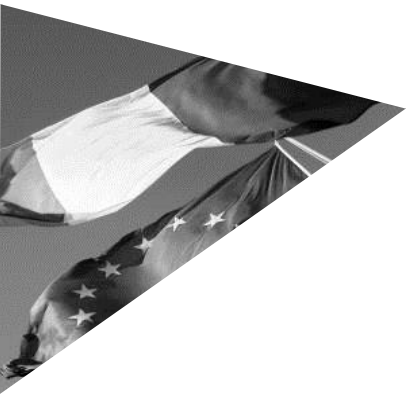
© 2015 Property of Ernst & Young Associés et Ernst & Young Société d'Avocats – Confidential. This report is reserved for your internal use and is indissociable from the contextual elements used as a basis for its elaboration.

European Commission – DG Justice

Evaluation study on Regulation (EC) No 45/2001

Case studies

May 2015



Building a better working world

This study was requested by the European Commission, DG Justice in view of the amendment of 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 (OJ L 8, 12.1.2001, p. 1–22).

Authors: EY France

- for EY Société d'avocats: Fabrice Naftalski, Christina Samaras;
- for EY Advisory: Marie Brunagel, Véronique Ménez.

With the support of academic experts:

- Alberto Alemanno (for "Access to documents" and "Articulation between the supervisory and advisory roles of the EDPS");
- Arnaud Van Waeyenberge (for "Data protection in the area of police and judicial cooperation in criminal matters").

The information and views set out in this study are those of the authors and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

1 Data protection in the area of police and judicial cooperation in criminal matters 6

1.1. Overview of the legal/normative framework 8

1.2. The use of Regulation (EC) No 45/2001 in the areas of police and judicial cooperation in criminal matters in a critical perspective 14

1.3. Scenarios 16

2 Coherence of Regulation (EC) No 45/2001 with the ePrivacy Directive (as amended in 2009) 22

2.1. Introduction 22

2.2. Preliminary remarks and methodology 23

2.3. Security of processing 24

2.4. Confidentiality, cookies and similar technologies 26

2.5. Traffic and billing data of users processed and stored by providers of communication services 31

2.6. Presentation and restriction of calling and connected line identification 34

2.7. Location data other than traffic data 36

2.8. Derogations 37

2.9. Automatic calls forwarding 37

2.10. Directories of subscribers 38

2.11. Unsolicited communications 39

2.12. Exception for national security, defence, public security and governance of criminal offences 41

Annex 1. Comparative table of Chapter IV of Regulation (EC) No 45/2001 with the ePrivacy Directive 44

3 Access to documents vs data protection 63

3.1. The relationship between Regulation (EC) No 45/2001 and Regulation (EC) No 1049/2001 63

3.2. Interpretation of Article 4(1)(b) Regulation (EC) No 1049/2001: threshold vs renvoi 65

3.3. The Bavarian Lager rulings 65

3.4. Criticism of the Bavarian Lager 67

3.5. The case- law post Bavarian Lager 68

3.6. Proposed solutions for the resolving the conflict 70

3.7. Conclusion 73

4 Data retention within the HR context 76

4.1. Introduction 76

4.2. General remarks on data retention within the EU institutional framework 76

4.3. Overview of practices regarding the conservation of personal data in HR context 82

5 Articulation between the supervisory and advisory roles of EDPS 102

5.1. Assessment of the powers provided to the EDPS 102

5.2. Allocation of resources between all the tasks of the EDPS 104

5.3. Legal feasibility of providing the EDPS with the power to impose financial sanctions (in the light of the GDPR) 108

In the context of the evaluation study on Regulation (EC) No 45/2001, the European Commission requested an in-depth examination of specific key issues of Regulation No (EC) 45/2001, especially to assess the articulation of Regulation No (EC) 45/2001 with other key Regulations. Cases studies were built in accordance with the data collection and analysis tools deployed for the answers to evaluation questions. Based on the evidence collected through interviews and survey, five case studies were developed focusing on a particular aspect of Regulation No (EC) 45/2001.

Based on the terms of reference and inception work of the tender, the following aspects have been addressed in case studies in order to guide the evaluation:

- Application of the regulation to agencies and bodies in the area of judicial cooperation in criminal matters and police cooperation;
- Articulation with the e-privacy directive;
- Articulation with the access to document rules of Regulation (EC) No 1049/2001;
- Data retention concerning data of EU institutions' staff;
- Evaluation of articulation of Supervisory and Advisory role of EDPS.

