Special Issue: Article

NJECL

New Journal of European Criminal Law
2019, Vol. 10(1) 34–43

DOI: 10.1177/2032284419837381
njecl.sagepub.com
SAGE

Data Protection and the EPPO

Paul De Hert
Vrije Universiteit Brussel, Belgium

Vagelis Papakonstantinou
Vrije Universiteit Brussel, Belgium

Abstract
The European Public Prosecutor's Office (the 'EPPO') necessarily processes personal data in order to fulfil its mission; As such, it falls squarely within the European Union (EU) data protection regulatory landscape. However, because the EU data protection regulatory landscape itself is currently found at a crossroads, an analysis of the EPPO data protection model may be twofold: First, placing it within the proper cross-organization dialogue currently taking place on the future regulatory model of personal data processing for law enforcement purposes carried out at EU level. Second, at an EPPO-specific level, whereby the actual data protection regime afforded to it may be assessed. This article purports to elaborate upon the above two data protection dimensions of EPPO personal data processing activities: It presents considerations and policy options during the lawmaking period that resulted in the establishment of the EPPO, it analyses the data protection regime ultimately awarded to it and attempts to, critically, place the EPPO data protection model within its proper operational and legislative environment.

Keywords
European Public Prosecutor's Office, EU data protection, regulation (EU) 2017/1939

Introduction

The European Public Prosecutor's Office (the 'EPPO') necessarily processes personal data in order to fulfil its mission. As per the tasks formally awarded to it, it

> shall be responsible for investigating, prosecuting and bringing to judgment the perpetrators of, and accomplices to, criminal offences affecting the financial interests of the Union [. . .]. In that respect the EPPO shall undertake investigations, and carry out acts of prosecution and exercise the functions

Corresponding author:
Paul De Hert, Vrije Universiteit Brussel, Pleinlaan 2, Brussel B-1050, Belgium.
E-mail: paul.de.hert@vub.be

> of prosecutor in the competent courts of the Member States, until the case has been finally disposed of.[1]

All of the above include personal data processing. As such, the EPPO falls squarely within the European Union (EU) data protection regulatory landscape.

Because the EU data protection regulatory landscape itself is currently found at crossroads, an analysis of the EPPO data protection model may be twofold: First, placing it within the proper cross-organization dialogue currently taking place on the future regulatory model of personal data processing for law enforcement purposes carried out at EU level. Second, at an EPPO-specific level, whereby the actual data protection regime afforded to it may be assessed. We believe that both perspectives are of critical importance. The first one may develop far reaching consequences, because the EPPO paradigm may be used as a case study for other EU agencies or bodies carrying similar missions as well. The second, because we believe that the EPPO's scope, while limited today, may be considerably extended in the not so distant future.

This article purports to elaborate upon the above two data protection dimensions of EPPO personal data processing activities. In order to do so, it will first present considerations and policy options during the lawmaking period that resulted in the establishment of the EPPO, before attempting to analyse the data protection regime ultimately awarded to it. Subsequently, it will briefly present the general EU data protection regulatory landscape for law enforcement organizations, so as to place the EPPO data protection model within its proper operational and legislative environment. Finally, the EPPO's relationship with Eurojust and OLAF, its two closest neighbouring organizations, will be discussed, prior to concluding with certain critical remarks on the EPPO data protection regime.

Brief background information from a data protection perspective: A tectonic shift during the lawmaking process

The EPPO-related background leading up to the current state of play, by mid-2018, is well known by now. Here, it will be only briefly discussed for picture-completeness purposes, and under a, biased, data protection, viewpoint. The discussion on establishing an EPPO was put forward in academic circles as early as in 1997.[2] Since the early 2000s, the Commission came on board this idea and started a number of initiatives that however met with no success.[3] Nevertheless, the Commission's initiative was vindicated through the Lisbon Treaty, whose Article 86 Treaty for the Functioning of the European Union (TFEU) states that 'in order to combat crimes affecting the financial interests of the Union, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor's Office from Eurojust'. Consequently, immediately after the ratification of the Lisbon Treaty in 2009, the EPPO project was put on track.

