EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

12 April 2021

Report

Interpretation of the EPPO Regulation in view of EPPO's supervision by the EDPS

edps.europa.eu

Disclaimer: The information and views set out in this study are those of the author(s) and do not necessarily reflect the official opinion of the EDPS. The EDPS does not guarantee the accuracy of the data included in this study. Neither the EDPS nor any person acting on his behalf may be held responsible for the use that may be made of the information contained herein. This Final report reflects the legal situation as of 9 April 2021.

Interpretation of the EPPO Regulation in view of EPPO's supervision by the EDPS

Final report[1]

Vanessa Franssen and Marine Corhay[2]

[1] *The final report of this study was finalised and submitted on 9 April 2021. This version of the report was preceded by two draft versions: the first one was handed in on 3 December 2020, the second one on 31 January 2021. The authors are grateful to the EDPS for its insightful feedback on the earlier versions of this report.*

[2] *Vanessa Franssen is Professor at the University of Liège and Affiliated Senior Researcher at the KU Leuven (Belgium); Marine Corhay is PhD Candidate at the University of Liège and FRESH Scholar of the F.R.S-FNRS. The authors would like to thank Anne Werding, assistant at the University of Liège, for her help with the legal analysis of sources in German.*

Contents

1. Introduction

1.1. Subject and scope of the research

This study **aims to delineate the supervisory role of the EDPS with respect to the European Public Prosecutor's Office** (hereinafter: EPPO) **and to analyse some practical consequences of the different possible approaches**.

While the EPPO is a body of the European Union (hereinafter: EU or Union), it is unique in its hybrid structure as it consists of a central office, located in Luxembourg, and decentralized offices at Member State level. Its operational functioning will involve actors at both levels. At decentralized level, the European Delegated Prosecutors (hereinafter: EDPs) play a pivotal role: while they act on behalf of, and clearly belong to the EPPO, they are also part of the national public prosecutor's office and endowed with the same powers as national prosecutors. Inherent to the functioning of the EPPO is its cooperation with national authorities on which the EDPs will rely heavily to conduct and/or authorize investigation measures. While the exchange of information with EU authorities is largely regulated by the Regulation establishing the European Public Prosecutor's Office[3] (hereinafter: EPPO Regulation or Regulation),[4] the cooperation with national authorities is mainly left to national law (with some punctual exceptions, which will be discussed in later parts of this report).

Considering the involvement of multiple actors in future EPPO investigations, the **processing** of **data** will inevitably take place at **different levels**, raising key questions regarding the applicable data protection regime and the competence of supervisory authorities. These questions, most of which have not yet received much attention (in legal literature and elsewhere), will prove to be **essential** for the smooth functioning and supervision of the EPPO's operational activities in terms of data protection.

---

[3] *Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), O.J., L 283, 31 October 2017, p. 1.*

[4] *See Articles 43(2), 49(1)(b), 54, and 99(2) of the EPPO Regulation. These general rules can be further specified in working arrangements between the EPPO and the EU authorities, as provided by Article 99(3) of the Regulation. In the meantime, two working arrangements have been adopted, with Europol and Eurojust. These working arrangements also address various data protection related issues; a detailed analysis of these working arrangements is, however, beyond the scope of this study. See EPPO, Europol and EPPO establish working relationship, press release, 21 January 2021, available at: https://www.eppo.europa.eu/press-releases/europol-and-eppo-establish-working-relationship; EPPO, Eurojust and EPPO sign Working Arrangement to facilitate cooperation, press release, 15 February 2021, available at: https://www.eppo.europa.eu/press-releases/eurojust-and-eppo-sign-working-arrangement-facilitate-cooperation. The text of the working arrangement with Europol is available at: https://www.eppo.europa.eu/sites/default/files/2021-01/EPPO%20_Europol_Working_Arrangement.pdf. The text of the working arrangement with Eurojust is available at: https://www.eppo.europa.eu/sites/default/files/2021-02/Working-Arrangement-Eurojust-EPPO.pdf.*

In particular, this study will focus on the **following questions**:

- What is the scope of application of the data protection regime laid down in the EPPO Regulation? How does this regime relate to the rules defined by Regulation (EU) 2018/1725,[5] Directive (EU) 2016/680 (hereinafter: LED)[6] and the national laws? The latter obviously includes legislation that implements the LED, but also other legislation having a direct impact on data protection in the context of criminal investigations. (**Part III**)
- What are the EPPO's powers and tasks regarding the processing of personal data? (**Part IV**)
- What is the theoretical interplay between the data protection rules of the EPPO Regulation and national legislation? In this respect, the study will primarily examine the following three areas: 1. Data subjects' rights (including limitations and restriction of these rights); 2. the processing of special categories of operational personal data; 3. transfers of operational personal data. (**Part V)**
- What is the concrete interplay between the data protection rules of the EPPO Regulation and national legislation? What is the responsibility of the EPPO and Member State authorities respectively with regard to the processing of personal data in the context of the EPPO's activities? Which law applies to this processing? (**Part VI**)
- Finally, what are the repercussions of the above on the EDPS's supervisory role with respect to the EPPO and to what extent is coordination with national supervisory authorities required? (**Part VII**)

Before addressing these questions, the study will briefly highlight some distinctive features of the EPPO that are relevant for the subsequent analysis (**Part II**).

---

[5] *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, O.J., L 295, 21 November 2018, p. 39 (hereafter: Regulation (EU) 2018/1725).*

[6] *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, O.J., L 119, 4 May 2016, p. 89.*

1.2. Research methodology

The research conducted for this study is based on a **three-pronged methodology** consisting of desk research, comparative research with surveys, and semi-directive interviews.

The desk research involved the analysis of legislative documents, parliamentary and other preparatory documents, policy studies and reports, and relevant legal literature. This documentary analysis was supplemented by semi-directive interviews with (EU and national) policymakers, public officials and practitioners which, due to the continuing COVID-19 pandemic, were conducted via videoconference or via phone.[7]

Third, the researchers also contacted academic experts and practitioners[8] in a selection of Member States, both to facilitate the access to national legislative documents and scholarly literature, and to better understand the functioning of these national systems. Particular attention went to the implementation of the LED and the preparation of the respective national legal systems to the EPPO becoming operational. These contacts were largely based on surveys (questionnaires). The selection entailed the following Member States (in alphabetical order): Belgium, Estonia, France, Germany, the Netherlands, Romania and Spain. These Member States were selected among the 22 participating Member States on the basis of a combination of the following criteria: their role in the perception of EU custom duties, the amount of EU subsidies they receive, the (perceived) problem of corruption, geographical and legal diversity. Additionally, one may note that some of the selected Member States were part of the initiative to establish the EPPO via enhanced cooperation early on, while others joined at a much later stage.

It should be noted that this research, which was launched on 1st July 2020, was conducted at a **crucial point in time**.

---

[7] *A full list of the conducted interviews is given in Annex 3.*

[8] *In addition to all interviewees, our special gratitude goes to: Prof. Sabela Oubiña Barbolla (Universidad Autónoma, Madrid), Prof. Lorena Bachmaier Winter (Universidad Complutense, Madrid), Prof. Agata Sanz Hermida (Universidad de Castilla La Mancha), Prof. Juan Carlos Ortiz Pradillo (Universidad Complutense, Madrid), Prof. Daniel Nitu (Babes-Bolya University, Romania), Dr Georges Zlati (practicing lawyer, Romania), Prof. Daniel-Mihail Sandru (University of Bucharest, Romania), Prof. John Vervaele (Utrecht University), Dr Maxime Lassalle (Université Paris Nanterre/Max Planck Institut zur Erforschung von Kriminalität, Sicherheit und Recht, Freiburg), Dr Agnes Kasper (Tallinn University of Technology), Dr Eneli Laurits (Public prosecutor Estonia), Dr Anna-Maria Osula (Tallinn University of Technology), Dr Dominik Brodowski (Universität des Saarlandes), Dr Garonne Bezjak (German Ministry of Justice), Juraj Sajfert (Vrije Universiteit Brussel), Erwin Dernicourt (General Public Prosecutor Ghent, Belgium), Patrick Vandenbruwaene (General Public Prosecutor Antwerp, Belgium). Any errors in the analysis of these national systems are the sole responsibility of the authors of this study.*

At EU level, the European Prosecutors, forming together with the European Chief Prosecutor the EPPO College, were appointed on 27 July 2020,[9] and after its official inauguration at the Court of Justice on 28 September 2020,[10] the EPPO College adopted a first series of decisions, including its Internal Rules of Procedure (hereinafter: IRP)[11] and rules concerning the processing of personal data (hereinafter: DP Rules),[12] which are important elements of the legal jigsaw puzzle as they give body to the EPPO Regulation and indicate how certain provisions of the Regulation are interpreted by the EPPO. Together, these legal instruments set the scene for the first EPPO investigations[13] and will thus contribute to forging this new EU body's practice.

In addition to these EU developments, **at national level**, most Member States were still in the process of adjusting their legal system to the EPPO. Whereas Germany had already adopted legislation to this end when this study started, the other Member States legislated in the course of this study: France published its new legislation on 26 December 2020,[14] Estonia on 29 December 2020,[15] Romania on 18 February 2021,[16] Belgium on 24 February 2021[17] and the Netherlands on 31 March 2021.[18] At the moment of finalizing this report, only Spain is still in the process of preparing legislative amendments.[19] As a result, there are still quite some uncertainties as to how exactly the EPPO will function at national level as these national legislations have only just entered into force.[20] Moreover, apart from Germany, none of the Member States seems to have reflected on data protection issues when adjusting their legislation in view of the EPPO Regulation. This as such is

---

[9] *Council Implementing Decision (EU) 2020/1117 of 27 July 2020 appointing the European Prosecutors of the European Public Prosecutor's Office, O.J., L 244, 29 July 2020, p. 18.*
[10] *Court of Justice of the EU, "Inauguration of the European Public Prosecutor's Office", Press release No 118/20, 28 September 2020.*
[11] *Internal Rules of Procedure of the European Public Prosecutor's Office, College Decision 003/2020, 12 October 2020, O.J., C 22, 21 January 2021, p. 3.*
[12] *Rules concerning the processing of personal data by the European Public Prosecutor's Office, College Decision 009/2020, 28 October 2020.*
[13] *According to the most recent information, the EPPO would start its operational activities on 1 June 2021. See EPPO, Start date of EPPO operations: European Chief Prosecutor proposes 1 June 2021 to the European Commission, 7 April 2021, https://www.eppo.europa.eu/news/start-date-eppo-operations-european-chief-prosecutor-proposes-1-june-2021-european-commission.*
[14] *French Act on the EPPO, Journal Officiel de la République Française, No 0312, 26 December 2020.*
[15] *Estonian Act on the EPPO, RT I, 29 December 2020, p. 1.*
[16] *Romanian Act on the EPPO, Monitorul Oficial, Part I, No 167, 18 February 2021.*
[17] *Belgian Act on the EPPO, Moniteur Belge, 24 February 2021.*
[18] *Dutch Act on the EPPO, Staatsblad van het Koninkrijk der Nederlanden, No 155, 31 March 2021.*
[19] *The Draft Bill on the EPPO has recently been published and is available at: http://leyprocesal.com/leyprocesal/dm/anteproyecto-de-ley-organica-por-la-que-se-adapta-el-ordenamiento-nacional-al-reglamento-ue-20171939.asp?cod=7792&nombre=7792&nodo=&sesion=1. For a recent analysis of the internal Spanish discussions, see Europa Press, "El CGPJ advierte de las dificultades de adaptar la Fiscalía Europea en España con la actual LECrim", 25 March 2021, https://www.europapress.es/nacional/noticia-cgpj-advierte-dificultades-adaptar-fiscalia-europea-espana-actual-lecrim-20210325174740.html.*
[20] *It should be noted, though, that the Dutch Act on the EPPO has not yet entered into force. Pursuant to Article VIII of this Act, the date of entry into force will be determined by a future Royal Decree.*

an important finding and suggests that many issues will only be addressed and clarified along the way, as the EPPO develops its operational activities.

Furthermore, as regards the **implementation of the LED** into national law, it should be pointed out that some Member States[21] have not yet adopted the necessary legislation. In particular Spain has not adopted any implementing legislation so far.[22] Others may not have implemented the LED fully or entirely correctly (e.g. Belgium and Romania). The European Commission will evaluate the LED (and the Member States' implementation of this Directive) by 6 May 2022.[23] A first preparatory study to this end has been commissioned, but the results thereof have not yet published at the moment of finalizing this research.

Therefore, the findings of this study are inevitably based on partial, incomplete information. The reader should be aware that the practical implementation of the EPPO at (EU and) national level in the months and years to come are likely to impact the answers given to aforementioned research questions. Nevertheless, the questions addressed by this study will remain highly relevant and definitely require further attention of all involved actors.

---

[21] Shortly after the expiry of the deadline for transposition, the European Commission initiated infringement proceedings (Article 258 TFEU) against several Member States (e.g. Poland, Romania, the Netherlands, Estonia), most of which have now transposed the LED, except for Germany, Slovenia and Spain. The European Commission sent a reasoned opinion to Germany on 14 May 2020 for failure to completely transpose the Directive. See https://ec.europa.eu/commission/presscorner/detail/EN/INF_20_859. As for Slovenia, the European Commission sent a reasoned opinion on 24 January 2019 and an additional reasoned opinion on 14 May 2020. On 3 December 2020, the European Commission referred the case of Slovenia to the Court of Justice of the EU for failure to communicate measures that fully transpose the provisions of the Directive.

[22] The European Commission referred the case of Spain to the Court of Justice of the EU on 4 September 2019 (Case C-658/19). On 25 February 2021, the Court of Justice ordered Spain to pay a lump sum of € 15 million and a daily penalty of € 89,000 for failing to transpose or communicate transposition measures. See CJEU, C-658/19, Commission v Spain, 25 February 2021, ECLI:EU:C:2021:138. According to recent press articles, the Council of Ministers has approved the Bill implementing the LED, but the full text of this bill has, to our knowledge, not yet been published. See e.g. ElDerecho, "Proyecto de Ley Orgánica de Protección de Datos Personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales", 10 February 2021, https://elderecho.com/proyecto-de-ley-organica-de-proteccion-de-datos-personales-tratados-para-fines-de-prevencion-deteccion-investigacion-y-enjuiciamiento-de-infracciones-penales-y-de-ejecucion-de-sanciones-penales.

[23] Article 62(1) of the LED.

2. THE EPPO as a new hybrid judicial actor

2.1. A unique EU body

The EPPO Regulation was adopted via the procedure of enhanced cooperation, as provided by Article 86(1) of the Treaty on the Functioning of the European Union (hereinafter: TFEU), involving 22 Member States.[24] The EPPO is the first (and thus revolutionary)[25] EU body with the power to conduct criminal investigations and to act directly as a prosecuting authority before national criminal courts.

The EPPO is a unique institution. Its creation stems from the perception that, despite the support of OLAF and Eurojust, Member States do not do enough to combat fraud affecting the financial interests of the EU, either because they lack the will to do so or because they are unable to do so.[26] On the one hand, the EPPO is therefore emerging from a feeling of distrust towards Member States. On the other hand, EU law has always been conceived as a single and indivisible legal order which is characterised by the fact that it is, directly or indirectly, part of the law of the Member States and by the fact that the national public and judicial authorities are the usual enforcement authorities of EU law.[27] Sincere cooperation between Member States and EU institutions is a reciprocal obligation.[28] Besides, pursuant to Article 325 of the TFEU, combatting fraud against the financial interests of the EU is a shared competence; Member States shall coordinate their action

---

[24] *The following Member States are participating in the EPPO:* Member States have joined the enhanced cooperation: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Germany, Greece, Spain Finland, France, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Portugal, Romania, Slovenia and Slovakia. OLAF, European Public Prosecutor's Office https://ec.europa.eu/anti-fraud/policy/european_public_prosecutor_en.

[25] *D. Flore, "Le parquet européen à la croisée des chemins", in S. Dewulf (ed.), La [CVDW]. Liber Amicorum Chris Van den Wyngaert, Maklu, 2017, p. 238.*

[26] *Several academic and institutional studies show that the fight against EU fraud has not always been treated as a priority by national authorities (for instance, due to a lack of resources, structural deficiencies, or because of other crime policy choices). See e.g. M. Wade, Euroneeds Report, Freiburg, Max Planck Institute, 2011, https://www.mpicc.de/media/filer_public/c6/d8/c6d81682-2c98-4e15-bda8-c36621e4c6f7/euroneeds_report_jan_2011.pdf; OLAF, The OLAF Report 2017, Luxembourg, Publications Office of the European Union, 2018, https://ec.europa.eu/anti-fraud/sites/antifraud/files/olaf_report_2017_en.pdf ; M.-A. Santos, "The Status of Independence of the European Public Prosecutor's Office and Its Guarantees", in L. Bachmaier Winter (ed.), The European Public Prosecutor's Office: The Challenges Ahead, Springer, 2018, p. 3; H. Aden et alii, The European Prosecutor's Office: strategies for coping with complexity, Study requested by the CONT Committee of the European Parliament, 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/621806/IPOL_STU(2019)621806_EN.pdf, p. 19. Previously, the lack of enforcement by national competent authorities was also identified as one of the main problems that justified the intervention of the EU legislator. See European Commission, Commission staff working document – Impact assessment accompanying the Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, SWD(2013) 274 final, Brussels, 17 July 2013, p. 11-17.*

[27] *See e.g. CJEU, C-26/62, Van Gend et Loos, 5 February1963, ECLI:EU:C:1963:1; CJEU, C-6/64, Costa/E.N.E.L., 15 July 1964, ECLI:EU:C:1964:66; CJEU, Simmenthal, C-106/77, 9 March 1978, ECLI:EU:C:1978:49; CJEU, Factortame Ltd. e.a., C-213/89, 19 June 1990, ECLI:EU:C:1990:257; K. Lenaerts and P. Van Nuffel, Europees recht, Intersentia, 2017, p. 15.*

[28] *Article 4(3) of the EU Treaty.*

aimed at protecting such interests in an equivalent manner, and cooperate with the European Commission.

It is therefore not so surprising that the structure of the EPPO as agreed upon in the Regulation is a **delicate compromise** between, on the one hand, a highly independent and autonomous EPPO and, on the other hand, an EU body that is as much as possible integrated into the law enforcement system of each Member State.[29] The **tensions** resulting from this compromise are visible in every aspect of the functioning of the EPPO, including when it comes to data protection, and in the delicate and sometimes ill-defined relationship between EU and national law in the EPPO Regulation, as will be illustrated below.

2.2. A hybrid structure and functioning

The political context outlined above has, indeed, left its mark on the structure of the EPPO, according to some authors even raising fundamental questions about the effectiveness of future investigations by the EPPO.[30] The EPPO is conceived as 'an indivisible Union body operating as one single Office with a decentralised structure'.[31] It is organized at a double level, with a central level in Luxembourg and decentralised offices at national level.[32]

The College, Permanent Chambers, European Chief Prosecutor (hereinafter: ECP), Deputy European Chief Prosecutors (hereinafter: DECPs), European Prosecutors (one per participating Member State; hereinafter: EPs) and the Administrative Director will exercise their functions from the seat of the EPPO in Luxembourg.[33] The **central office** shall take decisions on strategic matters and be responsible for the general oversight of the activities of the EPPO.[34] It shall monitor, direct and supervise the EPPO's investigations and prosecutions.[35]

In contrast, the actual investigations and prosecutions will be carried out at the **decentralised level**, in essence[36] by the EDPs (at least two per participating Member State).[37] The EDPs will thus

---

[29] *Or to quote A. Weyembergh and C. Brière, the Member States' 'willingness to renationalise the EPPO as much as possible, and to keep the strongest control possible over its activities'. A. Weyembergh and C. Brière, Towards a European Public Prosecutor's Office (EPPO), Study for the LIBE Committee of the European Parliament, 2016, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571399/IPOL_STU(2016)571399_EN.pdf, p. 51.*
[30] *A. Weyembergh and C. Brière, op. cit., p. 15.*
[31] *Articles 8(1) and 3(1) of the Regulation.*
[32] *Article 8(2) of the Regulation.*
[33] *Article 8(3) of the Regulation.*
[34] *On the role of the College, see Article 9(2) of the Regulation.*
[35] *On the role of Permanent Chambers and the EPs, see Articles 10(2) and 12(1) of the Regulation.*
[36] *There are, however, a number of exceptions provided by the Regulation.*
[37] *Article 13(2) of the Regulation.*

perform their tasks at national level,[38] but 'shall act in the interest of the Union as a whole'.[39] Hierarchically, the EDPs are subordinated to the central level[40] and shall only follow instructions from the EPPO to ensure their independence.[41] Nevertheless, at the same time, the EDPs are also members of the national public prosecutor's office for the duration of their mandate.[42] Article 13(3) of the Regulation specifies that an EDP 'may also exercise functions as national prosecutors, to the extent that this does not prevent them from fulfilling their obligations under [the] Regulation'. This raises the delicate and much debated issue of the EDP's 'double-hat'. For instance, in the Netherlands[43] and Estonia,[44] the EDPs would indeed be able to handle national cases next to their EPPO investigations,[45] and this was also the initial intention of the German legislator.[46] Furthermore, the EDPs 'shall have the same powers as national prosecutors in respect of investigations, prosecutions and bringing cases to judgment',[47] including when it comes to information stored in national databases,[48] and will rely on national authorities when conducting the EPPO investigation.[49]

2.3. Impact of the EPPO's hybrid structure on the processing and the protection of personal data: Some introductory illustrations

The profoundly hybrid structure of the EPPO is also reflected in the rules regarding the processing of information (Chapter VII of the Regulation) and in the data protection regime (Chapter VIII of the Regulation).

