the mandate of Europol (Quintel, 2019). Similar conditions for Europol access apply regarding the Interoperability components.[20] In addition, Europol data will be searchable via the European Search Portal[21] and will be entered into a watch-list that will be included in one of the underlying databases.[22]

The European Border and Coast Guard Agency (EBCGA), initially established as supranational Agency tasked to assist the EU Member States with migration management and border control functions, developed into a powerful coordination hub between the Member States and other EU Agencies as well as third countries, progressively gaining operational competences in further areas related to migration. Under the new EBCGA Regulation[23], the Agency's activities will be significantly broadened by strengthening the EBCGA with a new mandate to protect the EU's external

20 Article 22 of the Interoperability Regulations.

21 Chapter II of the Interoperability Regulations.

22 The European Travel Information and Authorization System (ETIAS) will contain a watchlist to which Europol shall add information on the basis of information related to terrorist offences or other serious criminal offences, see Article 34 (2) and (3) of Regulation (EU) 2018/1240 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 [2017] OJ L 236/1.

23 Council of the European Union Press Release, 'European Border and Coast Guard: Council confirms agreement on stronger mandate' (April 2019), https://www.consilium.europa.eu/en/press/press-releases/2019/04/01/european-border-and-coast-guard-council-confirms-agreement-on-stronger-mandate/?utm_source=dsmsauto&utm_medium=email&utm_campaign=European+Border+and+Coast+Guard%3a+Council+adopts+revised+regulation. (accessed 10 November 2019).

borders, carry out returns more effectively, and to cooperate with third countries. In addition, the Regulation builds upon the increasing number of tasks and responsibilities of the EBCGA regarding irregular secondary movements and the Agency's role in (forced) returns of TCNs.[24]

Both Agencies will play a central role with regard to the development and operation of EU databases and Interoperability. While Europol's databases will be connected to the interoperable system, the EBCGA will be responsible for the management of essential parts of the Interoperability regime.[25] Evidently, both Agencies will feed the databases with information gathered during their deployment and will be granted access to the systems for the performance of their tasks. While the growing synergy between the tasks of the two Agencies may be seen as progress towards a more harmonized and integrated EU border management approach, the overlapping purposes for which they may exchange personal data may lead to concerns, as different data protection regimes apply, not only to the two Agencies, but also on national level.

4. Data Protection Concerns

4.1 Data Protection Concerns related to Law Enforcement Access

As mentioned above, a police officer checking data for identification purposes in the CIR could discover links to a person in law enforcement databases and draw inferences that might lead to an unjustified suspicion against a person. While for data processing operations relating to immigration and asylum the General Data Protection Regulation (GDPR)[26] would be applicable, data pro-

24 Cf.: FRA Opinion 5/2018, *The revised European Border and Coast Guard Regulation and its fundamental rights implications Opinion of the European Union Agency for Fundamental Rights*, 17 (November 2018).

25 In relation to the processing of data in the Multiple Identity Detector, the European Border and Coast Guard Agency shall be a data controller within the meaning of point (8) of Article 3 of Regulation (EU) 2018/1725, see Article 40(3)(a) of the Interoperability Regulations.

26 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with

cessed for law enforcement purposes falls within the scope of Directive (EU)2016/680[27], which is applicable for processing carried out in the area of police and criminal justice (Sajfert and Quintel, 2019). Evidently, in that area, data subject rights may be restricted more flexibly and transparency requirements are considerably lower than under the GDPR, in order not to obstruct the work of law enforcement authorities. However, where migration is associated with security concerns, the unclear delineation between the Regulation and the Directive could easily lead to the application of the wrong instrument and a lowering of data protection rights for individuals where a police officer applies the rules under the Directive instead of the Regulation (Quintel, 2018). Hence, that officer, basing a search in the CIR on a suspicion that a person could be a perpetrator or suspect, would be able to apply the rules under the Directive and restrict data subject rights more flexibly than if he would apply the GDPR to his processing activities.

4.2. Different Data Protection Regimes Applicable to different Data Controllers

Interoperability will multiply the access points to the different systems in the Member States. While the intention to improve cooperation between the national authorities is certainly commendable, it is doubtful whether those authorities would be willing to share certain data in the systems if they cannot be sure who will have access. Consequently, instead of improving the work of competent authorities, Interoperability could lead to mistrust and negatively impact the information exchanges between those authorities.

The increased involvement of EU Agencies poses yet other data protection concerns, as discrepancies may arise in the con-

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) [2016] OJ L 119/1.

27 Directive (EU) 2016/680 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 [2016] OJ L 119/89.

text of interoperability where systematic data exchanges take place between actors that apply different data protection regimes. Against that background, concerns may arise where Europol staff is granted access to biometric data stored in EU databases and the interoperability components: Under the Europol Regulation, biometric data are not defined as special categories of data and may, therefore, be treated without the provision of additional safeguards.