1. Article 4 of the Council Regulation (European Union) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office, OJ L 283, 31 October 2017, pp. 1–71 (the 'EPPO Regulation').
2. For a brief historical overview, see European Parliament, *Towards a European Public Prosecutor's Office, Study for the LIBE Committee*, 2016, p. 9 f.
3. See also European Parliament, *The future of Eurojust*, *Study for the LIBE Committee*, 2012, p. 125 f.

It was in this context that on 17 July 2013, the European Commission released a proposal for a Council Regulation on the establishment of the EPPO.[4] From a data protection point of view, the Commission wished, perhaps expectedly,[5] that a set of EPPO-specific provisions would 'particularise and complement the Union legislation applicable to processing of personal data by EU bodies (in particular Regulation (EC) No. 45/2001)'.[6] These provisions were included in chapter VI (Articles 37–47) of the Commission's proposal. As a general rule, however, it was explicitly set that 'Regulation (EC) No 45/2001 shall apply to the processing of personal data by the EPPO in the context of its activities. This Regulation particularizes and complements Regulation (EC) No 45/2001 in as far as operational personal data are concerned'.[7] Consequently, the data protection legal framework for all personal data processing of the EPPO was to be set mostly by Regulation 45/2001.[8] Accordingly, the task of supervision was to be entrusted to the European Data Protection Supervisor (EDPS).[9]

What followed the release of the Commission's proposal is, after all, outlined in the EPPO Regulation's preamble. Four years later, on 7 February 2017, the Council registered the absence of unanimity on the draft EPPO Regulation.[10] Subsequently, the process already prescribed in Article 86 TFEU was followed, whereby on 3 April 2017, 16 Member States notified that they wished to establish enhanced cooperation on the establishment of the EPPO. On 12 October 2017, the Regulation establishing the EPPO was adopted by those member states which are part of the EPPO enhanced cooperation (the 'EPPO Regulation').[11] Until then, 20 Member States had joined the enhanced cooperation.[12]

Nevertheless, from a data protection perspective, a tectonic shift had taken place in the meantime.[13] The original model proposed by the Commission was completely overturned and replaced by a totally different approach, whereby, in essence, Regulation 45/2001 would only apply to

4. Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, COM/2013/0534 final (the 'Commission's Proposal'); see also V. Alexandrova, 'Presentation of the Commission's Proposal on the Establishment of the European Public Prosecutor's Office', as well as M. Coninsx, 'The European Commission's Legislative Proposal: An Overview of its Main Characteristics', both in L.H. Erkelens, A.W.H. Meij and M. Pawlik, eds., *The European Public Prosecutor's Office* (The Hague: TMC Asser Press, 2015), p. 11 f. This proposal was released together with the Commission's proposal on Eurojust ('Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust)', COM/2013/0535 final).
5. This was, after all, the Commission's preferred data protection model also for Eurojust, under its draft proposal above (COM/2013/535final).
6. See Explanatory Memorandum of the Commission's Proposal, and also its Article 37(5).
7. Article 37(5) of the Commission's Proposal.
8. Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, J L 8, 12 January 2001, pp. 1–22. It should be noted that this Regulation is in the process of being amended – see the relevant Commission's proposal, COM (2017) 8 final, 10 January 2017.
9. See Article 41 of the Commission's Proposal.
10. See para (5). In the meantime, the Parliament had released a number of Reports (in 2014, A7-0141/2014, and in 2015, A8-0055/2015), respectively, as well as Resolutions (in 2014, P7_TA(2014)0234, in 2015, P8_TA(2015)0173, and in 2016, P8_TA(2016)0376) on this matter.
11. Council Regulation (European Union) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31 October 2017, pp. 1–71.
12. Press release, European Council, *20 Member States confirm the creation of an European Public Prosecutor's Office*, 12 October 2017.
13. While it is difficult for the exact origins of this shift to be identified, it seems that lawmaking work under the Council well took this option under consideration, see M.J. Alink and N.D.A. Franssen, 'EPPO – Developments Under the

EPPO administrative (personnel) processing,[14] while its operational processing would fall under a special data protection regime detailed in the EPPO Regulation itself.[15] The only thing that remained intact from the original Commission proposal was EDPS supervision.[16] While this is indeed not an insignificant win for the Commission, it should be noted that the EDPS will however need to apply this ad hoc EPPO regime when performing its tasks, and not Regulation 45/2001.