---

[38] *Article 8(4) of the Regulation.*
[39] *Article 6(1) of the Regulation.*
[40] *Article 18 of the Decision of the College of the European Public Prosecutor's Office laying down rules on conditions of employment of the European Delegated Prosecutors, College Decision 001/2020, 29 September 2020.*
[41] *Article 6(1) of the Regulation.*
[42] *Article 17(2) of the Regulation.*
[43] *Article VII A of the Dutch Act on the EPPO.*
[44] *§ 7²(2) of the Prosecutor's Office Act: 'A European Delegated Prosecutor may perform the functions of a national prosecutor based on a decision of the Prosecutor General insofar this does not prevent him or her from performing any functions arising from Council Regulation (EU) 2017/1939.' Unofficial translation.*
[45] *The same approach was proposed by an academic study preparing the implementation of the EPPO into the Belgian legal order, in view of ensuring an optimal integration of the EDPs in the national judicial system, but the Belgian legislator decided not to follow this suggestion. See V. Franssen, F. Verbruggen, A.L. Claes and A. Werding, Implementatie van het Europees openbaar ministerie in de Belgische rechtsorde/Mise en oeuvre du parquet européen en droit belge, Brussels, June 2019, 231p. (on file with the authors); V. Franssen, A. Werding, A.L. Claes and F. Verbruggen, "La mise en oeuvre du Parquet européen en Belgique: Quelques enjeux et propositions de solution", in C. Chevallier-Govers and A. Weyembergh (eds.), La création du Parquet européen: simple évolution ou révolution au sein de l'espace judiciaire européen?, Brussels, Larcier, 2021, p. 149-154.*
[46] *The German Bill on the EPPO does not clarify whether the German EDPs may also exercise functions as national prosecutors.*
[47] *Article 13(1) of the Regulation.*
[48] *Article 43(1) of the Regulation.*
[49] *Article 28(1) and Recital 69 of the Regulation.*

2.3.1. Processing of information: 'e-case file' versus 'case file'

As regards the processing of information (or data)[50], the EPPO shall establish a case management system (hereinafter: CMS) which will contain a register of information obtained by the EPPO in accordance with Article 24 of the Regulation, an index of all case files, and all information from the EPPO's case files stored electronically (the so-called '**e-case file**'[51]).[52] The e-case file will be established at the level of the central office and obviously has to comply with all data protection rules laid down in the Regulation (see *infra*, Part VI).

Next to the e-case file, the EDP in charge of the investigation will open and handle a '**case file**', either manually or electronically depending on his or her national system. Contrary to the e-case file, this case file will be located at national level. While the EDP is in charge of the case file, this file will obviously be fed, on a continuous basis, by information brought forward by national authorities (e.g. police, customs authorities, national prosecutors (to the extent they are involved) and pre-trial judges) which conduct investigative measures,[53] or authorise them,[54] at the order or request of the EDP. What exactly the role and responsibilities of each of these actors in terms of data processing are, is subject to discussion (see *infra*, Part VI, Chapter d).

What is more, Article 45(2) of the Regulation provides that the 'case file' will be 'managed (…) *in accordance with the law of the [EDP]'s Member State*'.[55] The IRP adopted by the EPPO College add to this that 'the EPPO's case files shall be organised and managed in accordance with the [IRP] in order to ensure the proper functioning of the EPPO as a single office', yet '*without prejudice to the provisions of the national law applicable to the case*'.[56] The exact scope of this reference to national law is, however, unclear: to what extent does national law apply to the 'case file' of this EU body?

Even though there are some doubts as to what legal rules apply to the 'case file', it is definitely an EPPO file. Indeed, pursuant to Article 45(1), subparagraph 2 of the Regulation, this case file will 'contain all the information and evidence available to the [EDP] that relates to the investigation

---

[50] *The Regulation uses the terms 'information' and 'data' without a clear distinction. The term 'data' is most present in the provisions concerning data protection, while the term 'information' seems to be privileged elsewhere in the text.*
[51] *Admittedly, this term is not mentioned in the EPPO Regulation, but it is used by the EPPO Legal Service and therefore it is likely to become soon part of EPPO legal jargon. Moreover, by adopting this term, the authors of this study will be able to make a clear distinction between the file kept in the CMS and the case file stored at national level, which is highly significant for several reasons as the analysis in later parts of this report will show.*
[52] *Article 44(4) of the Regulation.*
[53] *Article 28(1) and Recital 69 of the Regulation.*
[54] *Article 30(3)-(4) of the Regulation.*
[55] *Emphasis added.*
[56] *Art. 43(2) of the IRP. Emphasis added.*

or prosecution by the EPPO'. Furthermore, the EDP in charge will have to ensure that the content of the e-case file reflects at all times the information contained in the case file,[57] which suggests that the case file is the original or primary EPPO file and the e-case file the copy (for further analysis, see *infra*, Part IV, Chapter c, Part V, Chapter a and Part VI, Chapter b).

Finally, while the access to the CMS and the case file is partly regulated by the EPPO Regulation,[58] the decision to grant access to other EDPs will be taken by the handling EDP '*in accordance with applicable national law*'.[59]

2.3.2. Data protection rules

As will be discussed in Part III, the data protection regime applicable to the EPPO differs in some respects from the general data protection rules applicable to EU institutions, bodies, offices and agencies[60] to account for the special nature of the EPPO. These rules also differ (slightly)[61] from the rules applicable to Eurojust, which as an EU agency[62] supports and coordinates the cooperation between national investigating and prosecuting authorities, yet which unlike the EPPO does not have the power to initiate criminal proceedings.[63] While the EPPO Regulation provides for a separate set of data protection rules, it is however important to note that these rules too, to some extent, refer back to national law.

For instance, with respect to the rights of data subjects, Article 49(6) of the EPPO Regulation explicitly states that the EPPO 'shall, where relevant, act in compliance with national procedural law on the obligation to provide information to the data subject and the possibilities to omit, restrict or delay such information'. This shows that the exercise of those rights will not only depend on the rules laid down in the EPPO Regulation, but also on national law. National law may refer

---

[57] *Article 45(3) of the Regulation, Article 61(6) of the IRP.*
[58] *Art. 46, subparas 1-2 of the Regulation.*
[59] *Art. 46, subpara. 3 of the Regulation. Emphasis added.*
[60] *See Regulation (EU) 2018/1725.*
[61] *Eurojust data protection regime, with regard to operational data, is composed of the Eurojust Regulation and of Article 3 and Chapter IX of Regulation (EU) 2018/1725. Article 26 of Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, O.J., L 295, 21 November 2018, p. 138 (hereinafter: Eurojust Regulation). The data protection rules contained in those instruments are not perfectly identical to the data protection regime under the EPPO Regulation. See, for instance, the provisions relating to automated individual decision-making, including profiling: Article 56 of the EPPO Regulation and Article 77 of Regulation (EU) 2018/1725.*
[62] *Art. 1(1) Eurojust Regulation.*
[63] *For an overview of Eurojust's functions and powers, see Article 4 of the Eurojust Regulation.*

to rules laid down in criminal procedure,[64] judicial organisation,[65] and/or data protection legislation,[66] and/or other legislations,[67] depending on the Member State at hand.

Another illustration of the hybrid legal regime with respect to the processing of data is provided by Article 47(3)(c) of the EPPO Regulation. According to this legal provision, '*applicable national procedural law* on the investigative measures taken in accordance with Article 30 [of the Regulation]'[68] may impose restrictions on the EPPO as regards the processing of the obtained data for other purposes than that for which it was collected (purpose limitation). In the Commission's view, the rules on national criminal procedure 'could be applicable' in this hypothesis, but only 'provided that such provisions do not go against the overarching data protection regime'.[69]

Similarly, if the EPPO receives data collected by national authorities, the latter may impose specific processing conditions in accordance with Article 9(3) and (4) of the LED.[70] Such conditions may be provided by 'Union or Member State law'.[71]

2.4. Conclusion

These examples show how much EU and national law are intertwined when it comes to the operational functioning of this new EU body. While Article 5(3) of the EPPO Regulation states that '[t]he investigations and prosecutions *on behalf of the* EPPO shall be governed by this Regulation',[72] that '[n]ational law shall apply to the extent that a matter is not regulated by this Regulation' and

---

[64] *This is e.g. the case of Belgium. See Act implementing the LED of 30 July 2018, Moniteur belge, 5 September 2018. It should be noted that this Act also implements the GDPR. On this topic, see Y. Liégeois and F. Bleyen, "Na een schijnhuwelijk en een schijnscheiding thans een gedwongen opname? Of de (uitoefening van de) rechten van de natuurlijke persoon bij de verwerking van diens persoonsgegevens in het strafproces", Speech by the Prosecutor General of the Court of Appeal of Antwerp on the occasion of the beginning of the judicial year 2020-2021, Nullum Crimen, 2020, p. 1-53.*

[65] *This is e.g. partly the case in Spain today. However, this may change in the near future as Spain has not yet implemented the LED. Furthermore, the Belgian Act implementing the LED also amends the Judicial Code.*

[66] *In Estonia, the rights of data subjects are laid down in the Personal Data Protection Act, but their exercise shall be guided by the provisions of Code of Criminal Procedure regardless of whether the data subject is a suspect, accused, victim, civil defendant, third party, witness or any other person. § 15[2](3) of the Code of Criminal Procedure. A comparable situation can be found in Romania, where relevant provisions are laid down in 13 et seq. of the Act implementing the LED and in various provisions of the Code of Criminal Procedure (e.g. article 142 (1[1]), 142 (6), 153 (2), 191 (5)).*

[67] *In France, data subjects' rights have been transposed in Title III of Act No 78-17 of 6 January 1978 relating to Information Technology, Files and Liberties (Journal Officiel de la République Française, 7 January 1978), as amended by the Act implementing the LED. However, when those rights relate to data processed in criminal proceedings, they should be exercised in accordance with the Code of Criminal Procedure (Article 70-24 of the Act No 18-17). See in particular Article 230-8 of the French Code of Criminal Procedure.*

[68] *Emphasis added.*

[69] *European Commission, Draft minutes, Ninth meeting of the EPPO Expert Group, 21 March 2019, p. 5.*

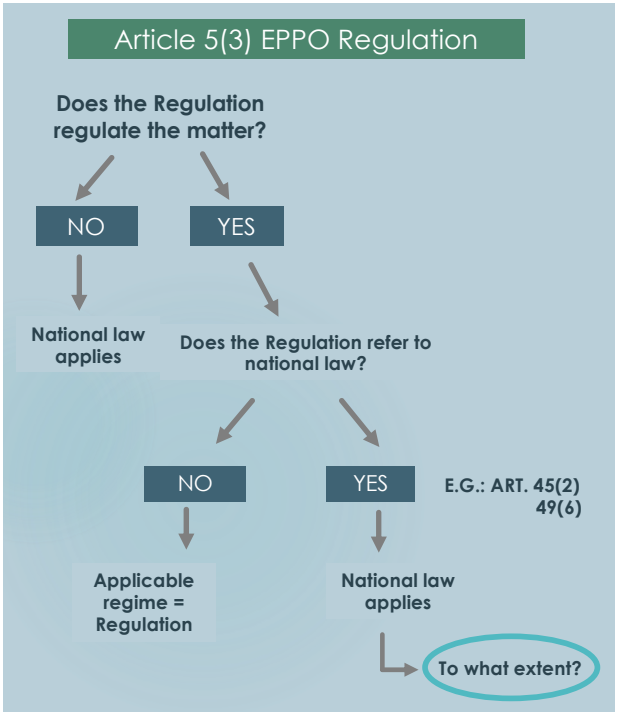
[70] *Art. 53(2) EPPO Regulation.*

[71] *Art. 9(3) LED.*

[72] *Emphasis added.*

that '[w]here a *matter is governed by both national law and this Regulation*, the latter shall prevail',[73] thereby confirming the primacy of EU law, the application of these *prima facie* clear rules addressing conflicts of law (see Figure 1) may not be so straight-forward after all. Indeed, it may in practice not always be easy to define the precise scope of EU and national law. This is particularly so because the interpretation of the references to national law leads, even at this stage, to diverging points of views. It is likely that these differences will one day become the object of proceedings before the Court of Justice of the European Union (hereinafter: CJEU). Until then, there is a risk that the patchwork of EU and national rules will result in quite diverse applications at the decentralized level of the EPPO. This situation will obviously not facilitate the delineation and exercise of the EDPS's supervisory role, as will be further explained in the subsequent parts of this study.

Figure 1. Article 5(3) of the EPPO Regulation



[73] *Emphasis added.*

3. THE EPPO AT THE CROSS-ROADS OF THREE DATA PROTECTION REGIMES: SCOPE OF APPLICATION

As a hybrid EU body with power to conduct criminal investigations, the EPPO is situated at the cross-roads of different data protection regimes. On the one hand, the EU legislator adopted for this new EU body a **two-pronged data protection regime**, consisting of the rules laid down in Regulation (EU) 2018/1725 as far as administrative personal data is concerned, and of special data protection rules laid down in the EPPO Regulation with respect to operational personal data.[74] On the other hand, the EPPO will be **closely and continuously cooperating with** national authorities, whose law enforcement activities are submitted to national data protection law which, in turn, has been partially harmonised by Directive (EU) 2016/680, and with EU institutions, bodies, offices and agencies,[75] whose activities are subject to Regulation (EU) 2018/1725 and, potentially, special data protection rules.[76]

In what follows, we will take a *prima facie* look at the relationship between these different data protection rules. While this relation is, at first sight, fairly straight-forward, the analysis in later parts of this study will show that, in practice, these rules will inevitably meet and intersect, rendering the relationship more complicated. This holds particularly true for the interplay between the EPPO Regulation and the LED.

---

[74] P. De Hert and V. Papakonstantinou, "Data Protection and the EPPO", N.J.E.C.L., 2019, p. 37 ; C. Paulet, "Le parquet européen et la protection des données à caractère personnel", in C. Chevallier-Govers and A. Weyembergh (eds.), La création du Parquet européen: simple évolution ou révolution au sein de l'espace judiciaire européen?, Larcier, 2021, p. 373-402.

[75] For instance, Article 100 of the EPPO Regulation provides that '[t]he EPPO shall establish and maintain a close relationship with Eurojust' and develop 'operational, administrative and management links between them'. On this topic see J. A. Espina Ramos, "The Relationship Between Eurojust and the European Public Prosecutor's Office", in L. Bachmaier Winter (ed.), The European Public Prosecutor's Office: The Challenges Ahead, Springer, 2018, p. 87-101; F. Spiezia, "The European Public Prosecutor's Office: How to Implement the Relations with Eurojust?", Eucrim, 2018, p. 130-137; N. Franssen and A. Weyembergh, "The future relationship between the European Public Prosecutor's Office and Eurojust", in C. Chevallier-Govers and A. Weyembergh (eds.), La création du Parquet européen: simple évolution ou révolution au sein de l'espace judiciaire européen?, Brussels, Larcier, 2021, p. 195-210.

[76] For instance, Eurojust may only process operational personal data listed in point 1 or 2 (depending on the categories of data subject) of Annex II of the Eurojust Regulation. See Article 27 of the Eurojust Regulation. Europol may only process data of certain categories of data subjects, e.g. witnesses and persons under the age of 18, if it is strictly necessary and proportionate for preventing or combating crime that fall within Europol's objectives. See Article 30(1) of 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 (hereinafter: Europol Regulation).

3.1. A two-pronged data protection regime: The relationship between Regulation (EU) 2018/1725 and the data protection rules in the EPPO Regulation

3.1.1. The distinction between operational personal data and administrative personal data

As indicated, the EPPO's activities are subject to two sets of EU data protection rules. The processing of administrative personal data is governed by Regulation (EU) 2018/1725,[77] while the processing of operational personal data is regulated by the EPPO Regulation which creates a specific and comprehensive data protection regime. The need for a separate, stand-alone data protection regime was considered necessary because of the 'special nature' of the judicial activities of the EPPO,[78] even though Regulation (EC) 2001/45[79] already provided for some specific derogations with respect to the prevention, detection, investigation and prosecution of criminal offences. Today, the Regulation (EU) 2018/1725 contains a whole chapter on the processing of operational personal data by Union institutions, bodies, offices and agencies when carrying out activities that fall within the scope of Chapter 4 or 5 of Title V of Part Three of the TFEU.

The distinction between the processing of these two types of personal data is not new. It was already made in the Europol Regulation, at least implicitly,[80] and subsequently in the Eurojust Regulation, but neither Regulation explains these two terms. The EPPO Regulation, in contrast, does provide a definition. Operational personal data are 'all personal data processed by the EPPO for the purposes laid down in Article 49'.[81] Administrative personal data are defined by opposition to operational personal data as 'all personal data processed by the EPPO apart from operational personal data'.[82] Administrative personal data are those the EPPO processes to conduct its management and administrative tasks. They include 'identification data of natural persons,

---

[77] *Article 48 of the Regulation.*
[78] *Recital 92 of the EPPO Regulation. Cf. Recital 9 of Regulation (EU) 2018/1725.*
[79] *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. This Regulation was repealed by Regulation (EU) 2018/1725.*
[80] *Indeed, contrary to the EPPO Regulation, the Europol Regulation does not define both types of personal data. Nor does it explicitly use the term 'operational personal data'. Recital 53 only refers to it in a negative way, stating that 'Europol also processes non-operational personal data, unrelated to criminal investigations, such as personal data concerning staff of Europol (...)'. Emphasis added.*
[81] *Article 2(18) of the Regulation.*
[82] *Article 2(17) of the Regulation.*

contact information, professional roles and tasks, information on private and professional conduct and performance, and financial data'.[83]

3.1.2. Consequences of the distinction

According to the operational or administrative purposes of the processing, the applicable data protection rules will differ to some extent,[84] although the principles of both regimes are the same.[85] These differences will, of course, impact the EDPS in the exercise of its supervision tasks.[86]

Regardless of the type of personal data, the EPPO is the controller of the data, although there will be situations where the allocation of responsibilities between the EPPO and national authorities may be subject to discussion (see *infra*, Part VI, Chapter d).[87] With respect to operational personal data, the EDP handling the case will in most situations be *de facto* responsible for the processing as he/she manages the case file, decides on requests for access to it,[88] and must ensure that the information in the e-case file corresponds at all times to the information contained in the case file.[89]

Practically speaking, the distinction between operational personal data and administrative personal data will also have ramifications in terms of storage location. While operational personal data will be stored, at central level, in the EPPO CMS and, at decentralised level, in the case file (which may take a paper or an electronic form) and potentially various information systems controlled by national authorities (see *infra*, Part VI, Chapter b and c), administrative personal data will be processed and stored in different locations depending the management and administrative tasks, though presumably only at the level of the central office.[90]

---

[83] *Recital 13 of the Internal Rules concerning restrictions of certain data-subject rights in relation to the processing of administrative personal data in the framework of activities carried out by the EPPO, College decision 006/2020, 21 October 2020.*
[84] *A detailed comparison of both regimes is beyond the scope of this study.*
[85] *Cf. Recital 11 of Regulation (EU) 2018/1725.*
[86] *As regards operational personal data, see Article 85 of the EPPO Regulation; with respect to administrative personal data, see Article 52(3) of Regulation (EU) 2018/1725 read in conjunction with Article 48(1) of the EPPO Regulation. P. De Hert and V. Papakonstantinou, op. cit., p. 38.*
[87] *Article 2(13) of the EPPO Regulation. Cf. Article 64(1) of the EPPO Regulation.*
[88] *Article 46, subpara. 3 of the EPPO Regulation, Article 61(5) of the IRP.*
[89] *Article 45(3) of the Regulation, Article 61(6) of the IRP.*
[90] *As the EPPO is not yet fully operational, an exact listing of those storage locations cannot be provided.*

3.2. The relationship between the data protection rules applicable to the EPPO and the LED

3.2.1. Distinct personal scope of application

The common denominator of Regulation (EU) 2018/1725 and the EPPO Regulation is that they apply to an **EU body**. By contrast, the LED applies to **national** 'competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.[91] At first sight, there should thus not be any overlap between both legal frameworks. Nevertheless, there are several reasons why the scope of application of these two sets of instruments is not so clear-cut after all. The EU legislator has, indeed, **interconnected** them in several respects.