In addition, the new EBCGA Regulation suggests strengthening the Agency with a new mandate and increased powers to protect the EU's external borders, to carry out returns more effectively, and to cooperate with third countries in the area of border protection. Moreover, the European Border Surveillance System (Eurosur), which will be integrated into the EBCGA under the new EBCGA Regulation, is mainly operated by national authorities that apply either the GDPR or the Directive (EU)2016/680 to their processing activities, while processing by the EBCGA falls within the scope of Regulation (EU)2018/1725.[28]

With Interoperability, the number and levels of authorities required to input information into the underlying systems multiply and the possibilities for a straightforward identification of the initial source will be obscured. This will make it more difficult to determine the authorities responsible for inputting the data that led to an incorrect result. Not only would this negatively affect the individual who might be wrongfully accused, but also obstruct his or her possibilities to complain against a decision that was based on inaccurate data (Demkova and Quintel, 2020).

4.3. Supervision and Effective Review of Processing Operations

Data processing activities within the AFSJ are rather opaque, which makes it difficult for data subjects to ascertain who is processing their personal data. Therefore, compliance with data pro-

28 Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance) [2018] OJ L 295/39.

tection principles, clearly defined processing purposes and strict supervision are of utmost importance to ensure fundamental rights standards. However, with the blurred lines between migration and security and the dilution of responsibilities between different data controllers, it will be challenging for DPAs to obtain a concrete picture of processing activities and the risks involved for data subjects.

The new layers that Interoperability adds to the already complex system of AFSJ databases make it extremely difficult to scrutinize the way in which data are collected, accessed and shared, and the new means to connect and link data within the Interoperability regime raise concerns regarding the review of processing operations.[29]

Supervisory authorities should be able to follow data flows across the different networks instead of looking at each specific controller separately. In order to achieve an effective supervision of the complex network of different processors, closer cooperation between national DPAs and the EDPS to better understand the steps behind certain decision-making processes and to handle complaints effectively is, therefore, essential, since any unfair processing can entail severe consequences for individuals.[30]

While on national level, access logs are to be kept for review by the national DPAs[31], on EU level, the processing of personal data by EU Agencies is supervised by the EDPS. In order to achieve full supervision, cooperation should be reinforced between the DPAs on different levels. Such coordinated supervision has been codified in the legal instruments of some of the underlying databases. Additionally, Article 62(1) of Regulation (EU)2018/1725 puts forward a harmonized model of coordinated supervision between the EDPS and the national DPAs to ensure an effective supervision of large-scale IT systems.[32]

29 Cf.: Ibid.

30 Ibid.

31 See: Article 25 of Directive (EU)2016/680.

32 See: EDPS, 'Supervision Coordination'; https://edps.europa.eu/data-protection/supervision-coordination_en. (accessed on 20 October 2019).

5. Conclusion

While the proponents of Interoperability portrayed it as some type of panacea for the existing shortcomings of information sharing in the AFSJ, several caveats in the anticipated regime simply cannot be ignored. One of the most pressing questions should be whether the interoperable system is necessary and proportionate, and whether Interoperability will lead to an improved exchange of information. Where additional actors will be authorized to access the system, this might have an impact on the trust among authorities, which might be reluctant to share information.

Moreover, there is no tangible proof that the broadened law enforcement access, which has been included in the amendments of the underlying databases during the past years and became a default feature for the CIR, will actually improve the work of competent authorities. While recent terrorist attacks are often used as an arguments to extend law enforcement access to EU databases and to support Interoperability, the failure to prevent such attacks derived mainly from the lack of coordination on national level and the absence of data sharing between Member States.

With Interoperability, designated police officers may access the underlying immigration databases via the CIR without checking their national databases beforehand. Moreover, the CIR search shall include a reference to all EU information systems to which the data belong. Hence, during an identity check, a police officer could, by inference, make erroneous conclusions about a person, simply because his or her personal data are stored in one of the underlying databases. Consequently, Articles 20 and 22 of the Interoperability Regulations increase the risk of situations where TCNs as well as EU citizens could become subject to unfair or discriminatory processing.

Ultimately, it remains to be seen whether Interoperability, once established, will indeed improve the scale of information sharing while ensuring effective oversight and safeguarding individuals' rights.

References

Demkova, S. and T. Quintel (2020), *Allocation of Responsibilities in Interoperable European Information Exchanges: Effective Judicial Control Compromised?* Cahiers Jean Monnet (forthcoming 2020).

Luyten, K. and S. Voronova (2019), 'Interoperability between EU border and security information systems', EPRS (June 2019), 2.

Quintel, T. (2018), 'Connecting personal data of Third Country Nationals Interoperability of EU databases in the light of the CJEU's case law on data retention' (March 2018). University of Luxembourg Law Working Paper No. 002-2018. Available at SSRN: https://ssrn.com/abstract=3132506.

Quintel, T. (2018), 'Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals', EDPL, 4(4): 470-482.

Quintel, T. (2019), The Impact of Interoperability on the processing of (Biometric) Data, KritV 4/2018, 27 (March 2019).

Sajfert, J. and T. Quintel (2019), 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities' in Mark Cole and Franziska Boehm (eds), GDPR Commentary (Edward Elgar Publishing 2019) available at SSRN https://ssrn.com/abstract=3285873 (accessed 16 October 2019).

Vavoula, N. (2020), 'Stepping up the Fight against Impunity in EU Law: Access to Immigration Databases by National Law Enforcement Authorities and Europol', in Luisa Marin and Stefano Montaldo (eds), The Fight against Impunity in EU Law (Hart forthcoming 2020).