This is a very important policy change, which may carry broader consequences. Not only does it create an ad hoc, unique personal data protection regime for the EPPO, whose compliance with the individual right to data protection (as set in Article 16 TFEU) needs to be assessed, but it also may set the tone for things to come. As it will be seen, the EU data protection field for law enforcement processing is already found at crossroads, whereby a coherent legal architecture is sorely missing. By accentuating, and even furthering, this deficit, the data protection model that was ultimately awarded to the EPPO may develop consequences that go well beyond the strict EPPO internal boundaries.

The EPPO data protection regime: Impracticality and fragmentation in play?

Assessing the ad hoc data protection regime awarded to the EPPO, apart from being premature, largely exceeds the purposes and limits of this article. Here, it is only noted that the EPPO Regulation includes a self-sufficient system of data protection rules of a hybrid nature. While apparently substantial effort has been placed for them to resemble these of the Police and Criminal Justice Data Protection Directive[17] or even these of the General Data Protection Regulation,[18] at the same time they differ in important aspects, creating ultimately a unique data protection legal framework to the benefit of the EPPO only.[19] This ad hoc data protection regime is laid down in Article 2 of the EPPO Regulation, where the, customary, set of data protection definitions is found, as well as in its chapter VIII, Articles 47–89. Therein are laid down, together with all basic data protection provisions on the principles of processing, individual rights, supervision and data transfers, also such newcomers in the field as provisions on privacy by design and by default,[20] impact assessments,[21] or provisions on data breach notifications.[22]

Presidency of the Netherlands', in W. Geelhoed, L.H. Erkelens and A.W.H. Meij, eds., *Shifting Perspectives on the European Public Prosecutor's Office* (The Hague: TMC Asser Press, 2018), p. 23.

14. EPPO Regulation, Article 48(1).
15. See chapter VIII of the EPPO Regulation.
16. See Article 85 of the EPPO Regulation.
17. Directive (European Union) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4 May 2016, pp. 89–131.
18. Regulation (European Union) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016, pp. 1–88.
19. Article 47 of the EPPO Regulation, on the principles for personal data processing, constituting a typical example in this regard.
20. Article 67.
21. Article 71.
22. Articles 74 and 75.

This carefully set, self-sufficient data protection system was necessary in order to construct an ad hoc data protection regime for the EPPO. No longer do the provisions of the EPPO Regulation 'particularize and complement' another legal instrument (Regulation 45/2001 or its successor) as the Commission had originally envisaged. By now extensive copying–pasting and a 'stealing' of ideas is necessary in order to construct a standalone data protection edifice. Whether this edifice lives up to adequate data protection standards, as set in Article 16 TFEU and particularized in the horizontal-effect texts of the General Data Protection Regulation (GDPR), the Police and Criminal Justice Data Protection Directive and Regulation 45/2001 (or its successor), or whether anything went missing during the lawmaking process, merits special, academic and even Court of Justice of the European Union (CJEU), attention. Here it is enough to be noted that the EPPO data protection regime, being an independent and standalone system, needs to convince us of its data protection merits – or even adequacy, despite its obvious fragmented character.

However, all of the above refer only to data protection substantive law. Supervision is a totally different matter. In essence, this task is to be carried out by the EDPS:

> The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation relating to the protection of fundamental rights and freedoms of natural persons with regard to processing of operational personal data by the EPPO, and for advising the EPPO and data subjects on all matters concerning the processing of operational personal data.[23]

This is an important concession to the EU establishment by Member States, who were generally concerned during the lawmaking process about the EPPO impeding the work of their national prosecutors. Even so, however, the EDPS will have to follow the EPPO terms of reference, and not its own:

> To this end, the European Data Protection Supervisor shall fulfil the duties set out in paragraph 2 of this Article, shall exercise the powers granted in paragraph 3 of this Article and shall cooperate with the national supervisory authorities in accordance with Article 87.