1. Legislative interplay between the data protection rules applicable to the EPPO and the LED

First of all, Recital 93 of the EPPO Regulation states that 'the rules of this Regulation on the protection of personal data *should be interpreted and applied in accordance with the interpretation and application of [the LED]*'.[92] So far, there is no case law yet on the LED,[93] but any future rulings of the CJEU in this respect may thus be relevant for the interpretation and application of the data protection regime of the EPPO.[94]

---

[91] *Article 1(1) of the LED.*
[92] *Emphasis added. Cf. Recital 10 of Regulation (EU) 2018/1725.*
[93] *That said, it is noteworthy that the Grand Chamber of the Court of Justice has recently clarified the personal scope of application of the General Data Protection Regulation and the LED. In Privacy International, it ruled that the latter only applies to processing activities carried out by national competent authorities for the purposes of the prevention and detection of criminal offences, including the safeguarding against and the prevention of threats to public security, and not to individuals or private actors (in particular, providers of electronic communication services) processing personal data for the same purposes. CJEU, C-623/17, Privacy International, 6 October 2020, ECLI:EU:C:2020:790, paras 47-48.*
[94] *That said, one can already find relevant analyses and interpretations of the LED by Article 29 Data Protection Working Party, national supervisory authorities and academics. See e.g. Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), adopted on 29 November 2017; Belgian Data Protection Authority, Opinion No 77/2020 on the reform of the Code of Criminal Procedure, 22 August 2020, available at https://autoriteprotectiondonnees.be/publications/avis-n-77-2020.pdf; P. De Hert and V. Papakonstantinou, "The New Police and Criminal Justice Data Protection Directive", N.J.E.C.L., 2016, p. 7-19; J. Sajfert and T. Quintel, "Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities", in M.D. Cole and F. Boehm (eds.), GDPR Commentary, Edward Elgar Publishing, Forthcoming, available at SSRN: https://ssrn.com/abstract=3285873.*

Second, Regulation (EU) 2018/1725 and the EPPO Regulation when defining certain terms, explicitly refer to the definitions laid down in the LED.[95] Similarly, the tasks of the European Data Protection Board (hereinafter: EDPB) are determined by cross-reference to the LED.[96]

Third, with respect to specific processing conditions, both regulations also refer to the procedure put forward by the LED.[97]

Fourth, regarding the transfer of personal data to a third country or an international organisation, Article 81 of the EPPO Regulation provides that the EPPO may transfer operational personal data if 'the Commission has decided *in accordance with Article 36 of the [LED]* that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection'.[98] In the absence of such an adequacy decision, the data may still be transferred if the specific conditions of Article 82 of the EPPO Regulation are met, or in case of a specific derogation.[99] With regard to administrative personal data processed by the EPPO, similar provisions can be found in Regulation (EU) 2018/1725, with that difference that, in the hypothesis where there is no adequacy decision, the EPPO enjoys less autonomy to assess the appropriateness of the safeguards rules (e.g. in some cases, it will need the authorisation of the EDPS).[100] The list of derogations is also different.[101]

3.2.2. Interplay between the data protection rules applicable to the EPPO and national law

Furthermore, as indicated (*supra*, Part II), the EPPO Regulation **refers** on a number of occasions **to national law**. Therefore, indirectly, there are also bridges between the Regulation and the LED, as national law may be an implementation of the LED. In this respect, it should be noted that the ways in which Member States have transposed the minimum rules of the LED into national law vary considerably. Some have only amended their national data protection legislation,[102] while others have also amended, or still should amend,[103] their rules on criminal procedure[104] and/or

---

[95] *See e.g. Article 3(22) of Regulation (EU) 2018/1725 and Article 2(22) of the EPPO Regulation ('national supervisory authority'); Article 2(15) of the EPPO Regulation ('recipient').*
[96] *Article 87(3) of the EPPO Regulation.*
[97] *Article 75(2) of Regulation (EU) 2018/1725 and Article 53(2) of the EPPO Regulation.*
[98] *Emphasis added.*
[99] *Article 83 of the EPPO Regulation.*
[100] *Articles 47-48 of Regulation (EU) 2018/1725.*
[101] *Article 50 of Regulation (EU) 2018/1725.*
[102] *For instance, Romania adopted Act No 363/2018, which is the main Act implementing the LED, but also amended Act No 102/2005, concerning the organisation and functioning of the National Supervisory Authority on Personal Data Processing.*
[103] *As mentioned earlier, Spain's failure to implement the LED has recently resulted in a conviction by the Court of Justice.*
[104] *In Germany, further adjustments of the Code of Criminal Procedure seem to be necessary. See S. Schwichtenberg, "Das neue BDSG und die stop: zwei, die bislang noch nicht zusammengefunden haben", NK, No 32, 2020/1, p. 91-105.*

judicial organisation.[105] Yet others have adopted or amended separate, sectorial laws applicable to specific authorities (e.g. the police, customs authorities, penitentiary institutions).[106]

In particular, the EPPO Regulation refers to national law in two areas that have been harmonised by the LED: data subjects' rights and transfers of operational personal data to a third country or international organisation.

Article 49(6) of the EPPO Regulation states that when applying Articles 57 to 62 – provisions relating to data subjects' rights – 'the EPPO shall, where relevant, *act in compliance with national procedural law* on the obligation to provide information to the data subject and the possibilities to omit, restrict or delay such information'.[107] The LED provides grounds for Member States' authorities to delay, restrict or omit the provision of information to data subjects[108] and to limit data subjects' rights.[109] The Directive allows Member States to adopt legislative measures in order to determine categories of processing which may wholly or partly fall under any of these grounds. Further explanations on this subject will be provided in Part V.[110]

In addition, where personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings, the LED specifies that Member States may provide for the exercise of the rights to information, access, rectification or erasure and restriction of processing 'to be carried out *in accordance with Member State law*'.[111] The EPPO Regulation follows the same logic by providing that '[a]ccess to the case file by suspects and

---

[105] For instance, Article 37, para. 4 of the Belgian Act implementing the LED refers to the existing rules in the Judicial Code, the Code of Criminal Procedure and specific legislation and delegated legislation relating to criminal procedure. The current rules on criminal procedure are, however, not entirely in conformity with the LED. For instance, there is no explicit right to information or to rectification. For a detailed analysis and proposals for amendment, see Y. Liégeois and F. Bleyen, "Na een schijnhuwelijk en een schijnscheiding thans een gedwongen opname? Of de (uitoefening van de) rechten van de natuurlijke persoon bij de verwerking van diens persoonsgegevens in het strafproces", op. cit., p. 22-48. Furthermore, there is no supervisory authority competent to control the conformity of processing operations for which the criminal judicial authorities are responsible. Article 37 para. 4 of the Act of 30 July 2018, read in conjunction with Article 41 of the Act, provides that the rights of the data subject may be exercised through the competent supervisory authority. At present, however, Belgian law does not designate a competent authority for judicial authorities (i.e. the public prosecutor's office and the courts), hence this right of indirect access cannot be exercised. See Belgian Data Protection Authority, Opinion No 77/2020, op. cit., paras 14, 16 and 17.

[106] For instance, in the Netherlands, the Act implementing the LED has amended the Police Data Act (Wet politiegegevens) and the Judicial and Criminal Records Act (Wet justitiële en strafvorderlijke gegevens). Some more general provisions (e.g. those defining the competent supervising authority) are, however, laid down in the Implementing Act of the GDPR (Uitvoeringswet Algemene verordening gegevensbescherming, 16 May 2018, Staatsblad van het Koninkrijk der Nederlanden, No 144, 22 May 2018). In Estonia, the LED was implemented (mainly) by the Personal Data Protection Act of 12 December 2018, which amended some 130 other Acts.

[107] Emphasis added.

[108] Article 13(3) of the LED.

[109] Article 15(1) of the LED.

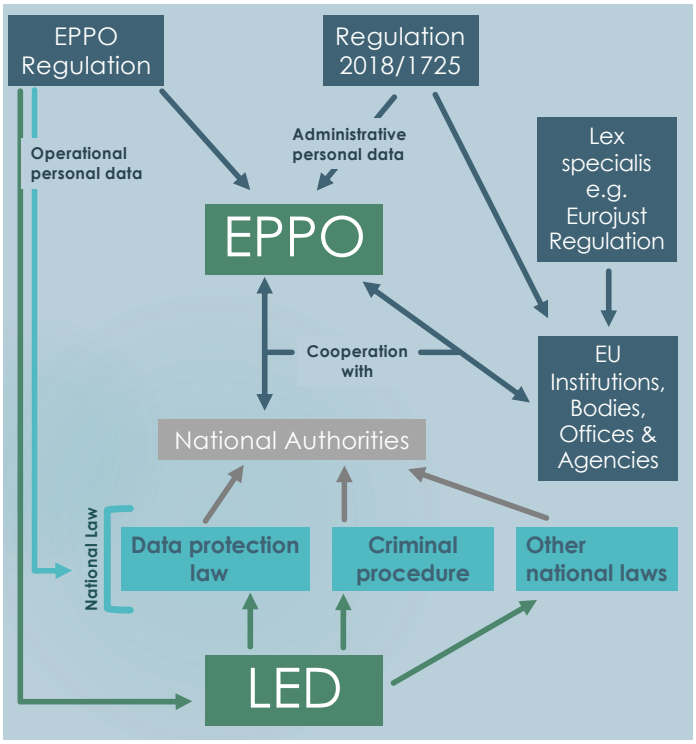
[110] Articles 13(4) and 15(2) of the LED

[111] Article 18 of the LED. Emphasis added.

accused persons as well as other persons involved in the proceedings shall be granted by the handling [EDP] *in accordance with the national law of that Prosecutor's Member State*'.[112]

When the EPPO transfers operational personal data to a third country or international organisation, and that such data have been transmitted or made available by a Member State of the European Union, the EPPO 'shall obtain prior authorisation for the transfer by the relevant competent authority of that Member State of the European Union *in compliance with its national law*, unless that Member State of the European Union has granted this authorisation to such transfer in general terms or subject to specific conditions'.[113]

Figure 2. The EPPO at the cross-roads of different data protection regimes



Finally, there are also references to national law that remain somewhat ill-defined. This particularly holds true for the reference in Article 45(2) of the EPPO Regulation, stating that '[t]he case file shall be *managed* by the handling [EDP] *in accordance with the law of his/her Member State*.'[114] To what extent national law applies to the case file, is far from clear: does this only refer to the way in which case files are kept, stored and/or organised (e.g. electronically or on paper, by automated means or in structured manual files), or does it also mean that national data protection

[112] *Article 45(2), subpara. 2 of the EPPO Regulation. Emphasis added.*
[113] *Article 80(1) (c) of the Regulation. Emphasis added.*
[114] *Emphasis added.*

rules (including, e.g., time limits on data retention) fully apply? These questions will be addressed in more detail in Part VI.

4. THE EPPO'S POWERS AND TASKS REGARDING THE PROCESSING OF OPERATIONAL PERSONAL DATA AND THEIR LIMITS

In order to fulfil its mission – carrying out investigations and prosecutions in matters that belong to its material competence – the EPPO will process[115], in most cases electronically,[116] operational personal data from different categories of data subjects. To determine the limits of the EPPO's powers and tasks in regard to the processing of operational personal data, the EPPO Regulation must be read in conjunction with the IRP, the DP Rules and the Rules concerning the data protection officer (hereinafter: DPO Rules)[117] which implement and complement the provisions of the Regulation. The definition of these powers and their limits are, of course, important for the future supervision of the EPPO's activities by the EDPS. That said, in the first place, the DPO of the EPPO will be in charge of monitoring and ensuring compliance with the DP Rules.[118]

4.1. Processing for specific purposes only

Similar to other data protection instruments, such as the GDPR[119] and the LED, the EPPO Regulation establishes principles relating to processing of personal data which are listed in Article 47. In addition to those, Article 49(1) of the Regulation specifies that operational personal data may be processed by automated means[120] or in structured manual files for **three specific purposes only**, and always in accordance with the Regulation:

- criminal investigations and prosecutions undertaken by the EPPO;
- information exchange with the competent authorities of Member States of the EU or other institutions, bodies, offices and agencies of the Union;

---

[115] Under the Regulation, processing means 'any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction' (Article 2 (8)).

[116] As stated in Recital 47 of the EPPO Regulation, 'the work of the EPPO should, in principle, be carried out in electronic form'.

[117] Rules concerning the Data Protection Officer of the European Public Prosecutor's Office, College Decision 005/2020, 21 October 2020.

[118] Art. 3(2) of the DPO Rules.

[119] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, O.J., L 119, 4 May 2016, p. 1 (hereinafter: GDPR).

[120] The Regulation mentions the possibility to create automated data files without however defining it (Article 44(5)). The IRP specify that the procedure for the processing of operational personal data in such files and applicable safeguards will be dealt with in accordance with Article 64 of the IRP (Article 65(2)). Article 19 of the DP Rules provide that the rules applicable to the processing of operational personal data will be adopted in consultation with the EDPS.

- cooperation with third countries and international organisations.

It should already be noted that national procedural law, in conformity with Article 47(3)(c) of the Regulation, could potentially limit the processing of data collected or obtained at national level through investigative measures taken in accordance with Article 30 of the Regulation (see *infra*, Chapter d).

As an exception to the rule contained in Article 49(1), the Regulation foresees the possibility for the EPPO to **temporarily process operational personal data prior to inserting it into the CMS** 'for the purpose of determining whether such data are *relevant* to its tasks and for the purposes referred to [above]'.[121] Hence, this type of processing is not an independent data processing purpose.

The EPPO College has further limited this possibility of temporary processing to the situation where the EPPO receives personal data from a **private person**.[122] In such case, the EPPO may process the personal data in order to assess whether it is '*manifestly* outside of the competence of the EPPO'.[123] In this regard, the wording of the rules adopted by the College seems more restrictive than the Regulation. This assessment can be made by an EDP, an EP or even 'another'[124] member of the EPPO staff, provided that one of the former two validates the assessment.[125] If the EPPO comes to the conclusion that the data do 'manifestly' not refer to an offence belonging to the EPPO's material competence, the data will not inserted into the CMS but transmitted without undue delay, by an EDP or an EP, to the respectively competent authority (e.g. national public prosecution office, national customs authorities or an(other) administrative authority) if identifiable, or if not, deleted.[126] During the assessment period, the personal data may also be processed 'for the purposes of the exercise of data subject's rights and related supervision'.[127] Even if this data will be not be entered into the CMS but transmitted or deleted, its processing can be

---

[121] *Article 49(4) of the Regulation. Emphasis added.*
[122] *Article 17(1) of the DP Rules read in conjunction with Article 38(7) of the IRP. It should be noted that such data may arrive in very different forms (letters, emails, calls, parcels, etc.). The way in which these data will be collected, treated and stored will be determined by the EPPO in the near future.*
[123] *Article 17(1) of the DP Rules. Emphasis added. Article 17(4) of the DP Rules specifies that the assessment 'shall be undertaken by a European Delegated Prosecutor or a European Prosecutor, or in case the assessment is performed by another staff member of the EPPO, the assessment shall be validated by a European Delegated Prosecutor or a European Prosecutor'.*
[124] *The use of this word by Article 17(4) of the DP Rules is somewhat surprising because the EDP and the EP are formally not part of the 'staff of the EPPO', as defined by Article 2(4) of the Regulation.*
[125] *Art. 17(4) of the DP Rules.*
[126] *Article 17(1) of the DP Rules read in conjunction with Article 38(7) of the IRP.*
[127] *Article 17(2) of the DP Rules.*

traced afterwards as Article 38(7) of the IRP imposes the requirement to keep 'an adequate log' (see *infra*, Chapter b).

In contrast, whenever the EPPO receives information from a **national or supranational authority** in accordance with Article 24 of the Regulation, this information will be inserted in the CMS' register, even if the EPPO subsequently decides not to exercise its right of evocation.[128] If the EPPO decides to investigate a case after the receipt of information, it will open a case file in the CMS, to which an identification number will be assigned in the index of case files and which will contain a permanent link to the initial registration created by the CMS.[129]

4.2. Traceability of operational personal data and record of processing activities

When an EDP decides to exercise the EPPO's competence by initiating or evoking a case, a case file will be opened in the EPPO CMS.[130] The Regulation imposes that the EPPO processes operational personal data 'in a way that it can be established which authority provided the data or where the data has been retrieved from'.[131] The IRP specify that 'the EPPO shall ensure that all receipts of personal data (...) are duly logged and traceable'.[132] Taking into account the fact that the EPPO will gather information from different sources – e.g. national authorities, databases and registers,[133] databases and registers from other EU agencies,[134] private parties – the ability of the EPPO to **retrace the original source of the personal data** inserted in the CMS is crucial, especially in case of rectification of inaccurate personal data following a request from a data subject. Article 61(6) of the Regulation requires that the EPPO 'communicate[s] the rectification of inaccurate operational personal data to the competent authority from which the inaccurate personal data originate'. Regarding personal data received from private parties but not inserted in the CMS (*supra*, Chapter a), the EPPO 'may'[135] keep an appropriate log 'at a central level of the

---

[128] *Article 38(1) of the IRP.*
[129] *Article 41(1) of the IRP.*
[130] *Article 45(1) of the Regulation; Article 41 of the IRP.*
[131] *Article 49(5) of the Regulation.*
[132] *Article 63(3) of the IRP.*
[133] *Article 43(1) of the Regulation: 'European Delegated Prosecutors shall be able to obtain any relevant information stored in national criminal investigation and law enforcement databases, as well as other relevant registers of public authorities, under the same conditions as those that apply under national law in similar cases.'*
[134] *Article 43(2) of the Regulation: 'The EPPO shall also be able to obtain any relevant information falling within its competence that is stored in databases, registers of the institutions, bodies, offices and agencies of the Union.'*
[135] *By contrast, Article 38(7) of the IRP obliges the EPPO to keep an adequate log of this kind of processing. The discrepancy in the auxiliary verbs used by these two College decisions ('shall' v. 'may') is surprising, but can perhaps be explained by their finality: while the IRP define the internal organisation of the EPPO, the DP Rules further specify the conditions under which the EPPO is allowed to process personal data as well as the conditions and modalities for the exercise of data subjects' rights and possible restrictions.*

name of the sender (if available), and a record of the action taken' (assessment and transfer or deletion), 'including the name of the EDP or EP who made or validated the assessment'.[136]

The EPPO must also keep a **record** of all **categories of processing activities** under its responsibility and must contain specific information relating to, *inter alia*, the purposes of processing, the categories of data subjects and categories of operational personal data, and the security of the processing.[137] The records must be made in writing, including in electronic form, and shall be available to the EDPS on request.[138]

The **CMS** will serve as a **tool** to record processing activities as well as transmission (see *infra*, f.) and receipt of operational personal data. Article 2(1) of the DP Rules provides that the CMS 'shall serve wherever possible as the record of all processing activities' relating to operational personal data.[139] The CMS will contain 'a full record of transmission and receipt of operational personal data'.[140] This will allow the EPPO, but also its DPO and the EDPS when monitoring or supervising the EPPO's compliance with the data protection rules, 'to establish any transmission of operational personal data and the identification of the authority, organisation or third country or international organisation which transmitted or received such information to/from the EPPO'.[141]

4.3. Times limits for storage

The EPPO may, of course, not store operational personal data for indefinite periods of time. Article 63(5) of the IRP states that 'no personal data, be it administrative or operational, shall be kept longer than necessary for the purpose for which it has been processed, or than required due to other legal obligations'.

With regard to the **time limits for the storage** of operational personal data, Article 50 of the EPPO establishes a **mixed system**, combining maximum time limits with periodical reviews of the continued need for the storage of operational personal data.

On the one hand, the EPPO is required to review the need for the storage not later than three years after the data were first processed and then every three years. The EDPS shall be informed when

---

[136] *Article 17(5) of the DP Rules.*
[137] *Article 68(1) of the Regulation.*
[138] *Article 68(2) and (3) of the Regulation.*
[139] *The second part of the Article indicates that 'whenever this is not possible, such as due to technical or operational circumstances, an alternative auditable record recording any such processing shall be made, such as physical logs'.*
[140] *Article 2(2) of the DP Rules.*
[141] *Article 2(2) of the DP Rules.*

operational personal data are stored for a period exceeding five years.[142] Meanwhile, the CMS has been designed to facilitate the EPPO's compliance with this review obligation: A system of automated flagging will alert the data controller of the need to perform a periodical review and will thereby also facilitate monitoring.[143]

On the other hand, the Regulation establishes maximum time limits for the storage of operational personal data which apply to tried cases. In case of an acquittal, operational personal data shall not be stored beyond five years after the decision has become final. In case the accused is found guilty, 'the time limits shall be extended until the penalty that has been imposed, is enforced or can no longer be enforced under the law of the sentencing Member State'.[144] In the latter scenario, the maximum time limits for the storage of operational personal data will therefore depend on the statute of limitations applicable to the penalty in the sentencing Member State, or potentially the law of the executing Member State in case the convict's sentence is executed in another Member State in order to facilitate his/her social rehabilitation.[145] In this regard, it should however be noted that Article 12 of Directive (EU) 2017/1371,[146] to which the EPPO Regulation refers to define the material competence of the EPPO,[147] imposes minimum 'limitation periods', not only relating to the investigation, prosecution and trial of PFI offences,[148] but also with respect to the enforcement of prison sentences imposed for such offences.[149] As a result, national law should provide a limitation period of at least five years starting from the date of final conviction. This five-year period may in practice be longer due to the extensions arising from interruption or suspension. The grounds for interruption and suspension are defined exclusively by national law.

Before one of these maximum time limits expires, the EPPO must review the need for the continued storage of the operational personal data. The data may be kept 'where and as long this is necessary

---

[142] Article 50(1) of the Regulation.
[143] It is worth noting this flagging system is not regulated by the IRP or the DP Rules in order to ensure technical flexibility. Interview with the EPPO Legal Service.
[144] Article 50(2) of the Regulation.
[145] Article 3(1) of Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union, O.J., L 327, 5 December 2009, 27. Article 17(1) of this Framework Decision provides that the enforcement of the sentence is governed by the law of the executing Member State. Therefore, one may conclude that the statute of limitations of this Member State is applicable.
[146] Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, O.J., L 198, 28 July 2017, p. 29 (hereinafter: PFI Directive).
[147] Article 22(1) of the Regulation.
[148] Article 12(1)-(3) of the PFI Directive.
[149] Article 12(4) of the PFI Directive.

to perform its tasks'.[150] The EPPO will have to justify and record the reasons for the continued storage.[151] In the absence of a decision, the data should, in principle, be 'deleted automatically'.[152]

It is quite obvious that the rules enshrined in Article 50 of the Regulation apply to the *operational personal data stored in the CMS*. In contrast, based on the interviews conducted with representatives from some of the selected Member States,[153] it is less clear whether the above rules also apply to the case file managed by the EDP and stored at national level. Indeed, some actors seem to interpret the reference to national law in Article 45(2) of the EPPO Regulation broadly, encompassing also national data storage rules. On the one hand, this point of view is quite understandable: Considering the case file is stored at national level in the same IT systems (or, in case of a paper case file, under the same conditions) as purely national case files (i.e. case files that do not relate to an EPPO investigation), it is practically speaking not so obvious to apply different data storage rules. Yet, on the other hand, the case file is an EPPO file (it is opened and managed by the handling EDP; *supra*, Part II, Chapter c, Section 1) and the data it contains are operational personal data *processed by the EPPO*, thus requiring the application of the data protection rules contained in the Regulation. This is far from a historical or mere theoretical debate, as the more detailed analysis in Part VI will show (see also *infra*, Part V, Chapter a).