Consequently, the EDPS is expected to monitor the EPPO personal data processing not according to the rules of Regulation 45/2001, but according to the EPPO special data protection regime. While this is indeed not a unique situation among EU agencies, it is a far from welcome one for data protection aims and purposes, as it will be explained in the analysis that immediately follows. Here, merely the impracticality of the applicable legal mechanism needs to be noted, whereby a single organization, the EDPS, is expected each time to assume a chameleon-like role and apply different data protection rules while supervising different EU agencies and bodies.

The EU data protection landscape found at crossroads leading either to comprehensiveness or incoherence

The data protection policy option made in the EPPO Regulation, as described earlier, comes at a critical point for the EU data protection model. After the ratification of the Lisbon Treaty, that after all enabled establishment of the EPPO, data protection lawmaking has picked-up speed substantially. Evidently, efforts focused on the 2012-released EU data protection reform package that led

23. Article 85(1).

to the GDPR and the Police and Criminal Justice Data Protection Directive. However, work was by no means restricted in these two instruments only. On the contrary, the Commission embarked on an ambitious project to overhaul all of EU data protection. In this context, the Passenger Name Record Directive was also released around the same period[24]; the Europol Regulation was introduced[25]; the Eurojust Regulation as well, despite of the fact that it still remains in draft[26]; the successor to Regulation 45/2001 was released on 10 January 2017[27]; significant work also took place with regard to OLAF,[28] Frontex[29] and other EU agencies and bodies; and, of course, the EPPO Regulation also came into effect during the same period.

The above, non-exhaustive, list serves to indicate the astonishing width and breadth of law-making work carried out these days. All of the above instruments deal with data protection, either incidentally or at their core. Collectively, they formulate the new EU data protection edifice. Whether such edifice has any coherent structure or architecture is debatable.[30] Too many actors and too many instruments antagonize for attention and specificity, ultimately constructing a competing and overlapping legal construction, where one has to tread carefully and make delicate distinctions in order to successfully navigate it.

A basic distinction needs to be made between personal data processing at EU and at Member State level. Different rules apply to each one. As regards Member States, the GDPR and the Police and Criminal Justice Data Protection Directive set the rules within their respective subject-matter; supervision is awarded to national Data Protection Authorities. At EU level, things are not as straightforward. In principle, Regulation 45/2001, or its successor, finds horizontal effect on all personal data processing by EU agencies and bodies; supervision tasks are to be carried out by the EDPS. However, this is by no means a universally applicable regulatory model. In fact, three models stem from it. The first one refers to EU bodies and agencies indeed applying directly Regulation 45/2001 onto their personal data processing. The second involves these EU agencies or bodies that carry substantive data protection rules in their respective constituting documents, that 'particularize and complement' the

24. Directive (European Union) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4 May 2016, pp. 132–149.
25. Regulation (European Union (EU)) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the EU Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24 May 2016, pp. 53–114.
26. See Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust), COM/2013/0535 final.
27. See Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No. 1247/2002/EC, COM/2017/08 final.
28. See Regulation No. 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No. 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No. 1074/1999, OJ L 248, 18 September 2013, pp. 1–22.
29. See Regulation (European Union (EU)) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No. 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No. 2007/2004 and Council Decision 2005/267/EC, OJ L 251, 16 September 2016, pp. 1–76.
30. See also the European Parliament, LIBE Committee study on '*The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area*', 2014.

provisions of Regulation 45/2001. Finally, the third model promotes EU organizations' data protection exceptionalism. As is notoriously the case of Europol (now to be followed also by the EPPO), an EU agency or a body has its own, ad hoc and standalone, data protection regime. With regard to supervision, while it is by now universally awarded to the EDPS, one has to be careful to note that the EDPS has to carry out its tasks not applying the Regulation 45/2001 rules, but the rules applicable to each agency and body under the above distinctions. These rules not only differ from those of Regulation 45/2001, but they also award the EDPS different supervisory powers each time.