Interestingly, the German legislator – the only one who really reflected on data protection issues in the context of the EPPO (*supra*, Part I, Chapter b) – highlighted these rules can be further supplemented by more specific national rules. For instance, according to Section 101(8) of the German Code of Criminal Procedure, personal data acquired by means of an undercover measure shall be deleted 'without delay' if they are no longer necessary for the purposes of criminal prosecution or a possible court review.[154] The same holds true for the labelling requirement laid down in Section 101a of German Code of Criminal Procedure applicable to traffic data collected on the basis of Section 100g of the German Code of Criminal Procedure.[155] Such national rules can, however, not contradict the rules laid down in Article 50 of the Regulation.[156] In practice, the difference between 'supplementing' and 'contradicting' may not always be so clear though. Could one argue that national rules that impose shorter storage limits or stricter conditions for periodical

[150] *Article 50(3) of the Regulation.*
[151] *Article 50(3) of the Regulation. See also Article 18 of the DP Rules.*
[152] *Article 50(3) of the Regulation.*
[153] *Interview with M.-H. Descamps; Interviews conducted with N. Franssen.*
[154] *Explanatory Memorandum to the German Bill on the EPPO, p. 40.*
[155] *Ibid.*
[156] *Cf. Article 5(3) of the Regulation.*

review are more protective from the data subject's perspective and thus 'supplement' Article 50 of the Regulation?[157] One day, this question might be raised before the Court of Justice… Moreover, the dividing line between storage rules and conditions imposed pursuant to Article 47(3)(c) in relation to investigative measures taken in accordance with Article 30 of the Regulation (which both refer to national procedural law) may not always be so easy to establish, as the above German example shows.[158]

Next, concerning data processed *prior to* insertion in the CMS,[159] the DP Rules specify that those may not be stored 'longer than necessary for the assessment and transfer' to take place and, 'in any event, no longer than 6 months after receipt by the EPPO'.[160] Once that deadline has passed, the data must be automatically deleted and/or destroyed.[161]

In contrast, for information received in accordance with Article 24 of the Regulation (*supra*, Chapter a), there are no specific time limits. This means that the general time limits laid down in Article 50(1) of the Regulation apply.

4.4. Limitations to processing: special categories of operational personal data, specific processing conditions and data categories in the index

Contrary to other EU agencies such as Eurojust,[162] there is no restriction regarding the data categories the EPPO may process. However, some provisions of the Regulation temper this principle.

As indicated above (see *supra*, Chapter a), in accordance with Article 47(3)(c) of the Regulation, national procedural law could potentially limit the processing to certain data categories. German legislation, for instance, imposes some additional processing conditions on the EPPO in case the data are collected in Germany in the context of an EPPO investigation. When processing such data for the purpose of either Article 49(1)(a) (the EPPO's own investigations) or Article 49(1)(b)-(c) of

---

[157] Cf. H.-H. Herrnfeld, D. Brodowski and C. Burchard, European Public Prosecutor's Office: Article-by-Article Commentary, Hart Publishing, 2020, p. 478.
[158] Cf. Explanatory Memorandum to the German Bill on the EPPO, p. 40.
[159] This refers to the earlier mentioned situation where the EPPO receives information from a private party and concludes that the information does 'manifestly' not concern an offence within its competence. Of course, if the EPPO considers the information is 'relevant', it will normally open an investigation, at which point a case file is created and the data are input into to CMS, unless the EPPO prefers to refer the case for investigation to the national authorities. As a reminder, even when the EPPO is competent, it is not obliged to open an investigation. Article 27(3) and 27(7) of the Regulation.
[160] Article 17(3) of the DP Rules.
[161] Article 17(3) of the DP Rules.
[162] As mentioned earlier, Eurojust may only process operational personal data listed in point 1 or 2 of Annex II of the Eurojust Regulation. Article 27 of the Eurojust Regulation.

the Regulation (information exchange with Member States or EU institutions, bodies, offices or agencies, or cooperation with third countries or international organisations), the EPPO must respect Section 479(1) to (3) of the Code of Criminal Procedure.[163] These provisions contain prohibitions on transfer and restrictions on use of data.

Another provision that may limit the data categories the EPPO may process can be found in Article 55(1) of the Regulation, which states that **processing of special categories of operational personal data**[164] is allowed 'only where strictly necessary for the EPPO's investigations, subject to appropriate safeguards for the rights and freedoms of the data subject and *only if they supplement other operational personal data already processed by the EPPO*'.[165]

Under Article 53(2) of the Regulation, the EPPO must comply 'with **specific conditions for processing** provided by a national authority in accordance with Article 9(3) and (4) of [the LED]'. Recital 36 of the LED provides as examples of such conditions, *inter alia*, a prohibition against using personal data for purposes others than those for which they were transmitted or the obligation to inform the data subject in the case of a limitation of the right of information without the prior approval of the transmitting competent authority. Taking into account the fact that the EPPO will obtain data, through the EDPs, from national authorities (for a more detailed analysis see *infra*, Part VI, Chapter c), this provision may play a significant role in limiting the EPPO's processing activities. The German legislator has indicated that, for instance, Section 161 paragraph 4 of the German Code of Criminal Procedure was applicable to the EPPO.[166] This provision contains restrictions on the use of personal data obtained on or from private premises by technical means for the purpose of personal protection during covert investigations.

Another example relates to the **limited categories of data that may be processed in the index of the CMS**. The index is a tool to identify cases and to establish cross-links to between different case files; contrary to the case files themselves, it is also accessible to EPPO officials who are not directly involved in the investigation (*infra*, e.). In accordance with Articles 49(2) and (3) of the Regulation, the categories of operational personal data and the categories of data subjects whose operational personal data may be processed in the index has been determined in an Annex adopted

---

[163] *Explanatory Memorandum to the German Bill on the EPPO, p. 39.*
[164] *Defined as 'operational personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, operational personal data concerning health or operational personal data concerning a natural person's sex life or sexual orientation'. Article 55(1) of the Regulation.*
[165] *Emphasis added.*
[166] *Explanatory Memorandum to the German Bill on the EPPO, p. 40.*

by the European Commission,[167] in line with the principles of purpose limitation and data minimisation.[168] The categories of data that may be processed in the index depend on the category to which the data subject belongs. In relation to natural persons who reported or are victims of offences that fall within the competence of the EPPO, the Annex specifies that the categories of operational personal data that may be processed in the index must be 'limited to what is necessary and proportionate in order for the EPPO to perform its investigative and prosecutorial tasks'. The same requirement applies to the categories of operational personal data that may be processed concerning contacts or associates of suspected, accused or convicted persons in or following the criminal proceedings of the EPPO. Furthermore, the data categories that may be processed in the index in relation to natural persons who are reported or are victims of offences, and contacts or associates of suspected, accused or convicted persons in or following the criminal proceedings of the EPPO, will be more limited than those that may be processed as regards suspected or accused persons and persons convicted following the criminal proceedings of the EPPO.[169]

It is, of course, very well possible that a person changes from one category to another during the investigation (e.g. a contact of the suspect becomes a suspect too).

4.5. Access to operational personal data

As processing includes the consultation of data,[170] it is also important to consider the powers and limitations in this respect.

In general, Article 76 of the EPPO Regulation specifies that only the ECP, the EPs, the EDPs 'and authorised staff assisting them may, for the purpose of achieving their tasks and within the limits provided for in [the] Regulation, have access to operational personal data processed by the EPPO'.[171]

As explained, operational personal data processed by the EPPO will be stored, to the extent possible, in the CMS which will be composed of a register, an index and the information from the

---

[167] *Commission Delegated Regulation (EU) 2020/2153 of 7 October 2020 amending Council Regulation (EU) 2017/1939 as regards the categories of operational personal data and the categories of data subjects whose operational data may be processed in the index of case files by the European Public Prosecutor's Office, O.J., L 431, 21 December 2020, p. 1. These categories correspond to the categories of data subjects listed in Article 51 of the Regulation. The same categories are repeated in Article 41(2) of the IRP.*
[168] *Article 47(1)(a)-(b) of the Regulation.*
[169] *Point B of the Annex refers to 13 categories of personal data that may be processed in the index while point C refers to 7 categories and point D to 6 categories.*
[170] *Article 4(2) of the GDPR.*
[171] *Article 76 of the Regulation.*

case files (i.e. the e-case file; *supra*, Part II, Chapter c, Section 1).[172] Yet, some operational personal data are or cannot be processed within the CMS, such as a printed version of the case file or data that are not available in electronic form (e.g. seized goods). In that respect, Article 15 of the DP Rules, however, provides that the rules and principles regarding access from the IRP title devoted to the CMS shall apply *mutatis mutandis*.

With regard to the right to **access to the CMS**, the Regulation sets the general rules, which are further supplemented by the IRP.[173] Not all members of the EPPO will have access to every component of the CMS, or on the same conditions, as will be explained below. By contrast, national authorities, even when directly involved in the EPPO investigation, will not have access to the CMS;[174] the CMS will, in principle, be purely internal to the EPPO.[175]

As regards the **register** and the **index**, Article 46 of the EPPO Regulation provides that the ECP, the DECPs, the EPs and the EDPs will have direct access. The IRP, however, specify that this access is limited 'to the extent required for the performance of their duties'.[176] Furthermore, the EPPO staff[177] may also be granted the right to access the register and/or the index if required for the performance of their duties. This decision will be taken by the ECP and define the level of access and the conditions for exercising it.[178] The ECP may, however, also decide to temporarily restrict access to a specific information in the register and/or to a specific case file in the index by making it available only to the permanent members of the Permanent Chamber, the supervising EP, the handling EP and other specifically designated staff. This may only be done in exceptional cases, if needed to ensure confidentiality.[179]

The supervising EP and the competent Permanent Chamber shall have direct access to the **e-case file** when exercising their competence in accordance with Articles 10 and 12 of the EPPO Regulation.[180] The supervising EP shall also have direct access to the **case** file (i.e. the one stored at national level, managed by the handling EDP; *supra*, Part II, Chapter c, Section 1**)**, while the

---

[172] *Article 44(4) of the Regulation.*
[173] *Article 2(3) of the DP Rules refers to the IRP for the rules concerning the operation and access to the CMS.*
[174] *This follows from Article 46 of the EPPO Regulation.*
[175] *This was confirmed in an interview with the EPPO Legal Service. This can also be inferred from the fact that only the EDP can enter information into the CMS, or the staff of the EPPO or other administrative staff at national level under the EDP's control. Article 61(6) of the IRP.*
[176] *Article 46, subpara. 1 of the EPPO Regulation read in conjunction with Article 6(1) of the IRP.*
[177] *Defined as the 'personnel at the central level who supports the College, the Permanent Chambers, the European Chief Prosecutor, the European Prosecutors, the European Delegated Prosecutors and the Administrative Director in the day-to-day activities in the performance of the tasks of this Office under this Regulation'. Article 2(4) of the Regulation.*
[178] *Article 61(2) of the IRP.*
[179] *Article 63(3) of the IRP.*
[180] *Article 46, subpara. 2 of the Regulation*

Permanent Chamber will have to request such access.[181] Moreover, the ECP and DECP shall have direct access to e-case file or access to the case file, but only 'to the extent required for the performance of their duties'.[182] EDPs other than the handling EDP may request such access to the handling EDP, who will grant or refuse the access 'in accordance with applicable national law'.[183] The IRP add to this that the handling EDP shall grant access to the assisting EDP or other EDPs, who must submit a 'reasoned request', 'only to the extent required for the undertaking of the tasks assigned to them'.[184] Interestingly, the same holds true for members of the EPPO staff, even though this option is not explicitly provided for by the Regulation when it comes to the case file. The Regulation does, however, not indicate what rules of national law could be relevant for access to the case file; this will be determined by the Member States. Moreover, this requirement to follow national law does not apply to the supervising EP and the competent Permanent Chamber (*supra*). In case of a refusal, an 'appeal' before the Permanent Chamber is possible, which will decide 'in accordance with applicable national law as well as this Regulation'.[185] In sum, for some persons, the access to operational personal data is regulated **by both EU and national law**.

4.6. Transfers of operational personal data: allowed but subject to specific conditions

The EPPO may transfer operational personal data to a third country or international organisations[186] as well as to institutions, bodies, offices and agencies of the Union[187] and non-participating Member States' competent authorities.[188] These transfers are subject to compliance with specific conditions contained in the Regulation and in the DP Rules (see *infra*, Part V, Chapter b, Section 3).

As foreseen for the receipt of personal data, the EPPO shall ensure that any transfers of personal data are 'duly logged and traceable, including, where required in line with these or other implementing rules, the grounds for their transfer'.[189] To this end, the DP Rules specify that transfers to any of the authorities mentioned above shall be recorded in the CMS 'together with

[181] *Article 46, subpara. 2 of the Regulation.*
[182] *Article 61(4) of the IRP.*
[183] *Article 46, subpara. 3 of the Regulation.*
[184] *Article 61(5) of the IRP.*
[185] *Article 46, subpara. 3 of the Regulation.*
[186] *Article 80 of the Regulation.*
[187] *Article 54 of the Regulation.*
[188] *Article 10 of the DP Rules.*
[189] *Article 63(3) of the IRP.*

the recipient, reasons and justification'. The record shall be made available to the DPO and upon request to the EDPS.[190]

[190] *Articles 10(2) and 12(6) of the DP Rules.*

5. THE INTERPLAY BETWEEN THE EPPO REGULATION, THE LED AND ITS NATIONAL IMPLEMENTATIONS

5.1. Introduction: An EU body relying on national legislation[191]

As discussed in Part II, the EPPO is the outcome of a delicate political compromise. During the four years of negotiation on the Regulation, the EPPO shifted from a rather centralised, hierarchical structure directed by one person to a more decentralised model led by a college with representatives from each Member State.[192] This gives the EPPO a strong intergovernmental flavour, contrary to the federal logic of the centralised model in the Commission's proposal,[193] which also transpires from the increased number of references to national law in the EPPO Regulation – 86 in total, compared to 37 in the Commission's proposal.[194]

These **references to national legislation** may result in a patchwork of EU and national rules, also when it comes to data protection, despite the fact that the EPPO Regulation 'provides for an autonomous, standalone and comprehensive data protection regime'.[195] In a number of instances, indeed, the EPPO will have to combine the data protection rules of the Regulation with national rules. For instance, Article 49(6) of the Regulation states that when applying provisions relating to data subject's rights, 'the EPPO shall, *where relevant*, act in compliance with national procedural law on the obligation to provide information to the data subject and the possibilities to omit, restrict or delay such information'.[196]

It is important to (re-)emphasize that such national rules may be laid down in data protection legislation, but also in criminal procedure (*supra*, Part III, Chapter b, Section 3). Indeed, not all Member States make a clear-cut distinction[197] between the rights of *data subjects* (data protection perspective) and the rights of *subjects, victims and other interested parties* (criminal procedural perspective). For instance, under Belgian law, the rights of data subjects in the context of a criminal investigation are to be exercised '*exclusively* within the limits and in accordance with the rules and

---

[191] *It should be noted that this analysis focuses on the investigation stage. Trial proceedings in EPPO cases are governed by national law.*
[192] *L. Bachmaier Winter, "Introduction: the EPPO and the Challenges Ahead", op. cit., p. vi; J.A.E. Vervaele, "The European Public Prosecutor's Office (EPPO): Introductory Remarks", in W. Geelhoed, L.H. Erkelens, A.W.H. Meij (eds.), Shifting Perspectives on the European Prosecutor's Office, Berlin, Springer, 2018, p. 12 et seq.*
[193] *For one of the first analyses of the Commission's proposal, see V. Franssen, "Proposed Regulation on the European Public Prosecutor – Thinking Federal?", European Law Blog, 8 August 2013, http://europeanlawblog.eu/?p=1887.*
[194] *D. Flore, op. cit., p. 230.*
[195] *European Commission, Draft minutes, Ninth meeting of the EPPO Expert Group, 21 March 2019, p. 3.*
[196] *Emphasis added.*
[197] *Some Member States do, of course. For instance, the Dutch legislation clearly distinguishes data subjects' rights, regulated by Article 17a through 26b of the Implementing Act of the GDPR, from the rights of suspects.*

conditions laid down in the (...) Code of Criminal Procedure, special laws relating to criminal procedure and their implementing decrees'.[198] In Estonia, the approach is more nuanced. Here, the rights of data subjects are regulated by the Personal Data Protection Act, but the exercise of these rights 'shall be guided by the provisions of the [Code of Criminal Procedure], regardless of whether the data subject is a suspect, accused, victim, civil defendant, third party, witness or any other person'.[199] Therefore, depending on the approach taken by the national legislator when implementing the LED, references to national law like those found in Article 45(2), subparagraph 2 of the Regulation stating that 'access to the case file by suspects and accused persons as well as other persons involved in the proceedings shall be granted by the handling [EDP] *in accordance with the national law of that Prosecutor's Member State*',[200] may also be relevant and need to be taken into consideration when determining the scope of data subjects' rights.

Furthermore, national law may also apply to complement the rules of the Regulation, even when there is no reference to national law, provided that the more specific provisions of national law 'do not go against the overarching data protection regime'.[201] For instance, as explained when presenting the time limits for storage of operational personal data (*supra*, Part IV, Chapter c), the German legislator considers that specific national rules on data storage and deletion regarding, e.g., undercover measures, complement the rules laid down in Article 50(1) of the Regulation.[202]

In view of potential conflicts of laws, Article 5(3) of the Regulation confirms the primacy of EU law. Whenever a matter is dealt with by the Regulation, these rules will prevail. National law applies when this is not the case *or* to supplement the rules of the Regulation. While this should, in principle, resolve any potential conflicts between the Regulation and national law, it may in practice not always be easy to determine the exact scope of national law (e.g. 'where relevant') and whether national law complements the Regulation or rather unduly restricts its scope of application (i.e. 'goes against' the Regulation's data protection rules) (see also *supra*, Part IV, Chapter c). This may lead to diverging interpretations at Member State level.

---

[198] *Unofficial translation of Article 37, § 4 of the Belgian Act implementing the LED. Emphasis added. This legislative choice was consciously made to reduce the tensions between data protection law and criminal procedure. See Y. Liégeois and F. Bleyen, "Na een schijnhuwelijk en een schijnscheiding thans een gedwongen opname? Of de (uitoefening van de) rechten van de natuurlijke persoon bij de verwerking van diens persoonsgegevens in het strafproces", op. cit., p. 4.*

[199] *§ 15²(3) of the Estonian Code of Criminal Procedure. By means of an example, the Explanatory Memorandum to the Bill implementing the LED (available at: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5c9f8086-b465-4067-841e-41e7df3b95af) refers to the situation where a witness's right to access to his or her personal data needs to be limited or delayed in order not to prejudice the ongoing criminal investigation.*

[200] *Emphasis added.*

[201] *European Commission, Draft minutes, Ninth meeting of the EPPO Expert Group, 21 March 2019, p. 5.*

[202] *Explanatory Memorandum to the German Bill on the EPPO, p. 40.*

In addition, in some instances, the relationship between EU and national law may be complicated by the fact that the Regulation refers to national law without clearly defining the extent to which national law applies. This is notably the case for the rules that apply to the 'case file' (*supra*, Part II, Chapter c, Section 1). Article 45(2), subparagraph 1 of the Regulation states that 'the case file shall be *managed* by the handling [EDP] in accordance with the law of his/her Member State'.[203] The legal meaning of the term 'manage' ('géré' in the French version, 'gestionado' in Spanish, 'geführt' in German) is not entirely clear. Does this only refer to the rules concerning the practical organisation and storage of the case file, or may it also include, e.g., rules on time limits for data storage? When speaking to certain Member State negotiators,[204] they indicate having a broad interpretation in mind at the time of drafting the EPPO Regulation, i.e. including the national rules on data protection, as Member States wanted to reinforce the decentralised structure of the EPPO. Yet, this interpretation would lead to the questionable situation where only the operational personal data processed in the CMS would be subject to the EPPO data protection regime, whereas those in the case file would be governed by national data protection law, even though the CMS and the case file are both in hands of the same data controller (see *supra*, Part IV, Chapter c).

In what follows, we will first give a presentation of the theoretical interplay between the EPPO data protection rules on the one hand, and the LED and its national implementations on the other hand. In the next Part, we will then analyse different scenarios on the organisation of data flows between the EPPO and the national level, and their data protection implications in order to define the responsibilities of the EPPO and Member State authorities with regard to the processing of operational personal data in the context of the EPPO's activities.

5.2. Theoretical interplay between the EPPO data protection regime, the LED and its national implementations

As said, the EPPO Regulation establishes a 'standalone' data protection regime. Nonetheless, it is important to emphasize that many data protection provisions of the EPPO Regulation are actually identical or largely identical to the corresponding provisions of the LED. A major consideration that played in favour of modelling the EPPO Regulation's provisions on data protection on those contained in the LED was the fact that the LED, or rather national laws implementing it, will apply to national judicial and law enforcement authorities which the EPPO will closely collaborate with in the investigation and prosecution of EPPO offences and thus will frequently exchange data with.

---

[203] *Emphasis added.*
[204] *Interview with M.-H. Descamps; interviews with N. Franssen.*

This approach would therefore help reduce the divergences between the data protection regime applicable to the EPPO and the one applicable to national authorities.[205]

Nevertheless, when implementing a Directive, Member States dispose of some margin of appreciation allowing them take into account their specific national characteristics which may lead to discrepancies. The wording of the LED, in several instances, allows Member States to decide whether or not to implement some provisions. For instance, Articles 15(1), 13(3) and (4) of the LED provide that Member States 'may adopt legislative measures'. Furthermore, not all Member States have correctly or completely transposed the LED (*supra*, Part I, Chapter b).

To identify potential conflicts or gaps between the data protection provisions contained in the Regulation and those provided by the LED and national implementing laws, we will compare the first two legal instruments and illustrate certain issues by means of examples drawn from the national law of the selected Member States.[206]

Our analysis will focus on **three specific areas**: data subject rights (1.), processing of special categories of operational personal data (2.), and transfers of operational personal data (3.).

5.2.1. Data subject rights (Articles 57 to 62 of the Regulation)

The Regulation provides data subjects with rights allowing them to exercise their fundamental right to data protection. Similar to the LED, the Regulation grants data subjects the rights to information (Article 58), access (Article 59), rectification or erasure of operational personal data and restriction of processing (Article 61), and the right to exercise all of the aforementioned rights through the supervisory authority, i.e. the EDPS (Article 62). The Regulation also specifies certain modalities regarding the exercise of these rights (Article 57) and establishes limitations to these rights. The DP Rules adopted by the EPPO College further implement these provisions by providing detailed rules specifying the practicalities of the exercise of the rights of the data subject.[207] While data subjects enjoy the same categories of rights under the LED and the Regulation, the applicable procedures for the exercise of these rights and the limitations thereof may differ somewhat

[205] *H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 456-457.*
[206] *It is important to emphasize that our analysis of the implementation of the LED is not meant to be exhaustive. Our goal is to offer an illustrative overview of certain issues that may arise in some Member States participating in the EPPO.*
[207] *Article 64(2)(a) of the IRP; Article 1(3) of the DP Rules.*

depending on the instrument and the national laws implementing the LED, as will be explained below.

5.2.1.1. Communication and modalities for exercising the rights of the data subject

Article 57 of the Regulation details a number of rules to be observed in the provision of information to and the communication with data subjects related to the rights set out in Articles 58 to 62 and 75 of the Regulation.[208] Data subjects' requests will be dealt with by different actors within the EPPO; most notably, the DPO and the EDP handling the case concerned will play a central role. The former will coordinate the requests for exercising the right of access and provide a reply to data subjects.[209] He/she will also liaise with the competent EDP when dealing with requests for rectification or erasure of operational data[210] and requests for right of access.[211] The EDP, for his/her part, will give information to the data subject in line with Article 58 of the Regulation.[212] Without prejudice to the powers of the DPO under Article 79(4) of the Regulation, the EDP will also decide whether or not to grant the right of access[213] and whether operational personal data shall be rectified, erased or its processing restricted.[214]

With respect to the time limit to follow up on the data subject's request, the LED simply states that the 'Member State shall provide for the controller to inform the data subject in writing about the follow up to his or her request *without undue delay*',[215] whereas the Regulation adds that this must done 'in any case *at the latest after 3 months* after receipt of the request by the data subject'.[216] In accordance with Article 5(3) of the Regulation, if national law provides a different time limit, the Regulation will prevail. Therefore, the insertion of such a time limit is welcomed in the context of the EPPO in order to streamline 22 potentially different national approaches.[217] Furthermore, it may be noted that, with regard to the right of access (see *infra*), Article 5(6) of the DP Rules provides for a shorter internal time limit. It specifies that the EDP 'shall provide his/her decision to the

---

[208] *H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 491.*
[209] *See Articles 5(2), (3), (4), (5) and (7) of the DP Rules.*
[210] *See Article 6(3) of the DP Rules.*
[211] *See Article 5(5) of the DP Rules.*
[212] *Article 4(1) of the DP Rules. If there is no EDP assigned to the file, the competent EP shall deal with the request (Article 4(2) DP Rules). When there is neither a supervising EDP nor a competent EP, the ECP shall deal with the request (Article 4(3) DP Rules).*
[213] *Article 5(5) of the DP Rules read in conjunction with Article 5(7) of the DP Rules.*
[214] *Article 6(3) of the DP Rules.*
[215] *Article 12(3) of the LED. Emphasis added.*
[216] *Article 57(3) of the Regulation. Emphasis added.*
[217] *In a study conducted in 2020 concerning eleven EU Member States (Belgium, Cyprus, France, Greece, Ireland, Italy, Luxembourg, Malta, the Netherlands, Portugal and the United Kingdom), researchers found that it took, on average, three to sixty-one days for the competent national authority to reply to a data subject request, except for Luxembourg which took six months to reply. See P. Vogiatzoglou, K. Quezada Tavárez, S. Fantin and P. Dewitte, "From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives", JIPITEC, 2020, p. 496, para. 78.*

[DPO] within a reasonable period of time, and in any event, *no later than 2 months after the receipt of the request*'.[218] This leaves the DPO with another month to reply to the data subject's request.

5.2.1.2. Rights of information and access[219]

Concerning the **information** to be made available or given to the data subject, the list provided in the Regulation is identical to the list contained in the LED.[220] With regard to the **right of access**, Article 14 of the LED and Article 59 of the Regulation are both phrased in a way which implies that the data subject has the right to obtain directly from the controller positive or negative confirmation of the processing of his/her personal data.[221] In positive cases, this includes the access to the said personal data and the communication of different categories of information to the data subject.[222]

The right of information and the right of access are, obviously, not absolute. Indeed, if these rights were to be exercised to their fullest extent, this would undermine much police and criminal justice work.[223] Both the LED and the Regulation provide grounds to delay, restrict or omit, wholly or partly, the provision of information to the data subject under certain conditions as well as grounds to restrict, wholly or partly, the data subject's right of access.[224] **Limitations** may apply only for as long as it constitutes a necessary and proportionate measure, and due respect has to be taken of the fundamental rights and legitimate interests of the data subject. Hence, any limitation should be compatible with the EU Charter of Fundamental Rights.[225] The restriction should also pursue at least one legitimate ground, namely: avoiding to obstruct official or legal inquiries, investigations or procedures; avoiding to prejudice the prevention, detection, investigation or prosecution of

---

[218] *Emphasis added.*
[219] *For an overview of the exercise of the right of access under the LED in eleven Member States, see P. Vogiatzoglou, K. Quezada Tavárez, S. Fantin and P. Dewitte, "From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives", op. cit., p. 274-302.*
[220] *Article 16(1) and (2) of the LED and Article 58(1) and (2) of the Regulation.*
[221] *Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), op. cit., p. 16; D. Dimitrova and P. De Hert, "The Right of Access Under the Police Directive: Small Steps Forward", in M. Medina et al. (eds), Privacy Technologies and Policy: 6th Annual Privacy Forum, APF 2018, Springer, 2018, p. 123.*
[222] *See Article 14 of the LED and Article 59 of the Regulation.*
[223] *P. De Hert and V. Papakonstantinou, "The New Police and Criminal Justice Data Protection Directive: A First Analysis", op. cit., p. 12.*
[224] *See Article 58(3) of the Regulation for the right to information and Article 60 for the right of access.*
[225] *P. De Hert and D. Dimitrova, op. cit., p. 121.*

criminal offences or the execution of criminal penalties; protecting public security; protecting of national security;[226] protecting the rights and freedoms of others.[227]

The DP Rules further specify that, prior to making the information available or giving it to the data subject, the EDP must assess whether any of these grounds exist under national procedural law *or* in the EPPO Regulation.[228] Article 58(3) of the Regulation must indeed be read in conjunction with Article 49(6) of the Regulation, requiring the EPPO to also take into account 'relevant' national procedural law when deciding to restrict data subject's rights.[229] This would include any national legislative measures taken in accordance with Article 13(4) of the LED, allowing Member States to determine categories of processing which may wholly or partly fall under any of the points listed in Article 13(3) of the LED. The latter provision contains the grounds and conditions to delay, restrict or omit the provision of the information to the data subject.[230]

The question is, of course, when national law is considered 'relevant'. According to the German legislator, national rules of criminal procedure containing specific information and disclosure obligations are to be applied. For instance, Sections 101(4) to (7) and 101a(6) of the German Code of Criminal Procedure must be observed in accordance with Article 49(6) of the EPPO Regulation.[231] These provisions contain obligations of notification relating to certain investigation measures. In contrast, the Estonian legislator simply emphasizes that the Regulation is directly applicable and takes precedence over national law, without identifying which particular rules of national law could potentially be relevant, thus leaving this up to the authorities which will have to apply the Regulation.[232]

---

[226] *The list of grounds under Articles 13 and 15 of the LED is largely identical to the list provided in Articles 58 and 60 of the Regulation, the only difference being that the EPPO Regulation adds 'Member States of the Union', while the LED simply refers to public security and national security. However, when referring to public security and national security, Articles 13 and 15 of the LED presumably mean 'of the respective Member State'. See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 494.*
[227] *See Articles 13(3) and 15(1) of the LED; Articles 58(3) and 60(1) of the Regulation.*
[228] *Article 4(1) of the DP Rules.*
[229] *See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 495.*
[230] *Ibid., p. 493.*
[231] *Explanatory Memorandum to the German Bill on the EPPO, p. 40.*
[232] *Explanatory Memorandum to the Estonian Bill on the EPPO.*

5.2.1.3. Rights of rectification or erasure and restriction of processing

The data subject has the right to obtain the **rectification of inaccurate personal data**[233] relating to him or her as well as the right to have **incomplete personal data completed**.[234] Whether the personal data should be considered incomplete and whether the data subject has the right to have them completed in any particular way will depend on the specific processing purposes.[235]

Concerning the **erasure** of personal data, Article 16(2) of the LED and Article 61(2) of the Regulation are structured in a two-fold way: the controller/the EPPO has the obligation to erase operational personal data under certain circumstances and this obligation is independent of a request by the data subject ('shall require the controller'/'the EPPO shall'), but the data subject is also provided with the possibility to specifically request the controller/EPPO to erase personal data ('provide for the right of the data subject'/'the data subject shall have the right'). Personal data must be erased where the processing infringes the provisions concerning the principles relating to processing, the lawfulness of processing (LED)/processing of operational personal data (Regulation), or the processing of special categories of (operational) personal data.[236] In addition, there may also be situations where operational personal data must be erased 'in order to comply with a legal obligation to which the EPPO is subject'.[237]

Both the LED and the EPPO Regulation provide for the possibility to **restrict processing**, instead of erasing the data, and under the same circumstances.[238] However, Article 61(4) of the Regulation has no equivalent in the LED.[239] It specifies two circumstances for which, even though processing has been restricted, data may still be processed: 'for the protection of the rights of the data subject or another natural or legal person who is a party of the proceedings of the EPPO' or for the purposes of evidence.

---

[233] *Some consider that, despite the wording of Article 61(1) of the Regulation, the obligation of the EPPO to rectify inaccurate personal data could nevertheless be considered to apply independently of a request made by the data subject. This interpretation would be in line with the 'accuracy principle' under Article 47(1)(d) and with Article 52(3) of the Regulation. It would also ensure that, in accordance with Article 52(1) of the Regulation, the EPPO does not transmit or make available inaccurate personal data. See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 501.*
[234] *Article 16(1) of the LED and Article 61(1) of the Regulation.*
[235] *Article 61(1), second sentence. See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 501-502.*
[236] *Article 16(2) of the LED refers to its Article 4, 8 and 10. Article 61(2) of the Regulation refers to its Articles 47, 49 and 55.*
[237] *Article 61(2) of the Regulation. Article 16(2) of the LED provides that Member States shall require the controller to erase personal data and provide for the right of the data subject to obtain the erasure of personal data 'where personal data must be erased in order to comply with a legal obligation to which the controller is subject'.*
[238] *Article 16(3) of the LED and Article 61(3) of the Regulation.*
[239] *This paragraph was inserted late in the course of negotiations in the Council Working Group on proposal of a delegation. It is inspired by the respective provision in Article 18(2) of the GDPR. See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 500.*

When these rights are restricted, Article 9 of DP Rules shall apply.[240] This provision implements an additional safeguard for data subjects by providing that the DPO must be involved in any decision restricting data subject rights or reviews thereof. Unless the DP Rules provide otherwise, the DPO is also allowed to give advice at his/her own initiative, or at the request of the party undertaking the restriction or review.[241]

5.2.1.4. Right of indirect access

While the right of direct access to the controller, as detailed above, is the rule, in case national law or the Regulation allows for limitations to the rights of information, access, rectification or erasure and restriction of processing, the data subject may also turn to the competent supervisory authority. This right of indirect access is provided in the LED as well as in the Regulation.[242]

It should be noted that granting data subjects the right of direct access, unless a restriction applies, represents a departure from previous practice.[243] Some Member States, such as Belgium, have, however, not completely embraced this approach. While Articles 37 to 39 Belgian Act implementing the LED establish a right of direct access, Article 41, subparagraph 1 of the Act permits derogations by authorising the rights to be exercised through national supervisory authorities.[244] With regard to databases belonging to the Belgian police, there is no right of direct access. Article 42 of the Belgian Act implementing the LED states that these rights are exercised through the supervisory authority, i.e. l'*Organe de contrôle de l'information policière*.[245] The same 'derogation' applies to the databases controlled by customs authorities.[246] In contrast, the Estonian Personal Data Protection Act provides that data subjects have the right to obtain a confirmation

---

[240] *Article 4(6), 5(14) and 6(5) of the DP Rules.*
[241] *Article 9(8) of the DP Rules.*
[242] *Article 17(1) of the LED and Article 62(1) of the Regulation.*
[243] *P. De Hert and D. Dimitrova, op. cit., p. 124. The authors refer to right of indirect access under Article 17(1) (a) of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters; Article 58 (1) and (2) of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II); Article 14 (1) and (2) of Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. Under these instruments, the right of access may be exercised through the national supervisory authority which may decide what and how information is to be communicated to the data subject.*
[244] *Whether or not such a derogation is in conformity with the LED is debatable.*
[245] *Belgian Act implementing the LED. Article 42 refers to the supervisory authority mentioned in Article 71 of the Act. See also P. Vogiatzoglou, K. Quezada Tavárez, S. Fantin and P. Dewitte, "From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives", op. cit., p. 290, para. 53.*
[246] *Article 43 of the Belgian Act implementing the LED.*

from the controller[247] of the processing of their personal data.[248] However, as noted above, the exercise of this right may be restricted on the basis of Code of Criminal Procedure.[249]

5.2.1.5. Right to judicial review

Concerning the right to judicial review, contrary to the LED and the GDPR, the Regulation does not contain any general rule on the data subject's right to a judicial remedy against the controller or the processor.[250] While 'procedural acts' of the EPPO 'that are intended to produce legal effects vis-à-vis third parties' shall be subject to review by national courts in accordance with Article 42(1) of the Regulation, this does not apply to EPPO decisions that affect data subjects' rights. Indeed, Article 42(8) of the Regulation provides that data subjects may seek judicial review by the CJEU in accordance with Article 263(4) TFEU of EPPO decisions 'that affect data subjects' rights under Chapter VIII'. Besides, some provisions of the Regulation do explicitly refer to the possibility for data subjects to seek judicial review against the EPPO's decision, e.g. in case of limitation to the right of access.[251]

5.2.2. Processing of special categories of operational personal data

Both the LED and the Regulation provide a specific regime for the processing of special categories of personal data, i.e. sensitive personal data. While both instruments specify that the processing of such data 'shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject',[252] the grounds for processing differ.

According to Article 55(1) of the Regulation, these may only be processed if they supplement other operational personal data already processed by the EPPO.[253] In other words, sensitive categories of operational personal data will not be processed by the EPPO without being associated with other operational personal data.

In contrast, Article 10 of the LED provides that processing of special categories of personal data is allowed on three grounds: where authorised by Union or national law; to protect the vital interests of the data subject or of another natural person; or where such processing relates to data which

---

[247] *In the context of criminal proceedings, the data controller is the body conducting these proceedings (i.e. courts, the public prosecutor's office and 'investigative bodies'). § 15²(2) and (6) and 16(1) of the Estonian Code of Criminal Procedure.*
[248] *§ 24(1) of the Estonian Personal Data Protection Act.*
[249] *See in particular § 15²(4)-(5) of the Estonian Code of Criminal Procedure.*
[250] *See Article 54 of the LED and Article 79 of the GDPR.*
[251] *Article 60(2) of the Regulation. See also H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 460-461.*
[252] *See Article 10(1) and Article 55(1) of the LED.*
[253] *A similar provision may be found in Article 30(2) of the Europol Regulation.*

are manifestly made public by the data subject.[254] In the selected national legal systems, the implementation of this provision appears to be quite faithful to the LED. For instance, the Estonian Personal Data Protection Act almost literally replicates the content of Article 10 of the LED.[255] Article 10 of the Romanian Act implementing the LED includes the three conditions with only a slightly different wording for the second condition: 'to prevent an imminent danger at least to the life, bodily integrity or health of the data subject or of another natural person'.[256]

Considering that many operational personal data of the EPPO will be gathered at national level through the intermediary of national authorities or obtained from national databases and registers, national law implementing the LED will in practice work as a filter. Next, before processing such personal data, the EDP will have to verify if these data are associated with other operational personal data to meet the requirements of Article 55 of the Regulation. Still, if one were to consider that national law applies to the case file (see *supra*, Part IV, Chapter c and *infra*, Part VI), then the differences between the grounds for processing would create a risk of dichotomy between what may be processed at national level and what is allowed to be processed in the CMS. Indeed, in that hypothesis, it is possible that more data could be processed in the case file at national level than in the EPPO CMS. Such an approach seems to be at odds with Article 45(3) of the Regulation, which imposes that the content of information in the CMS reflects the case file at all times.

5.2.3. Transfers of operational personal data to a third country or an international organisation

The LED and the Regulation establish **identical principles** for the transfer of personal data to a third country or an international organisation.[257] Both texts provide for transfers on the basis of an adequacy decision from the Commission.[258] In the absence of such a decision, transfers may take place where appropriate safeguards with respect to the protection of personal data are provided for in a legally binding instrument[259] or where the controller/EPPO has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate

---

[254] Article 10(1)(a), (b) and (c) of the LED.
[255] § 20(1) of the Estonian Personal Data Protection Act.
[256] Romanian Act No 363 implementing the LED. For Belgium, see Article 34, para. 1 of the Act implementing the LED, and for France, see Article 88 of the Act No 78-17 of 6 January 1978 relating to Information Technology, Files and Liberties.
[257] See Article 35(1) of the LED and Article 80(1) of the Regulation. It is worth noting that EU Member States not participating in the EPPO do not fall under the category of 'third country'. See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 537.
[258] Article 36 of the LED and Article 81 of the Regulation. So far, the Commission has not taken any adequacy decision in accordance with Article 36 of the LED. Hence, Article 81 of the Regulation cannot yet serve as a basis for the transfer of personal data by the EPPO. H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 541.
[259] Article 35(1)(d) of the LED read in conjunction with Article 37(1)(a); Article 80(1)(d) of the Regulation read in conjunction with Article 82(1)(a) of the Regulation.

safeguards exist with respect to the protection of personal data.[260]

In the absence of an adequacy decision or of appropriate safeguards, the Regulation and the LED both allow for the transfer of personal data if necessary and only in specific situations,[261] i.e. on a case-by-case basis. But the rules are not identical. On the one hand, the EPPO Regulation, contrary to the LED,[262] does not allow for the transfer of operational personal data in an individual case for the establishment, exercise or defence of legal claims relating to the task of the EPPO.[263] On the other hand, the Regulation provides for an additional safeguard that is not included in the LED with regard to transfer of data in individual cases. Article 83(1)(d) of the Regulation specifies that such transfer may take place, 'unless the EPPO determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer'.

With regard to **the personal scope of application** of transfers, Article 35(1)(b) of the LED read in conjunction with Article 1(1) indicates that transfers to third countries and international organisations are limited to authorities competent for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The personal scope of application of transfers under the EPPO Regulation is somewhat similar. Article 80(1)(b) of the Regulation refers to Article 104 which means that the EPPO may transfer operational personal data to the authority in a third country or international organisation competent to undertake judicial cooperation in criminal matters.[264]

As to the **conditions** for such transfers, the EPPO may transfer operational personal data only 'where this necessary for the performance of the tasks of the EPPO'.[265] The reference to the 'tasks of the EPPO' does raise the question as to whether the EPPO may transfer personal data where it serves the purposes of the receiving authority rather than the investigation or prosecution conducted by the EPPO. Some authors consider that this reference should be interpreted broadly and allow for transfer of personal data by the EPPO where such transfers serve the purpose of the receiving authority in the third country or international organisation, as implied in Article 104(6)

---

[260] *Article 35(1)(d) of the LED read in conjunction with Article 37(1)(b); Article 80(1)(d) of the Regulation read in conjunction with Article 82(1)(b) of the Regulation.*
[261] *Article 38(1) of the LED and Article 83(1) of the Regulation.*
[262] *Article 38(1)(e) of the LED.*
[263] *There is no ground (e) in Article 83(1) of the Regulation.*
[264] *See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 538.*
[265] *Article 80(1)(a) of the Regulation.*

of the Regulation.[266]

Although the provisions of the Regulation on data transfers do not refer to **national law**, national law may nevertheless be relevant in some instances. As explained in Part IV, Chapter d, national law may limit the purposes for which the EPPO is allowed to process the data collected in the Member State concerned, not only for the EPPO's own investigations and for the information exchange with other Member States and EU institutions, bodies, offices and agencies, but also for the cooperation with third countries and international organisations.[267] Such national processing limitations[268] will thus have to be respected when transferring data to third countries or international organisations based on Articles 80-83 of the Regulation.

Furthermore, both the Regulation and the LED regulate the direct transfer of personal data to **recipients** (i.e. other persons than the above competent authorities)[269] established in third countries; the procedural conditions for such transfer are the same.[270] The Regulation, contrary to the LED,[271] does however not provide that the supervisory authority (i.e. the EDPS) shall be informed of the transfer. Rather, the transfer shall be documented and the document 'shall be made available to the EDPS on request'.[272]

Where personal data to be transferred have been **transmitted or made available by a Member State**,[273] the EPPO shall, in principle, obtain prior authorisation for the transfer, unless that Member State 'has granted this authorisation to such transfer in general terms or subject to specific conditions'.[274] Nevertheless, the LED and the Regulation both allow for transfers without the prior authorisation by another Member State, though 'only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State [of the EU] or a third country or to essential interests of a Member State [of the EU] and the prior authorisation cannot be obtained in good time'. In this scenario, the authority that should

---

[266] *See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 538. The authors are of the opinion that transfers should not be limited to investigations concerning EPPO offences.*
[267] *Article 49(1)(a)-(c) of the Regulation.*
[268] *One may recall the aforementioned example of Article 479(1)-(3) of the German Code of Criminal Procedure.*
[269] *Article 2(15) of the Regulation and Article 3(10) of the LED.*
[270] *See Article 84 of the Regulation and Article 39 of the LED.*
[271] *Article 39(3) of the LED.*
[272] *Article 84(3) of the Regulation.*
[273] *The wording 'by a Member State' in Article 80(1)(c) of the Regulation (as opposed to 'from a Member State' in Article 35(1)(c) of the LED) was intended to clarify that the provision applies only where a competent authority of a Member State has transmitted or made available the data to the EPPO. In other words, this provision does not cover personal data directly obtained by the EPPO in the course of its investigation measures on the territory of a Member State, e.g., by way of a house search. Presumably, the provision applies where a national authority transmitted personal data when reporting to the EPPO in accordance with Article 24 of the Regulation. See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 538-539.*
[274] *Article 80(1)(c) of the Regulation.*

have given prior authorisation is informed without undue delay.[275]

Furthermore, both the LED and the Regulation authorise **onward transfers**, but the conditions differ. Under Article 80(3) of the Regulation, the transfer of operational personal data received from the EPPO to a third country or an international organisation by a Member State or an EU institution, body, office or agency is prohibited, unless the EPPO has authorised such transfer 'after taking into due account all relevant factors'. Under the LED, onward transfers are allowed 'subject to compliance with the national provisions adopted pursuant to other provisions of the [LED] and only where the conditions laid down in [Chapter V of the LED] are met'.[276]

[275] *Article 35(2) of the LED and Article 80(2) of the Regulation.*
[276] *Article 35(1) of the LED.*

6. Data flows and the concrete interplay between the EPPO data protection regime and national law

6.1. Introduction: A hybrid EU body relying on the cooperation of national authorities

The inclusion of several references to national law in the EPPO Regulation is not the only reason for the interplay between the EPPO data protection regime and national law. The **continuous flows of information** between the EU level and the national level will inevitably result in data being collected, processed and stored at different levels, by a variety of authorities. How exactly these flows will be organised and where the exchanged data will be stored, does not seem entirely clear at this point. The least one can say, is that there were, and still are, diverging points of view among the different stakeholders (EPPO,[277] European Commission, Member States), ranging from a strongly EU approach to a much more hybrid model with a substantial national component.