As if the above regulatory model at EU level was not complicated enough, one has to keep in mind that particularly EU law enforcement agencies and bodies are based for performance of their work on personal data processing done at Member State level, by national (police and other law enforcement) agencies.[31] This processing, evidently, falls under the rules of the Police and Criminal Justice Data Protection Directive and national Data Protection Authority (DPA) supervision. Once however uploaded on an EU server, the same personal data fall under the respective agency's or body's data protection regime and EDPS supervision as per the above clarifications. For all these cases of personal data processing, which obviously constitute the norm given EU structure, a 'coordinated supervision' model has been devised between national DPAs and the EDPS.[32] This model, apart from being in theory the only conceivable way out of this regulatory mess, has yet to prove its data protection worth, particularly under the post-Lisbon environment.

It is in view of the above that we believe the EPPO data protection example to be a counterproductive one for the data protection purposes. Rather than contributing to coherence, by at least falling under the category of EU agencies and bodies that apply Regulation 45/2001 with a few specific extra provisions, it chose to introduce a new data protection system by itself. While in the EU law enforcement field it was only Europol that followed that path, and has been repeatedly criticized for a low data protection level afforded by it,[33] now the EPPO is added to the list, creating a negative precedent, that could even develop a spillover effect and infest also the data protection regime of Eurojust, as it will be seen in the analysis in the following.

The EPPO relationship with Eurojust and OLAF: Is operational separation even possible from a data protection perspective?

The wording of Article 86 TFEU that the EPPO is to be created 'from Eurojust' originally left a wide spectrum of theoretical and practical speculation. In principle, the relationship between the

31. See also European Parliament, *Towards a European Public Prosecutor's Office*, p. 20 f; C. Deboyser, 'European Public Prosecutor's Office and Eurojust: Love Match or Arranged Marriage?', in L.H. Erkelens, A.W.H. Meij and M. Oawlik, eds., *The European Public Prosecutor's Office*, p. 79 f; A. Weyembergh and C. Brière, 'Relations Between the EPPO and Eurojust – Still a Privileged Partnership?', in W. Geelhoed, L.H. Erkelens and A.W.H. Meij, eds., *Shifting Perspectives on the European Public Prosecutor's Office* (The Hague: TMC Asser Press, 2018), p. 171 f.
32. Naming from the European Data Protection Supervisor (EDPS) annual reports, see for instance the EDPS annual report for the year 2013, *2013 – A single set of rules for all: EU Data Protection Reform can support businesses and protect citizens*, chapter 4.2.
33. See F. Boehm, *Information Sharing and Data Protection In the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange At EU level* (Berlin: Springer, 2012), p. 177 f; S. Puntscher Riekmann, *'Security, Freedom and Accountability: Europol and Frontex'*, in F Geyer, ed., *Security versus Justice? Police and Judicial Cooperation in the European Union* (Routledge, London, 2008); G. Fuster Gonzalez and P. Paepe, 'Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects', in F Geyer, ed., *Security versus Justice? Police and Judicial Cooperation in the European Union* (Routledge, London, 2008).

two EU agencies could have taken any one of four types: Eurojust became the EPPO, the EPPO became part of Eurojust, two separate entities were established or the EPPO and Eurojust were merged.[34] As seen, the model finally implemented is that of 'a close relationship based on mutual cooperation within their respective mandates'[35] of two otherwise separate entities. This separatist approach is reflected in the EPPO Regulation provisions describing the relationship between the two.[36] The exact same wording, and therefore the exact same approach, is adopted on OLAF as well.[37]

In essence, operational separation ultimately refers to each organization's case management system. Is this to be independent and wholly-owned, or is, for example, the EPPO to share the system of Eurojust? The initial proposal of the Commission tended towards the EPPO not having an independent case management system, but rather it being dependent on that of Eurojust, working with temporary files and an index.[38] The EPPO Regulation decided otherwise: The EPPO is to have an independent system after all.[39] Consequently, its exact relationship with neighbouring case management systems (in essence, these of Eurojust and OLAF) needs to be clearly delineated.