In this part of the study, we will first examine more thoroughly the EPPO case file and the relation it bears to the e-case file, in order to determine which rules – the EPPO Regulation or national law – apply to the operational personal data they process. Then, we will consider how the data flows between the EU and the national level may be organised, as well as the respective roles and responsibilities of the EPPO and national authorities regarding the processing of operational personal data in the context of the EPPO's activities. This step in the analysis is crucial for the next one, which consists in delineating the EDPS's supervisory role.

6.2. The EPPO case file and applicable law

As explained earlier (Part II, Chapter c, Section 1), the EPPO Regulation distinguishes between the 'case file' of the EPPO[278] and the CMS, which contains a register, an index and the e-case file.[279] The latter should at all times reflect the case file.[280] The case file is opened and handled by the EDP and 'shall be managed (...) in accordance with the law of his/her Member State'.[281] Despite these seemingly simple rules, their practical application raises a lot of questions, which go to the heart of the EPPO's hybrid nature. In the run-up to the establishment of the EPPO, and even today,

---

[277] The viewpoints of the EPPO presented below are based on the decisions of the College, supplemented with information obtained during the interviews with the EPPO Legal Service. Given that the EPPO is still in the setup process and the completion of this study took several months, some views may have evolved in the meantime.
[278] Article 45 of the Regulation.
[279] Article 44(4) of the Regulation.
[280] Article 61(6) of the IRP.
[281] Article 45(2), subpara. 1 of the Regulation.

there is quite some controversy as to where and how the EPPO case file will actually be stored, what data it will contain, what its relation to the e-case file exactly is and, most importantly, which rules will apply to it. Different, even diametrically opposite points of views have been expressed.

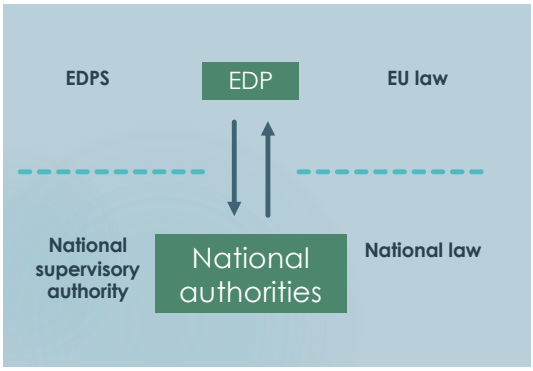
In the analysis below, these different positions will be reflected and taken into consideration – a well-considered approach that calls for a methodological explanation. Indeed, as indicated (*supra*, Part I, Chapter b), the decisions of the EPPO College and underlying considerations will be determining for the first EPPO investigations and give direction to the application of the EPPO Regulation, especially in areas where the rules of the Regulation and their interaction with national law are not crystal-clear. The way in which this new EU body interprets and applies the legal framework will thus, without any doubt, be highly important. Nevertheless, in certain respects, the position of the EPPO may still evolve over time as this body is very much aware of national diversity in terms of criminal procedure and judicial organisation.[282] In particular, the relation between the e-case file, stored in the CMS, and the case file, stored at national level, which is at the heart of many questions regarding data protection as the analysis in previous parts of this study has shown, is not set in stone. Neither is the way in which national authorities will in practice cooperate and exchange information (or data) with the EPPO, and their respective responsibilities, as will be discussed in this Part. Rather than taking firm stances, the EPPO seems to privilege a pragmatic approach and an openness toward the Member State rules and practices, which, considering the unprecedented nature of this new EU judicial body and the complexity of the applicable legal framework, is definitely a welcome approach. Furthermore, the ultimate guarantor of the correct and uniform interpretation and application of the EU legal framework is, of course, the Court of Justice. Most probably, this Court will be invited to rule on several aspects of the Regulation in the years to come. Therefore, despite the institutional weight of the EPPO's position, the viewpoints of the other stakeholders (Commission, Member States) remain relevant and need to be included in the analysis below.

For a start, the **European Commission** has advocated, even after the adoption of the Regulation, that there 'should be *one single case file* to avoid legal uncertainty' and that it 'should be held by the EPPO in the EPPO CMS'.[283] Still, in line with Article 45(2) of the Regulation, the Commission also acknowledges that the 'file should be managed by the EDP under national law and the

[282] *As emphasised by Recital 15, the Regulation 'is without prejudice to Member States' national systems concerning the way in which criminal investigations are organised'.*
[283] *European Commission, Draft minutes, Seventh meeting of the EPPO Expert Group, 10 December 2018, p. 4. Emphasis added.*

[IRP]'.[284] This approach seems to suggest that the information gathered at national level, in connection with the EPPO case, should be deleted after it has been transmitted to the handling EDP. Indeed, in some documents, the Commission has advocated that 'operational data [should be] stored in the EPPO CMS at central level', while only 'reference data' or 'case identification data' should be kept 'in the national systems'.[285] If this approach were followed, the data processed and stored at national level would be limited and would basically only exist by reference to the EPPO case. Consequently, since there would only be one case file, stored in the CMS, it is quite obvious that the EPPO data protection regime would apply all the way through, unless of course the EPPO Regulation refers to national law or the latter supplements the rules laid down in the Regulation (see *supra*, Part IV and Part V).

Figure 3. 'One-case-file' approach



This approach raises a number of questions, though. First, it is hard to see how this 'one-case-file' approach (see Figure 3) with minimal data storage at national level (even by the EDP) can be reconciled with the requirement of Article 45(3) of the Regulation that the e-case file in the CMS must at all times reflect the case file. Second, one may wonder whether this strongly European model is workable in practice. It would complicate the work of national authorities as they would conduct an investigation without being able to keep trace of the results of previous investigation measures. Indirectly, this could also hamper the EPPO investigation as (experienced) national authorities would not be able to establish useful links between the various parts of the investigation, or even other investigations at national level. Imagine, for instance, that the police would have to delete every report each time they have questioned a suspect or a witness in the context of an EPPO investigation. This would imply that they would have to start 'from scratch'

[284] *Ibid.*
[285] *European Commission, Draft minutes, Ninth meeting of the EPPO Expert Group, 21 March 2019, p. 3-4.*

each time they receive a new instruction from the EDP, even though they have been involved in the investigation before.

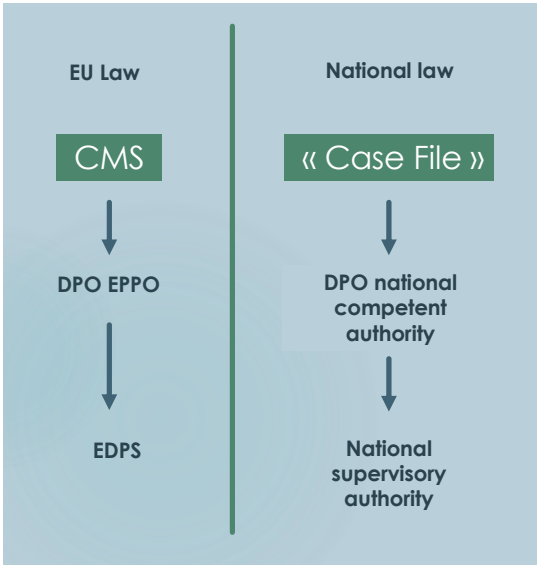
The Commission's approach notably differs from the positions adopted by the **Member States**. As explained, during the negotiations of the Regulation, Member States had in mind a broad interpretation of the reference to national law in Article 45(2), subparagraph 1 of the Regulation, in an attempt to keep control of the EPPO case files.[286] According to authors who were involved in those negotiations, the proposal to consider 'case files' to be a component of the CMS was not taken up.[287] After the adoption of the EPPO Regulation, this point of view was reiterated in the EPPO Expert Group, where some Member States expressed the opinion that, in their view, 'the criminal case file is kept by the EPDs outside of the CMS and the CMS is to contain "information from the case file" rather than the case file itself'.[288] Put differently, the Member States regard the case file as the original file, the e-case file as the copy. What this means in terms of applicable law today, is not entirely clear as few legislators have reflected on this issue when adjusting their national legislation for the arrival of the EPPO. Will they stick to their initial broad interpretation of the reference to national law, or not? The German legislator seems to adopt a narrower approach, according to which Article 45(2) of the Regulation relates to national (i.e. federal and regional) provisions on the creation, management and storage of case files.[289] Still, it is unsure what legislation the EDPs of the various participating Member States will apply when the EPPO will launch its operational activities.

Similarly, the **EPPO** adheres to the idea of two files, the 'e-case file' which is stored in the EPPO CMS and the 'case file' which is handled at national level.[290] The case file kept at national level is considered to be the original file, essential to the daily functioning of the EPPO investigation, whereas the e-case file constitutes a copy thereof (at least for all information that can be stored electronically)[291] 'to ensure that the EPPO can function as a single office'[292]. The case file may indeed contain certain elements that cannot be stored in the CMS (e.g. seized goods). In accordance with the Regulation, the 'case file' would be managed by the EDP in accordance with national law. The EPPO thus makes a clear distinction between the EU level and the national level (see Figure

[286] *Interview with M.-H. Descamps; interviews with N. Franssen.*
[287] *See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 444.*
[288] *European Commission, Draft minutes, Ninth meeting of the EPPO Expert Group, 21 March 2019, p. 3.*
[289] *Explanatory Memorandum to the German Bill on the EPPO, p. 37.*
[290] *Interviews with the EPPO Legal Service.*
[291] *Article 45(3) of the Regulation.*
[292] *Article 61(6) of the IRP.*

4). The EPPO only directly 'controls' the operational personal data stored in the CMS and thus is fully responsible for their processing. If that assumption were followed, consequently, one could posit that for the purposes of data protection, only the CMS would fall under the EPPO data protection rules; the case file at national level would resort under national law, including national data protection law. So, it seems the applicable law would be determined on the basis of the location of the storage of the operational personal data.[293]

Figure 4. 'Two-case-files' approach



Clearly, such an approach would be based on pragmatic considerations (e.g. who is in charge of ensuring compliance with the data protection rules and who is the best placed to exercise the supervision) and aims to respect as much as possible national diversity regarding criminal files, as this touches upon the way in which criminal investigations are organised in the Member States' national systems.[294]

There are indeed substantial differences in how Member States organise and store criminal files. In some Member States, the information may be stored in one single IT system.[295] In Estonia, for instance, a platform called X-Road connects all government information systems and core registers.

---

[293] *This would somehow reflect the EDPS reasoning according to which the competent supervisory authority should be determined depending on where the processing activity takes place (national or EU level). According to the EDPS, on the one hand, 'when the processing takes place on the territory of a Member State, the relevant data protection authority of that Member State should be competent for supervising the processing'. On the other hand, 'when data are processed at EU level, the appropriate EU data protection authority should exercise the supervision'. See Opinion of the EDPS on the package of legislative measures reforming Eurojust and setting up the European Public Prosecutor's Office ('EPPO'), adopted on 5 March 2004, para. 31.*

[294] *Recital 15 of the Regulation.*

[295] *Some Member States indeed pointed out that 'there is an integrated case file, set up by the police, administered the prosecution and used by the court'. European Commission, Draft minutes, Seventh meeting of the EPPO Expert Group, 10 December 2018, p. 3.*

This platform enables national authorities, e.g. police officers, to access data from different local and EU databases.[296] In such integrated systems, applying different data protection rules to the case file of the EPPO than to other case files concerning purely national investigations may be complicated (see also *supra*, Part IV, Chapter c); the option not to apply the data protection rules of the Regulation would thus be easier, not only for the EPPO, but also for the Member States. As a consequence, national supervisory authorities would be competent, which would also facilitate things as they are familiar with the national rules and the practical organisation of criminal investigations.

What is more, in many Member States, criminal files may also or even only exist on paper as not all criminal justice systems have been digitalised. In Germany, for instance, the case files will probably be kept as paper files as the obligation to maintain a digital case file will not enter into force until 2026.[297] In Belgium, criminal files are in the (slow) process of being digitalised. Even in Estonia, a criminal file may be maintained, in whole or in part, in digital form.[298] Should the EPPO data protection rules apply to such paper files, this would definitely complicate the EDPS's supervisory task as it is, at present, not equipped to conduct its supervision in 22 Member States.

Another position argued by certain authors seems to take a middle-ground between the approaches of the Commission and the EPPO. On the one hand, just like the EPPO, they consider the case file as the 'leading file' for the EPPO in conducting its investigations.[299] This case file will be kept at national level, separately from national case files, and will be under full control of the EDP who will 'manage' it in accordance with national law as provided by Article 45(2), subparagraph 1 of the Regulation. This implies the EPPO case file 'shall be kept either manually or electronically in the manner prescribed by the applicable national law'.[300] According to this interpretation, the reference to national law also involves national rules on the structure and necessary content of case files as well as procedural rules on the opening and keeping of the case files.[301] In contrast, the EPPO CMS will only contain an electronic 'copy' of the case file.[302] On the

---

[296] *Information received through exchanges with practitioners from Estonia.*
[297] *Sections 32 et seq. of the German Code of Criminal Procedure provide for optional electronic file management until the mandatory introduction of the electronic file on 1 January 2026.*
[298] *§ 160[1] (4) of the Estonian Code of Criminal Procedure.*
[299] *Hans-Holger Herrnfeld considers that this does not mean that the available evidence has to be physically made part of the case file. In accordance with national law, evidence may be stored outside of the actual case file such as in storage spaces or separate manual or electronic files, provided that the case file clearly refers to the existence of such separately stored evidence. See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 450.*
[300] *H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 450.*
[301] *Ibid.*
[302] *Ibid., p. 446.*

other hand, these authors draw a different conclusion as to the applicable law, which resembles more the Commission's approach. Indeed, notwithstanding the fact that the case file of the EPPO and its electronic 'copy' are stored at different levels, both will be regulated by the data protection rules contained in the EPPO Regulation.[303] The location of storage is thus not determining for the applicable rules.

In our view, this middle-ground position is most in line with the wording of the EPPO Regulation and the principles of data protection law, but also matches the intentions of the EU legislator and takes into consideration the practical functioning of a criminal investigation. The Regulation clearly refers to a case file and its electronic copy in the CMS,[304] the 'e-case file'. Both will contain (largely) the same operational personal data that are collected and processed for the purpose of EPPO investigations and prosecutions. Therefore, logically, the data controller seems to be in both cases the EPPO, through the intermediary of the EDP.[305] Consequently, the EPPO data protection regime laid down in the Regulation, including a number of references to national law, applies to both the case file and the CMS. We share the opinion that it would not be appropriate to have different data protection rules apply to the case file kept in the EDP's office, at decentralised level, than those that apply to the copy of that file contained in the EPPO CMS,[306] even if this has major implications for the exercise of the EDPS's supervisory tasks (see *infra*, Part VII). For sure, the EDP manages the case file in accordance with national law, but this reference to national law should be interpreted narrowly and hence restricted to the practical organisation of the case file: The case file is stored at national level, in a comparable way to national case files, using national infrastructures.

6.3. Data flows between the EPPO and national authorities

In this section, we will make a closer analysis of the data flows between the EPPO and national authorities, from the very start of the investigation to its termination.[307] Based on that analysis, we will subsequently, in Chapter d, try to identify which authorities are controllers, processors or mere

---

[303] *Ibid., p. 459.*
[304] *Articles 44(4) and 45(3) of the Regulation.*
[305] *As indicated, the EDP is also responsible for keeping the e-case file in the CMS up to date. Article 45(3) of the Regulation, Article 61(6) of the IRP.*
[306] *H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 459-460.*
[307] *The trial stage is not taken into account in this study as the control of the file then shifts to the competent national trial jurisdictions in accordance with national law. That said, the trial stage too raises a number of interesting questions, which would merit further analysis. For instance, even though national law applies to this stage, one may wonder it does not give rise to a situation of joint control. During trial, while the case file would be controlled by the national courts but, at the same time, the CMS would continue to contain the e-case file.*

recipients of operational personal data, in order to determine their respective responsibilities and the competent supervisory authorities.

As explained in Part IV, Chapter a, information collected by national authorities will be communicated to the EPPO in accordance with Article 24 of the Regulation, upon which the EPPO may decide to exercise its right of evocation.

Once an EPPO case has been opened, the **EDP** will play a **pivotal role**, not only in conducting the investigation, but also in the interaction with national authorities. Indeed, as explained in Part II, the EDP handling the case has the same powers as a national public prosecutor.[308] He/she can either undertake investigation measures on his/her own, or instruct national authorities to undertake them (e.g. the police, customs or other authorities), 'in accordance with the Regulation and with national law'.[309] Assuming the future EDPs will have a substantial workload, it seems very unlikely they will undertake many investigation measures themselves. Instead, they will rely heavily on the intervention of national authorities. Furthermore, it should also be noted that the Regulation contains very few minimum rules approximating national criminal procedure. It only requires that the EDP has a number of investigation measures in his/her 'tool box'.[310] But the applicable procedures are defined by national law. When national law requires the authorisation of a judge, the EDP will therefore have to *request* the competent national pre-trial judge to authorise the measure, before proceeding.[311] Several national authorities will thus be involved throughout the EPPO investigation and will communicate with the EDP on a regular basis.

In other instances, the EDP will not require national authorities to collect new data, but to transmit relevant data that are stored in national databases or registers – systems to which the EDP does not necessarily have direct access. Indeed, it is worthwhile pointing out that, in accordance with Article 43(1) of the Regulation, the handling EDP has the right 'to *obtain* any relevant information stored in national criminal investigation and law enforcement databases, as well as other relevant registers of public authorities *under the same conditions as those that apply under national law in similar cases*'.[312] In other words, the Regulation does not require that the EDP has *direct access* to

---

[308] *Article 13(1) of the Regulation.*
[309] *Article 28(1) of the Regulation.*
[310] *Article 31 of the Regulation.*
[311] *Article 30(1) of the Regulation. On the relationship between the EPPO and national pre-trial judges, see A.L. Claes, A. Werding and V. Franssen, "The Belgian Juge d'Instruction and the EPPO Regulation: (Ir)reconcilable?", European Papers, forthcoming 2021, 36 p.*
[312] *Emphasis added.*

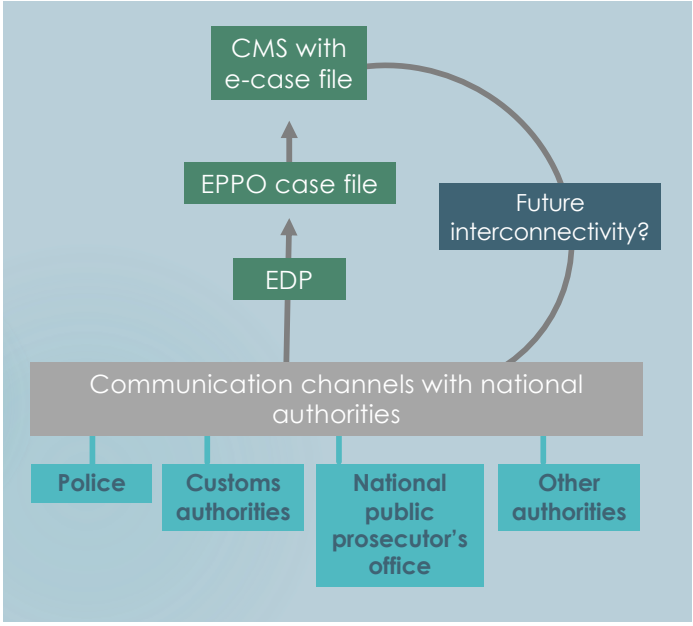
those databases. Only if national law grants direct access to the databases to national public prosecutors, the EDP will have such access which will, for instance, be the case for Estonian EDPs.[313] In all other cases, he/she will have to request the competent national authority to transmit the information.[314]

The documents (orders, requests, etc.) **communicated** to the national authorities and their replies (including the results of the investigation measures they conduct) will not be transmitted through the CMS as national authorities have no access to it (*supra*, Part IV, Chapter e). Instead, the European Commission has clarified that '[t]he EDPs would continue to use their national software and communication infrastructure to communicate with national authorities, e.g. when a house search needs to be conducted, the national system would be used to prepare such a request and send it to the appropriate national authority as required'.[315] In this respect, there would be no difference between an EDP communicating with the police and a national public prosecutor doing so. Moreover, '[a]ll means currently available and used at national level (e.g. public files used by lawyers to submit appeals to court) would continue to be used in the same way'.[316] This approach (see Figure 5) has also been defended by national authorities as they fear a multiplication of parallel systems, which would complicate their work on a daily basis.[317] Moreover, the creation of new exclusive communications tools (IT systems, databases) would also be costly. That said, in the future, it would probably be desirable to ensure interconnectivity between the national systems and the CMS to facilitate the exchange of information.[318]

---

[313] *According to the survey submitted by the authors of this study to academics and practitioners from Estonia, the Estonian EDPs enjoy the same powers as national prosecutors, hence they will have direct access to national databases and registers.*
[314] *This view is shared by H.-H. Herrnfeld who considers that the possibility for the EDP 'to obtain' the information may also be fulfilled by providing for procedures under which a search request issued by an EDP is processed and answered by the respective national public authority. See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 442.*
[315] *European Commission, Draft minutes, Seventh meeting of the EPPO Expert Group, 10 December 2018, p. 3.*
[316] *Ibid.*
[317] *Interview with the Belgian federal and local police.*
[318] *Interconnectivity is, however, a very complex issue and far from obvious considering the diversity of national legal systems. It requires, first of all, a thorough mapping exercise to understand the specific needs and obstacles. At this stage, one has only just started to explore the possibilities in this area. Interview with the EPPO Legal Service. See also Expert EPPO Group, Minutes VTC Meeting, 24 April 2020, p. 4.*

Figure 5. Communication with national authorities



6.4. Roles and responsibilities of the EPPO and national authorities

In light of the aforementioned data flows, it is crucial to determine the **role** of each actor when processing operational personal data. This is important to define their respective **responsibilities**, as well as the competent **supervisory authorities**.