From a data protection point of view, the relationship between the case management systems of the EPPO, Eurojust and OLAF inevitably means the sharing of personal data among them. In principle, a cautious approach has been adopted in this regard. In the case of Eurojust, the EPPO may 'share information, including personal data' in operational matters, whereby it may 'associate Eurojust with its activities concerning cross-border cases'.[40] The other way around, Eurojust transmitting personal data to the EPPO, has been placed under a strict 'hit/no hit' filter:

> The EPPO shall have indirect access to information in Eurojust's case management system on the basis of a hit/no-hit system. Whenever a match is found between data entered into the case management system by the EPPO and data held by Eurojust, the fact that there is a match shall be communicated to both Eurojust and the EPPO, as well as the Member State of the European Union which provided the data to Eurojust. The EPPO shall take appropriate measures to enable Eurojust to have access to information in its case management system on the basis of a hit/no-hit system.[41]

The exact same solution has been applied with regard to OLAF too.[42]

Despite this theoretical exercise on case management system separation, the fact remains that personal data are indeed expected to flow between the above EU organizations at an increased volume. However, whenever this takes place, there will be no coherent data protection regime in place to govern them. One can easily imagine a single personal data file first being assembled at Member State level, thus under the Police and Criminal Justice Data Protection Directive,

34. Policy options outlined in European Parliament, *The future of Eurojust, Study for the LIBE Committee*, 2012.
35. See Preamble, para 10.
36. See Article 3(3) and 100.
37. See Article 101. With regard to both Eurojust and OLAF relationships, see also the relevant analysis in European Parliament, Towards a European Public Prosecutor's Office, p. 40 f.
38. See para 44 of the Preamble, Article 22, as well as para 1.5.4 of the Explanatory Memorandum of the Commission Proposal.
39. See para 47 of the Preamble, Article 44, as well as Article 45(1) ('The internal rules of procedure of the EPPO may include rules on the organization and management of the case files to the extent necessary to ensure the functioning of the EPPO as a single office') of the EPPO Regulation.
40. Article 100(2) and also para 102 of the Preamble.
41. Article 100(3).
42. See Article 101(4)(5), respectively, as well as para 105 of the Preamble.

subsequently stored at Eurojust servers, thus most likely applying Regulation 45/2001, and then being transmitted also to the EPPO, where its ad hoc data protection regime becomes applicable. Overall, three data protection regimes to be applied consecutively over the same file. Even mapping which provisions apply which time would be difficult – exercising any meaningful supervision over such a personal data processing would be a formidable task indeed, one that some people may find hard to believe.

Concluding remarks: An epic fail for EU data protection?

Establishment of the EPPO is an exercise on legal complexity. Even within its current limited, financial crime-related scope, the EPPO has to address the legal difficulties of establishing itself and cooperating with Member States, reassuring them that the work of their national prosecutors will not be impeded, while also working together closely with Eurojust and OLAF, its neighbouring EU agencies, in terms of mission statement. Particularly, its relationship with Eurojust will be an open issue. As early as in 2012, the European Parliament identified challenges brought by the EPPO coming into life – back then, still only an eventuality.[43] However, even at that time it was foreseeable that the enhanced cooperation model would most likely be the way forward, as well as that, 'from the moment of its potential establishment, the EPPO will add a degree of complexity to the current way judicial cooperation in criminal matters is administered'.[44] If the EPPO ever acquires scope expansion to cover other crimes as well, difficulties shall only accentuate.

As if putting this legal model to work was not a difficult enough task, when it comes to the EPPO data protection model, difficulties increase exponentially. This is because EU data protection is still at crossroads itself. Namely, the legal architecture of data protection at EU level is yet to be decided. While at Member State level the recent EU data protection reform package has created a comprehensive and coherent structure (the Police and Criminal Justice Data Protection Directive for law enforcement processing and the GDPR for all else), this is not the case at EU level. There, Regulation 45/2001, currently under replacement process, that would supposedly constitute the standard-setting text still has to fulfil its mission. In practice, only rarely does it apply as such on processing of EU law enforcement organizations. The majority among them benefits from own substantive legal provisions, inserted in its constituting legal text, that 'particularize and complement' these of Regulation 45/2001. A third category has been represented, until now, by Europol alone: Europol insisted, and eventually won, to be granted its own, ad hoc, data protection regime, different to any of the above.

For the moment, the decisive vote will be cast by Eurojust. The Commission has released its proposal since 2013 on amending its constituting text – but it has not been finalized yet, after more than 5 years since its release. With regard to data protection, the Commission opted for direct application of the Regulation 45/2001 provisions.[45] The Eurojust establishment bitterly contested this policy option.[46] Europol, who finally succeeded in breaking the link of all EU law enforcement personal data processing with Regulation 45/2001, constitutes a most relevant precedent in this regard. However, until recently it was a unique case, alone in being awarded its ad hoc data protection regime.

43. See European Parliament, *The future of Eurojust, Study for the LIBE Committee*, 2012.
44. See European Parliament, *The future of Eurojust, Study for the LIBE Committee*, 2012, p. 141.
45. See Article 27(5) of the relevant Commission's proposal.
46. See Eurojust JSB critical position in '*Opinion of the Joint Supervisory Body of Eurojust regarding data protection in the proposed new Eurojust legal framework*', 14 November 2013.

It is against this background that the EPPO data protection model needs to be placed. By siding with Europol's data protection uniqueness, it tilts the balance towards EU organization's data protection exceptionalism. By now, it is no longer one but two EU law enforcement organizations that have their own data protection regime. While the majority continues to be regulated by Regulation 45/2001, either directly or as 'particularized and complemented' by their own data protection provisions, it is clear that they all keep an open eye on regulatory developments. If the link with Regulation 45/2001 is broken, when it comes to EU personal data processing for law enforcement purposes, then they too may wish to benefit from a data protection model of their own. After the EPPO example, the argument of uniformity, whenever put forward by the Commission, would be a hard one to accept.

Why is the data protection exceptionalism advocated by many, if not all, EU law enforcement organizations a bad thing for the data protection purposes? We believe that this is substantiated upon two grounds. First, from a data subjects' perspective, any meaningful protection of its rights would involve identification and assembly of a number of different legal provisions at Member State and EU level. The expert legal work required would be time-consuming and expensive, making it thus inaccessible to the majority of individuals across the EU. Second, from a supervision perspective, we find it hard to believe that the EDPS (or any agency for these purposes) has the resources and the ability to exercise its monitoring powers effectively while having to apply simultaneously at least a dozen different legal regimes, one per each organization concerned, each carrying its own substantive data protection regime and each awarding the EDPS with different supervisory powers. Consequently, while fragmentation itself is not prohibited by Article 16 TFEU, we believe that the effective data protection that it mandates necessarily includes a possibly uniform and coherent applicable legal framework.

Data protection politics aside, an assessment of the actual EPPO data protection provisions is premature. As seen, their wording differentiates them from the relevant provisions of Regulation 45/2001 or the Police and Criminal Justice Data Protection Directive, which constitute the standards in the field at the moment. Whether the level of data protection awarded by them will be above or below Article 16 TFEU standards remains to be seen, when they are put to practice. Points of attention are expected to refer particularly to intra-EU agency personal data transmissions, particularly among the EPPO, Eurojust and OLAF.

We believe that it is important for the above difficulties to be addressed. While the EPPO is established today with a relatively restricted scope, we think that this will not continue to be the case in the, not so distant, future. The procedure for scope expansion is already prescribed in Article 86 TFEU. The Member States that formulated the EPPO enhanced cooperation have demonstrated their resolve to push forward, leaving reluctant partners behind. There is no reason why this will not continue to be the case, particularly if the EPPO demonstrates its effectiveness in practice. From a data protection perspective, any scope expansion means an increased level of personal data processing and exchanges, accentuating thus even further the aforementioned, already visible, data protection difficulties.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.