National authorities may be mere processors or rather controllers of the data they receive from, collect for (new data) or transmit to (pre-existing data) the EPPO. A controller is 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purposes and means of the processing* of personal data',[319] whereas a processor is 'a natural or legal person, public authority, agency or other body which processes personal data *on behalf of* the controller'.[320] Put differently, two basic conditions are required for qualifying as processor: being a separate entity in relation to the controller and processing personal data on the controller's behalf.[321] The processor's role stems from the concrete activities of an entity processing data in a specific context, not from the nature of such entity.[322] When a controller transfers personal data to

[319] *Article 4(7) of the GDPR and Article 3(8) of the LED. Emphasis added.*
[320] *Article 4(8) of the GDPR and Article 3(9) of the LED. Emphasis added.*
[321] *European Data Protection Board, Guidelines 07/2020, op. cit., p. 24, para. 74.*
[322] *Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', adopted on 16 February 2010, p. 25.*

another entity, this entity is a recipient which shall be considered a controller for any processing that it carries out for its own purposes(s) after it receives the data.[323]

Whether national authorities are controllers[324] or processors[325] in the context of the EPPO's activities, thus depends on whether they merely process the data on behalf of the EPPO or whether they also determine the purposes and means of the data processing. Even if, ideally, the law determines which authority is the controller, the attribution of this role is usually based on a factual assessment of the powers and autonomy of the authority concerned.[326]

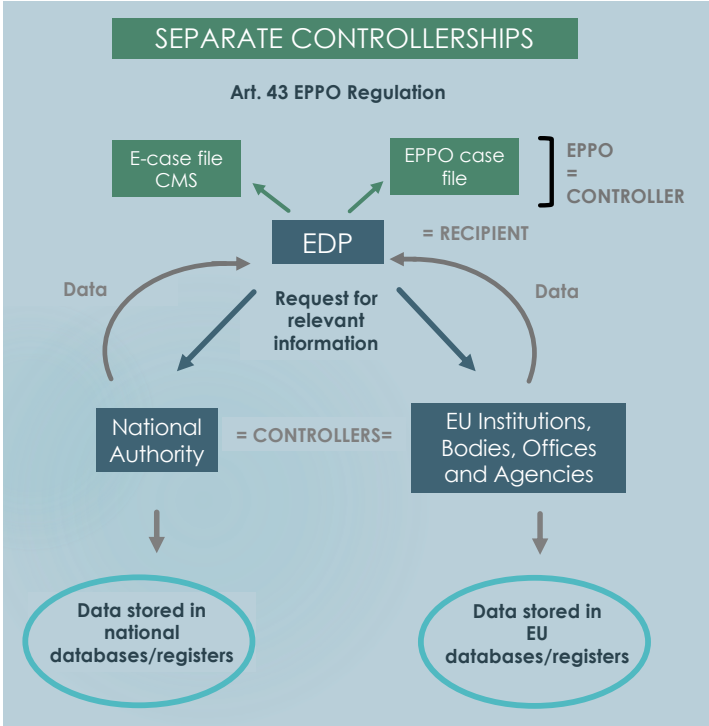
In the context of the data flows between the EPPO and national authorities, one may distinguish **different possible scenarios**.

A **first scenario** is the one where the EDP obtains **pre-existing data** from national authorities (e.g. police or custom authorities), either upon his/her request[327] or spontaneously.[328] In that case, the EDP is to be considered a recipient while national authorities are controllers. Once the EDP processes the data **for the purpose of the EPPO investigation**, the EPPO becomes the controller of the said data.[329] This scenario would have for consequence that the national authorities and the EPPO are **separate, consecutive controllers** (see Figure 6). The same analysis could be made for data received from EU institutions, bodies, offices and agencies, and even data handed over by private parties.

---

[323] Under the GDPR, the term 'recipient' covers anyone who receives personal data. European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, adopted on 2 September 2020, para. 90, p. 29.
[324] Defined in Article 2(13) of the Regulation.
[325] Defined in Article 2(14) of the Regulation.
[326] European Data Protection Board, Guidelines 07/2020, op. cit., para. 20, p. 10; Belgian Data Protection Authority, Opinion No 77/2020, op. cit., para. 28, p. 9.
[327] Article 43(1) of the Regulation, Recital 53 of the Regulation.
[328] Article 24(2)-(3) of the Regulation, Recital 49 of the Regulation.
[329] As underlined by the EDPB, a recipient of personal data 'may well simultaneously be regarded as a controller or processor from other perspectives'. European Data Protection Board, Guidelines 07/2020, op. cit., p. 27.

Figure 6. Separate controllerships



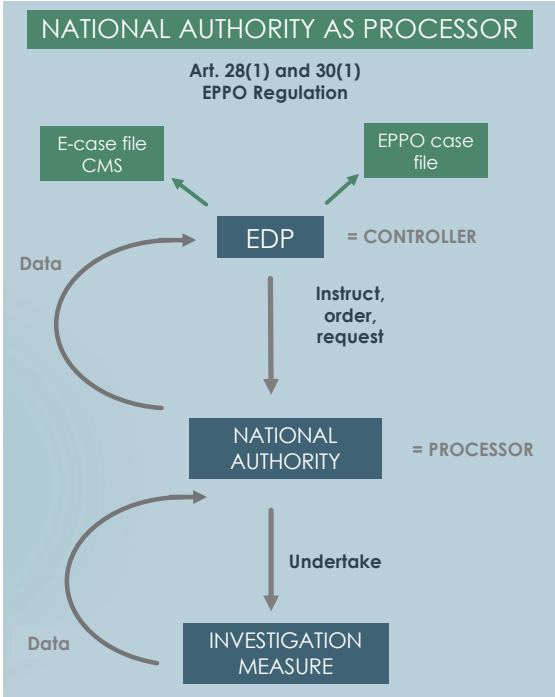
In a **second scenario**, the EDP instructs, orders or requests a national authority to undertake an investigation measure.[330] The latter will then process the data it received from the EDP and collect new ones for the purpose of the EPPO investigation, and subsequently will transmit them to the EDP. In this case, the **national authority** is clearly a **processor**, carrying out processing activities on behalf of the EPPO which determines the purposes and means of the processing of personal data.[331] In sum, the processor essentially processes the data as an extended arm of the controller.[332] This scenario was also suggested during the negotiations on the EPPO Regulation in the Council Working Group.[333]

Being processor is not without consequences. Processors have obligations in terms of security and confidentiality.[334]The processor's activity is regulated by Article 65 of the Regulation.

---

[330] *See Articles 28(1) and 30(1) of the Regulation.*
[331] *It should be noted that national authorities other than those falling under the scope of Article 3(7) (a) of the LED do not qualify as 'recipient' and must process data received from the EPPO 'in compliance with the applicable data protection rules according to the purposes of the processing'. See Article 2(15) of the Regulation.*
[332] *H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 511.*
[333] *Ibid.*
[334] *See Article 65(1) and (3)(b) of the Regulation.*

Figure 7. National authority as processor



These are the two most straight-forward scenarios, in which cases the respective roles of the EPPO and the national authorities can be well delineated. When the EPPO is the controller, the EDPS will be the competent supervisory authority. For the second scenario, due to the fact that EDPs will act on behalf of the EPPO when processing data in the case file,[335] the EPPO retains controllership of the data and the EDPS is the supervisor, regardless of the fact that data will be processed at national level and even if this has far-reaching practical consequences (see *infra*, Part VII). To the extent national authorities are autonomous controllers, they are supervised by the competent national supervisory authorities.

However, there may be **situations where the division of roles is less clear**. For instance, as explained above (Chapter b), it is unlikely that national authorities will delete the data processed on behalf of the EPPO after having transmitted them to the EDP as they will continue to be involved in the investigation. The data received from the EPPO and/or collected for the EPPO investigation and stored in national databases and systems could also be used for other law enforcement activities or criminal investigations,[336] and with respect for any specific conditions for processing imposed by the EPPO in accordance with Article 53(1) of the Regulation. To the extent

[335] *At the end of the day, even though the EDPs will be responsible of processing operations, it is the EPPO that will ultimately be responsible in case of infringement of the rules in its capacity as controller. EDPB, Guidelines 07/2020, op. cit., p. 10, para. 18.*
[336] *Of course, only to the extent this is legally allowed.*

the national authorities determine the subsequent purposes of the processing data, they are likely to become autonomous controllers of the (same) data held by the EPPO,[337] in which case national data protection law applies.[338] However, in our view, this does not necessarily imply they are joint controllers (*infra*).

Another situation where the roles would be somewhat blurred, is when the national authority would go beyond the EPPO's instructions or undertakes autonomously certain investigation measures. In this case, considering it at least partially determines the purposes and means of the data processing, it would have to be considered a controller in respect of the processing concerned.[339]

Finally, as explained in Part II, Chapter b, the EDP has a double hat and in some Member States (e.g. Estonia and the Netherlands) may effectively be dealing with both EPPO cases and national cases. In this hypothesis, there may be situations where the EDP processes the same data for two different purposes, for an EPPO investigation and for a separate national criminal case.

The above analysis yields an important **interim conclusion**. Evidently, the hybrid nature of the EPPO and its multi-faceted cooperation with national authorities give rise to a large variety of possible situations, each of which will have important consequences for the allocation of responsibilities in terms of data protection and, subsequently, also for the competent supervisory authorities (see Figure 8). The practical implications of all this have probably been underestimated so far and urgently require further attention. In particular, one should be aware that supervisory authorities at both EU and national level will be facing huge challenges, in terms of applicable legal framework but perhaps even more so in terms of logistics, to fulfil their legal role.

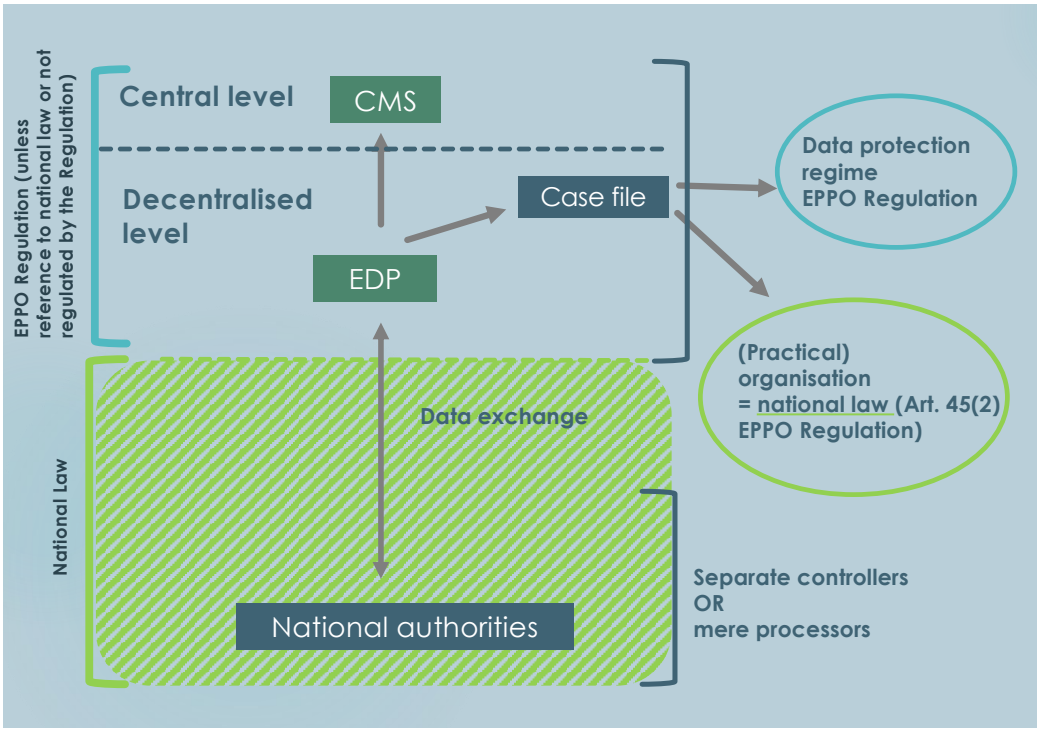
---

[337] *In this respect, it is relevant to refer to the European Commission's position that 'the databases of police authorities are under their controllership', suggesting that the data stored in these databases, even for the purpose of the EPPO investigation, fall under the police's control as they may be re-used in a different investigation. European Commission, Draft minutes, Ninth meeting of the EPPO Expert Group, 21 March 2019, p. 4.*

[338] *European Commission, Draft minutes, Ninth meeting of the EPPO Expert Group, 21 March 2019, p. 4.*

[339] *European Data Protection Board, Guidelines 07/2020, op. cit., p. 25, para. 79. See Article 65(5) of the Regulation.*

Figure 8. Summary role and responsibilities of the EPPO and national authorities



In addition to the above, another highly delicate question is whether there will be situations of **joint controllerships**. The Regulation envisages this possibility.[340] Some consider that such scenario would be applicable where the EPPO cooperates, for instance, with the police authorities of a Member State[341] or with OLAF[342] when carrying out an investigation.[343]

We consider that an approach where the EPPO and national authorities would be joint controllers is legally debatable. For the EPPO and another entity to be considered as 'joint controllers', they would have to *jointly* determine the purposes and means of processing.[344] We believe situations of separate controllerships, as explained above, are much more likely. However, the authors wish to draw attention to the CJEU jurisprudence which has 'stretched'[345] the concept of joint

[340] *See Article 64 of the Regulation.*
[341] *Article 28(1) of the Regulation.*
[342] *Article 101(3) of the Regulation.*
[343] *H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 508-509.*
[344] *European Data Protection Board, Guidelines 07/2020, op. cit., p. 3.*
[345] *Expression used by C. Millard, C. Kuner, F. H. Cate, O. Lynskey, N. Ni Loideain and D. J. Svantesson in an editorial entitled "At this rate, everyone will be a [joint] controller of personal data!", Intl Data Privacy L Rev., 2019, p. 217.*

controllers,[346] hence national authorities and the EPPO shall act with caution if they wish to avoid being qualified as 'joint controllers'.

Joint controllership entails a number of specific legal consequences laid down in Article 64 of the Regulation.[347] In particular, if the EPPO and a national authority were to be regarded as joint controllers, this would require a precise allocation of responsibilities and thus the conclusion of a joint controllership agreement.[348] At present, the EPPO has not concluded any such agreement. Furthermore, in such cases, the data subject 'may' exercise his/her rights in respect of and against each of the controller.[349] This applies to 'his/her rights under this Regulation', despite the fact that the data subject's rights defined in Article 58 to 61 of the Regulation are only rights of the data subject *vis-à-vis* the EPPO.[350]

To conclude, the precise role and responsibility of the EPPO and national authorities involved in the EPPO investigation will depend on the concrete situation, but also on the way in which the EPPO's activities will be deployed in the months and years to come. Yet, it is likely that, depending on the Member State where the EPPO is conducting its investigation, the concrete situation will differ. Important variables are the manner in which the EPPO is implemented at national level (e.g. does the EDP have an 'operational' double hat, i.e. the possibility to conduct both EPPO and national investigations, or is his/her double hat limited to the combination of national powers and formal membership of the national judiciary?), the degree of autonomy national authorities have in conducting the investigation, the responsibilities defined by national law and the legal possibilities to use data gathered in the context of an EPPO investigation for other purposes.[351]

Considering that many Member States have not even reflected on questions of controllership, it is likely there will be different approaches. The German approach gives a first indication in this respect. According to the German legislator, the primacy of the provisions of the EPPO Regulation does not apply to data processing by other German authorities (such as the police and customs authorities) which, for example in accordance with Article 28(1) and (2) of the Regulation, participate in the investigative procedures conducted by the EPPO and in this respect as a

---

[346] On this topic see T. Rothkegel and L. Strassemeyer, "Joint Control in European Data Protection Law – How to make sense of the CJEU's Holy Trinity", Computer L Rev. Intl, 2019, p. 161-171.
[347] This Article was copied from Article 26 of the GDPR. See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 509.
[348] Article 64(1) of the Regulation.
[349] Article 64(3) of the Regulation.
[350] H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 509.
[351] Certain authors emphasize that: 'Whether in the case referred to in Article 28(1) the police or customs authorities would act as "processor" or as "joint controller" may depend on the relevant national law on the respective roles, competences and responsibilities in conducting criminal investigations.' See H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 512.

'controller' under data protection law[352] manage personal data with the same content. The applicability of Section 161(2) of the Code of Criminal Procedure and Sections 483 to 481 of the Code of Criminal Procedure for processing by these authorities is not affected by the EPPO Regulation.[353] This seems to suggest that German national authorities, even in the context of the EPPO investigation, would be autonomous controllers and thus be supervised by national authorities. However, the German legislator does not take an explicit stance on the nature of this controllership (joint or separate).[354] Besides, the German legislator considers that insofar as the EPPO is the 'controller' in the sense of data protection, there is no room for the application of the Federal Data Protection Act.[355] Therefore, how the notion of controller is interpreted and implemented will be of crucial importance.

As for Estonia, while the legislator does not take position on the role that national authorities would have when they cooperate with the EPPO, it is most interesting that the Code of Criminal Procedure states that '[b]odies conducting proceedings are joint controllers of personal data processed in the course of criminal proceedings in accordance with their competence'.[356] This could suggest that Estonian authorities are more easily inclined to classify a cooperation as joint controllership.

In Belgium, where the Act on the EPPO does not take into account related data protection issues,[357] a particular situation of joint control might arise in the context of a judicial inquiry. A judicial inquiry is a criminal investigation led under the authority and direction of an investigating judge; the latter thus not only guarantees that the procedural rights of suspects and other concerned parties are respected, but actively investigates the case and gives instructions to other authorities (e.g. the police). As we have argued elsewhere,[358] the existence of a judicial inquiry is, as such, not incompatible with an EPPO investigation – an approach that is shared by the Belgian legislator[359] – even if the underlying philosophy of the EPPO Regulation is quite different. Nevertheless, once a judicial inquiry is opened, the investigation is conducted by the investigating judge, who thus

---

[352] See Section 46(7) of the German Federal Data Protection Act and Article 3(8) of the LED.
[353] Explanatory Memorandum to the German Bill on the EPPO, p. 55-56.
[354] In a follow-up questionnaire addressed to H.H. Herrnfeld by the authors of this study, the former indicated that, in his opinion, when national authorities and the EDP store data with the same content, they would be joint controllers.
[355] Explanatory Memorandum to the German Bill on the EPPO, p. 40.
[356] § 15²(6) of the Estonian Code of Criminal Procedure.
[357] These issues could, however, still be dealt with later on, in a separate piece of legislation.
[358] A.L. Claes, A. Werding and V. Franssen, op. cit.
[359] While in France the legislator decided that EPPO investigations would always be conducted under the authority of the EDP, thus excluding the possibility of a judicial inquiry in EPPO cases, the Belgian legislator aims to maintain the judicial inquiry but intends to designate specialized investigating judges for EPPO investigations. Articles 696-115, para. 2, 696-116 and 696-117 of the French Code of Criminal Procedure; Articles 2, 6 and 8 of the Belgian Act on the EPPO.

determines the purposes and means of data processing. In the context of an EPPO case, one could however also argue that the EPPO is the data controller as this body can still request the investigating judge to undertake certain investigation measures and as it will decide on the direction to be given to the case once the judicial inquiry is terminated. The investigating judge and the EPPO could thus potentially be joint controllers, the former subject to national law and the latter to the Regulation.

Moreover, as suggested earlier,[360] situations of joint controllership could also arise at the trial stage. This, however, exceeds the scope of this study.

To conclude, the risk of diverging approaches at Member State level is very real. While the EPPO Regulation is 'without prejudice to Member States' national systems concerning the way in which criminal investigations are organised',[361] one may nevertheless wonder whether these divergences will be beneficial for the EU-wide functioning of the EPPO.

[360] *See footnote 331.*
[361] *Recital 15 of the Regulation.*

7. IMPLICATIONS FOR THE EDPS'S SUPERVISORY ROLE

7.1. Introduction

As explained in Part III, the EDPS is responsible for monitoring the EPPO personal data processing in accordance with Regulation (EU) 2018/1725 as far as administrative personal data are concerned, while ensuring that the data protection rules laid down in the EPPO Regulation are complied with in relation to operational personal data. This study has mainly focused on the latter type of data. In this regard, the EDPS's duties and powers are defined under Article 85(2) and (3) of the EPPO Regulation.[362] In addition to supervision, the EDPS shall also *advise* 'the EPPO and data subjects on all matters concerning the processing of operational personal data' and '*cooperate* with national supervisory authorities in accordance with Article 87 [of the Regulation]'.[363]

In this last Part, we will analyse the repercussions of the analysis in the preceding parts (particularly Parts V and VI) on the EDPS's supervisory task and reflect upon the need for coordination with national supervisory authorities.

7.2. Relevant factors for delineating the EDPS's supervision

In order to delineate the EDPS's supervision tasks with regard to the operational personal data processing in the context of the EPPO's activities, it is essential to distinguish between personal data processing at central level and at decentralised (i.e. Member State) level, to determine the applicable legal regime and to identify the roles and responsibilities of the authorities that are involved in the processing.

One of the **difficulties**, as shown by our analysis in Part VI, is that the borderlines between the EU and the national level may be blurred. This is due to different conceptions of the case file,[364] diverging interpretations of the scope of national law and the potentially dispersed storage of personal data gathered in the context of an EPPO investigation, but also to the organisation of data flows between the EPPO and national authorities. The debate is indeed fueled by practical considerations stemming from the hybrid nature of the EPPO and its cooperation with national

---

[362] *The EDPS's supervision will be similar to that in respect of Europol and Eurojust. However, contrary to what is provided in the Europol Regulation, the EDPS does not have the power to impose a temporary or definitive ban on processing operations to the EPPO. See Article 43(3) (f) of the Europol Regulation in comparison with Article 85(3) of the Regulation.*
[363] *Article 85(1) of the Regulation. Emphasis added.*
[364] *As explained above, even though the EPPO will certainly set the level playing field, it is important to consider all possible points of views. Indeed, the approach chosen by the EPPO might not followed and agreed upon by all stakeholders and it might lead to proceedings before the CJEU.*

authorities.[365] The EDPs will operate at decentralised level and conduct much of their investigation based on data collected at Member State level, by various national authorities, giving rise to continuous data flows. Therefore, data processing in EPPO cases inevitably implies the intervention of multiple actors with different roles and responsibilities, as discussed in Part VI, Chapters c and d.

With respect to these roles and responsibilities, we have argued that in many cases national authorities will either be processors on behalf of the EPPO or separate controllers. The EPPO is conducting the investigation in an independent manner, and in many cases will instruct national authorities what to do, thereby defining the data processing purposes and means. However, national authorities may also process the data gathered for the EPPO for other purposes afterwards and, in case of pre-existing data passed on the EPPO too, they are separate controllers. Joint controllership is another option, but this would require that both controllers – the EPPO and the national authority concerned – jointly determine the purposes and means of the data processing. The Belgian example of the judicial inquiry seems like a rather clear case of joint controllership, thus calling for an adequate joint controllership agreement. The German approach will also lead to joint controllership between the EPPO and the German police and customs authorities, but would not require a joint controllership agreement because the respective responsibilities of these actors are sufficiently defined by EU law and German law.[366]

7.3. Two main conceptions of the EDPS's supervisory role

In principle, the EDPS's supervision extends to all data processed by the EPPO.[367] Yet, in light of the above, it is clear that processing of operational personal data in the context of an EPPO investigation will require supervision at different levels and, depending on the respective roles of the other actors involved in the investigation, also by national supervisory authorities.

In the next paragraphs we will describe the two possible approaches to the EDPS's supervisory role – a pragmatic approach and a functional approach – and the arguments against and in favour of each.

---

[365] *See European Commission, Draft minutes, Ninth meeting of the EPPO Expert Group, 21 March 2019, p. 3 and European Commission, Draft minutes, Seventh meeting of the EPPO Expert Group, 10 December 2018, p. 3.*
[366] *At least this is the opinion of H.H. Herrnfeld, expressed in a follow-up questionnaire addressed to him by the authors of this study.*
[367] *Article 85(1) of the Regulation.*

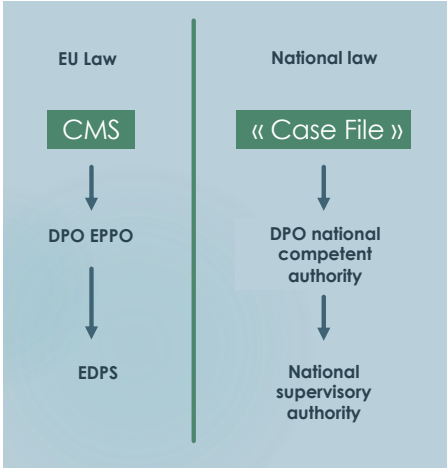
The **pragmatic approach** is based on the position adopted by the EPPO,[368] according to which the data protection regime established in the EPPO Regulation governs the data processed and stored in the CMS (in particular, the 'e-case file'). These data are processed under the 'full' control of the EPPO at central level (see *supra*, Part VI, Chapter b). In contrast, the 'case file' and data flows would both be governed by national law, in particular the law of Member State of the handling EDP.

This approach has the advantage of creating a clear-cut division between the central level and the national level, in an attempt to circumscribe the respective responsibilities of each level (see Figure 4). The EDPS could, for pragmatic reasons, follow this approach and limit its supervision to the operational personal data processed in the CMS. Because the CMS contains a copy of the case file (except for the pieces that cannot be electronically stored), the EDPS would *de facto* supervise virtually all data processed by the EPPO. Still, in order to verify that the CMS does indeed reflect the case file, the EDPS would also need to have access to the case file.

A major argument against this approach is that it is based on a peculiar interpretation of controllership, taking the location of data processing as main criterion. This interpretation does not seem to be in line with the legal definitions of controllership and the Court of Justice's case law. While the case file will be located at national/decentralised level, it is, as we have pointed out from the very start, an EPPO file because it is managed by the handling EDP who belongs the EPPO. Moreover, this approach fails to account for the hybrid characteristics of the EPPO and the complexity of data flows.

[368] *As noted above, this position may in the meantime have changed, as the EPPO is preparing for becoming operational in June 2021.*

Figure 4. 'Two-case-files' approach



In contrast, a **functional approach** (see Figure 9) to the EDPS's supervision would be precisely based on the EPPO's controllership, extending to all data that is processed for the purposes of EPPO investigations. This approach is legally more defendable, but definitely encompasses a lot of practical challenges which require careful consideration.

The functional approach is in conformity with the concept of controller as defined in EU instruments and the Court of Justice's case law. The EPPO is not only controller of the data stored at central level, but also of those contained in the case file managed by the EDP, who is part of the EPPO,[369] because the data in this case file are clearly processed for the purposes of the EPPO investigation, thus making the EPPO responsible for compliance with the Regulation's data protection rules.[370] This is in line with what we argued in Part VI, Chapter b: The data protection regime created by the Regulation applies to both the data stored in the CMS and those in the case file handled by the EDP at national level; the reference to national law in Article 45(2) of the Regulation should be interpreted rather narrowly, relating mainly to the practical organisation and storage of the case file.

Yet in addition, considering the data flows between the EPPO and national authorities, the EPPO may also be regarded as the controller of data processed by the latter for the purpose of the EPPO

[369] *It is highly worthwhile pointing out that the EPPO case file is not the first case where EU documents are stored at decentralised level. In the context of the EU Banking Union, the Grand Chamber of the CJEU has recently decided that documents kept by national central banks also belong to the 'EU archives' under Article 2 of Protocol No 7 on the Privileges and Immunities of the Union. This Protocol also applies to the EPPO and its staff, in accordance with Article 96(5) of the Regulation. CJEU, C-316/19, Commission v Slovenia, 17 December 2020, ECLI:EU:C:2020:1030. For an analysis, see K. Croonenborghs, "CJEU clarifies the inviolability of EU and European Central Bank archives – Case C-316/19 Commission v. Slovenia", European Law Blog, 20 January 2021, https://europeanlawblog.eu/2021/01/20/cjeu-clarifies-the-inviolability-of-eu-and-european-central-bank-archives-case-c-316-19-commission-v-slovenia/. Interestingly, the author suggests this ruling may also be relevant for the EPPO.*

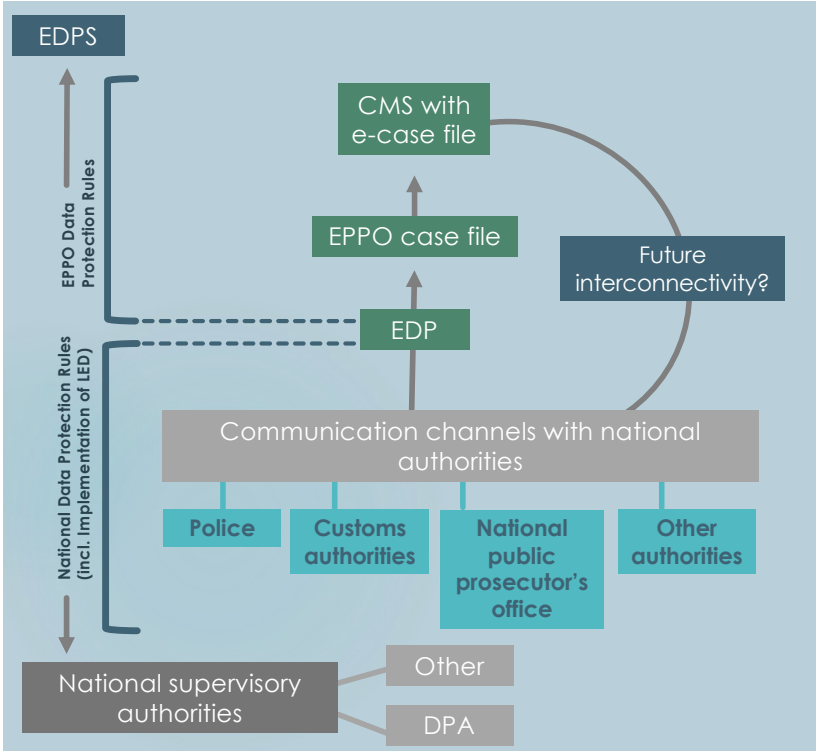
[370] *Cf. Article 47(2) of the Regulation.*

investigation, even if they are stored by national authorities (Part VI, Chapter d). In some cases, there may also be a situation of joint control. In contract, the EPPO would not be controller of the data that national authorities use for other purposes than the EPPO investigation.

Obviously, this approach will have major implications for the organisation of the EDPS's supervision. First of all, this approach entails important consequences in terms of workload for the EDPS. Because the data processing takes place at different levels and by various authorities, the supervision will be more demanding in terms of time and resources. Second, in order to fully exercise its supervisory task, the EDPS will have to have access to the data stored at national level. In accordance with Article 85(4) of the Regulation, the EDPS 'shall have access to the operational personal data processed by the EPPO and to its premises to the extent necessary for the performance of its tasks',[371] and the EPPO has the duty to cooperate with the EDPS. That said, such access will definitely require more efforts and might also present practical difficulties for the EDPS. Third, due to the multiple references to national law in the EPPO Regulation, the EDPS would also need to gain some knowledge of the national law of the 22 Member States participating in the EPPO, in particular national criminal procedure. Some of these obstacles could, however, be overcome by a close cooperation or coordination with national supervisory authorities, which already have experience in supervising the national authorities concerned.

[371] *In this respect, it may be relevant to refer to the earlier discussions in the Council Working Group: 'During the negotiations in the Council Working Group it has been discussed whether Article 79(3) should also give the DPO (and assisting staff of the EPPO's Central Office) access to the offices of the EDPs, considering them as well to be "premises" of the EPPO in terms of Article 79(3). This question may cause further debate in the future and the answer may depend on whether such access can be considered "necessary for the performance of their tasks".' H.-H. Herrnfeld, D. Brodowski and C. Burchard, op. cit., p. 533.*

Figure 9. Functional approach to the EDPS's supervision



7.4. Need for coordinated supervision

Regardless of the approach the EDPS will choose, it is clear that processing of operational personal data in the context of an EPPO investigation will require supervision at different levels. Even the European Commission recognises that the 'coordinated supervision model' will apply to the EPPO, although they advocate for limited data storage at national level (*supra*, Part VI, Chapter b).[372] For instance, to make sure that data, if need be, are corrected or erased at all levels, coordination between the EDPS and the national supervisory authorities would be valuable, if not indispensable.

The intensity of this coordination may, of course, vary. The Regulation provides that the EDPS 'shall act in close cooperation with national supervisory authorities with respect to specific issues requiring national involvement'.[373] But this leaves ample margin of discretion to the supervisory authorities to decide how they will design their future cooperation. Considering the EPPO activities and the far-reaching impact its investigations may have on suspects and other data categories, we would plea in favour of strong coordination.

[372] *European Commission, Draft minutes, Ninth meeting of the EPPO Expert Group, 21 March 2019, p. 3.*
[373] *Article 87(1) of the Regulation.*

The following **issues** in particular would benefit from a coordinated approach in order to avoid 'major discrepancies'[374] between the different actors involved in the EPPO's activities:

- The scope of application of national law with respect to the case file, as there is clearly quite some controversy regarding the interpretation of the reference to national law in Article 45(2), subparagraph 1 of the Regulation;
- The scope of application of other references to national law in the Regulation and the extent to which national law may supplement the provisions of the Regulation, even without explicit reference to national law, because the analysis in this study has shown that the rules laid down in Article 5(3) of the Regulation are in practice not so easy to apply to solve potential conflicts of law;
- The clarification of the roles and responsibilities of national authorities in the context of EPPO investigations, as this issue already seems prone to diverging approaches.

Admittedly, a major **challenge** for such coordination is the multitude of national supervisory authorities. While in some Member States (e.g. the Netherlands[375]) there may be one single data protection supervisory authority which is also competent for public authorities competent for the prevention, investigation, detection or prosecution of criminal authorities, in others the legislator designated one or more specific competent supervisory authorities, at least with respect to the 'other independent judicial authorities when acting in their judicial capacity'.[376] This is the case for Belgium, where the Data Protection Authority has no competence to supervise the following law enforcement and judicial authorities: the customs administration, the police, the public prosecutor's office and the courts (including investigating judges). For the latter two, a supervisory authority has yet to be created.[377] In Romania, there is a similar exception but only for the courts;[378] for all other national authorities (including the police and the public prosecutor's office) the National Supervisory Authority for Personal Data Processing is the competent authority. The same approach is taken in France.[379]

---

[374] *Article 87(1) of the Regulation.*
[375] *The Dutch national competent authority is the 'Autoriteit persoonsgegevens'. Article 6 of the Dutch Implementing Act of the GDPR.*
[376] *Article 45(2) of the LED.*
[377] *This is an important gap in Belgian law, which has been criticized by the Belgian Data Protection Authority, most recently in its opinion on the pending reform of the Code of Criminal Procedure. See Belgian Data Protection Authority, Opinion No 77/2020, op. cit., para. 14, p. 5.*
[378] *Article 52(2) of the Romanian Act implementing the LED.*
[379] *France's national supervisory authority is the 'Commission nationale de l'informatique et des libertés' (CNIL), with exception to the courts when acting in their judicial capacity. See Articles 8 et seq. and in particular 19(V) Act No 78-17 of 6 January 1978 relating to Information Technology, Files and Liberties as modified by the Act implementing the LED.*

8. Conclusions

At the end of this study, it may be concluded that there is still quite some legal uncertainty with respect to the theoretical and practical interplay between the data protection regime laid down in the EPPO Regulation and national legislation. This is due to the references to national law in the Regulation, but particularly to the fact that the scope of national law is sometimes ill-defined and the extent to which national law can supplement the Regulation also raises questions.

Moreover, with regard to the implementation of the EPPO at EU and national level, various elements still need to be defined, in particular with regard to the legal regime that applies to the case file and the organisation of data flows between the EPPO and national authorities. As a result, it is somewhat premature to define the precise roles and responsibilities of the actors that will be involved in the EPPO's activities. Yet, it is obvious that the implications of the allocation of responsibilities are considerable and will influence the scope of the EDPS's supervision.

Despite all these uncertainties, the study has identified two possible approaches to the EDPS's supervisory role – a pragmatic one and a functional one – and presented the advantages and disadvantages of each approach. Regardless of the approach that will be chosen, the supervision of the EPPO's operational activities will bring a number of unprecedented challenges and there will be a strong need for coordination with national supervisory authorities to avoid major discrepancies between the EU level and the Member State level. Considering the start of the EPPO's operational activities is imminent, it is high time for all stakeholders concerned to prepare such coordination.

9. Annexes

Annex 1: List of abbreviations

CJEU	Court of Justice of the European Union
CMS	case management system
DECP	Deputy European Chief Prosecutor
DP	data protection
ECP	European Chief Prosecutor
EDP	European Delegated Prosecutor
EDPB	European Data Protection Board
EP	European Prosecutor
EPPO	European Public Prosecutor's Office
(EPPO) Regulation	Regulation (EU) 2017/1939
EU	European Union
IRP	Internal Rules of Procedure
LED	Directive (EU) 2016/680
TFEU	Treaty on the functioning of the European Union
TEU	Treaty on the European Union

Annex 2: National laws implementing the LED and Acts/Draft Bills on the EPPO Regulation: Original titles

Belgium

- Act implementing the LED: Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *Moniteur Belge*, 5 September 2018;
- Bill on the EPPO (including the Explanatory Memorandum): *Doc. Parl.*, Ch. représ., sess. 2020-2021, No 1696/001, available at: https://www.lachambre.be/kvvcr/showpage.cfm?section=/none&leftmenu=no&language=fr&cfm=/site/wwwcfm/flwb/flwbn.cfm?lang=F&legislat=55&dossierID=1696.
- Act on the EPPO: Loi du 17 février 2021 portant des dispositions diverses en matière de justice, *Moniteur Belge,* 24 February 2021.

Estonia

- Act implementing the LED: Isikuandmete kaitse seadus, *RT I*, 4 January 2019, p. 11;
- Bill on the EPPO (including the Explanatory Memorandum): available at: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/31b99c07-53a2-4ab2-8c7b-bdae4a21dbb5/Kriminaalmenetluse%20seadustiku%20ja%20kohtueksper tiisiseaduse%20muutmise%20seadus%20(arestimis-%20ja%20konfiskeerimisotsuste%20vastastikuse%20tunnustamise%20määruse%20ning%20Euroopa%20Prokuratuuri%20määruse%20rakendamine).
- Act on the EPPO: Kriminaalmenetluse seadustiku ja kohtueksper tiisiseaduse muutmise seadus (arestimis- ja konfiskeerimisotsuste vastastikuse tunnustamise määruse ning Euroopa Prokuratuuri määruse rakendamine), *RT I*, 29 December 2020, p. 1.

France

- Act implementing the LED : Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles modifiant la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *Journal Officiel de la République Française*, No 0141, 21 June 2018;
- Act on the EPPO : Loi n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée, *Journal Officiel de la République Française,* No 312, 26 December 2020.

Germany

- Act implementing the LED: Gesetz vom 30. Juni 2017 zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU), *Bundesgesetzblatt* I, 2017, No 44, 5 July 2017 o. 2097;
- Bill on the EPPO (including the Explanatory Memorandum): Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2017/1939 des Rates vom 12. Oktober 2017 zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft und zur Änderung weiterer Vorschriften, Drucksach 47/20, *Bundesrat*, Version 31 January 2020, available at: https://www.bundesrat.de/SharedDocs/drucksachen/2020/0001-0100/47-20.html.
- Act on the EPPO: Gesetz vom 10. Juli 2020 zur Durchführung der Verordnung (EU) 2017/1939 des Rates vom 12. Oktober 2017 zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft und zur Änderung weiterer Vorschriften, *Bundesgesetzblatt* I, No 35, 16 July 2020 o.01648-01652.

Netherlands

- Act implementing the LED: Wet van 17 oktober 2018 tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, *Staatsblad van het Koninkrijk der Nederlanden*, No 401, 12 November 2018;
- *Bill on the EPPO: Aanpassing van enkele wetten ter uitvoering van de Verordening (EU) 2017/1939 van de Raad van 12 oktober 2017 bettreffende nauwere samenwerking bij de instelling van het Europees Openbaar Ministerie ("EOM"), PbEU 2017, L 283, Invoeringswet EOM, Kamerstuk 35429, available at: https://www.tweedekamer.nl/kamerstukken/detail?id=2020D12627;*
- *Act on the EPPO, Staatsblad van het Koninkrijk der Nederlanden, No 155, 31 March 2021.*

Romania

- Act implementing the LED: Legea nr. 363/2018 privind protecția persoanelor izice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente ın̂ scopul prevenirii, descoperirii, cercetă rii, urmă ririi penale ș i combaterii infracțiunilor sau al execută rii pedepselor, mă surilor educative siguranță, precum și privind libera circulație a acestor date, *Monitorul Oficial*, Part I, No 13,7 January 2019.
- Act on the EPPO: Legea nr. 6/2021 privind stabilirea unor măsuri pentru punerea în aplicare a Regulamentului (UE) 2017/1.939 al Consiliului din 12 octombrie 2017 de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO), *Monitorul Oficial*, Part I, No 167, 18 February 2021.

Spain

- Draft Bill implementing the LED: not yet published;

- Draft Bill on the EPPO: available at: http://leyprocesal.com/leyprocesal/dm/anteproyecto-de-ley-organica-por-la-que-se-adapta-el-ordenamiento-nacional-al-reglamento-ue-20171939.asp?cod=7792&nombre=7792&nodo=&sesion=1.

Annex 3: List of interviews

Name	Function/Institution	Date
Steven Ryder	EPPO Legal Service	9 October 2020
Thomas Zerdick	EDPS	13 October 2020
Nicholas Franssen	Dutch Ministry of Justice and Security	2 November 2020
Peter Csonka, Fabio Giuffrida	European Commission, DG Just	6 November 2020
Olivier Micol	European Commission, DG Just	11 November 2020
Diana Alonso-Blas	DPO Eurojust	19 November 2020
Christophe Bierlaire, Julie Godfroid, Eric Wauters	Belgian Federal and Local Police	27 November 2020
Hans Herrnfeld	German Ministry of Justice	7 December 2020
Steven Ryder	EPPO Legal Service	22 December 2020
Marie-Hélène Descamps	Belgian Ministry of Justice and Member of the *Centre de connaissance* of the Belgian Data Protection Authority	11 January 2021
Nicholas Franssen	Dutch Ministry of Justice and Security	15 January 2021

Annex 4: Meetings with the EDPS

Date	Participants	Videoconference/Call
14 July 2020	Constantin Chira-Pascanut – Thomas Zerdick – Vanessa Franssen – Marine Corhay	Videoconference
16 October 2020	Michal Fila – Vanessa Franssen	Call
30 October 2020	Michal Fila – Vanessa Franssen	Call
3 November 2020	Michal Fila – Angelov Plamen – Priscilla de Locht – (Thomas Zerdick) – Vanessa Franssen – Marine Corhay	Videoconference
12 January 2021	Michal Fila – Thomas Zerdick – Niksa Stolic – Vanessa Franssen – Marine Corhay	Videoconference
26 February 2021	Michal Fila – Vanessa Franssen – Marine Corhay	Videoconference

Annex 5: List of figures