1 Data protection in the area of police and judicial cooperation in criminal matters

European integration is often understood through neo-functionalist theories, the theoretical bases of which lie in the concept of the « spill-over effect, » which refers to integration in a given area leading to enhanced cooperation in a related area.[1] This interpretation seems especially appropriate for an understanding of the European Union former third pillar system regarding the protection of data in the area of police and judicial processing.

The gradual and differentiated construction of a European judicial system since the creation of the European Union and its pillar system by the Treaty of Maastricht, inevitably led to a fragmented legal framework.[2] While the Community and its pillar structure have been replaced since the Treaty of Lisbon, this congenital differentiation persists in a number of areas of European Union law and provides explanation for the co-existence of unstandardized bodies of law. Such is the case in the legal framework concerning the protection of personal data.

This fragmented legal framework[3] may be summarized in the following manner:

Directive 95/46/EC[4] was conceived as a first pillar instrument. The directive has broad scope in the regulation of personal data processing.[5] However, as stated by Article 3(2) of the Directive, it shall not apply « *to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union, and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law* ».

[1] E. Haas, « International Integration: The European and Universal Process », *International Organization*, n° 15, 1961, p. 229 to 260.

[2] The procedural and substantive law established in the « Community » pillar (former first pillar) often did not correspond to the procedural and substantive law established by the former third pillar (Police and Judicial Cooperation in Criminal Matters), where inter-governmentalism and unanimity prevailed.

[3] For a detailed overview of this fragmentation, see annex 3 "Data Protection in the area of Police and Judicial Co-operation in criminal matters" of the *Impact Assessment accompanying the "Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and the "Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data"*, SEC (2012) 72 final, p. 48 and sub. (hereafter "Impact Assessment"); see also for an analysis P. De Hert and V. Papakonstantinou, *The data protection regime applying to the inter-agency cooperation and the future architecture of the EU criminal justice and law enforcement area*, Study for the European Parliament, PE 510.001, November 2014, p. 10 and sub.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995, p. 31 – 50.

[5] See Article 3 (1) of the Directive 95/46/EC - For an general analysis of the Directive 95/46/EC see Y. Poullet, "EU data protection policy. The Directive 95/46/EC: Ten years after », *Computer Law and Security Review: The International Journal of Technology and Practice*, 2006, Volume 22, Number 3, p. 206 - 217 and for an analysis of its implementation see D. Korff, *EC Study on Implementation of Data Protection Directive 95/46/EC*, 2002, 253p. Available at SSRN: http://ssrn.com/abstract=1287667 and for an analysis of its proposal to consider revising the Directive, R. Wong, « The Data Protection Directive 95/46/EC: Idealisms and Realisms », *International Review for Computers and Law*, 2012, p. 229 – 244.

Regulation (EC) No 45/2001[6] was also intended as a first-pillar instrument and, thus, regulates the personal data processing of EU institutions and agencies and establishes the position of the European data protection supervisor (hereafter "EPDS")[7]. When enacted in 2001, criminal justice and law enforcement (including personal data processed by police and judicial cooperation in criminal matters) was understood to be exempt from its scope. The primary basis for this exemption was the use of the term "Community" throughout, as opposed to the term "Union," especially in Article 3.1 on the scope of the regulation.

Given that the regulatory framework concerning the protection of personal data was primarily dedicated to activities of the first pillar, the Council decided to cover the activities of the third pillar by the Framework Decision 2008/977/JHA[8] which provides protocol for the protection of personal data processed in police and judicial cooperation in order to prevent, investigate, detect or prosecute a criminal offense, or to enforce a punishment. Nevertheless, this Framework Decision only partially met its objective[9]. In fact, its scope is particularly limited in that it is restricted to regulating data subject to a cross-border transmission[10] and does not therefore apply to domestic data processing[11]. As the European Commission noted, this distinction is surprising because it is not present in either the materials promulgated by the Council nor in Directive 95/46/EC[12]. Moreover, the distinction raises certain practical difficulties because « personal data gathered in a purely domestic context can hardly be factually distinguished from data that has been subject to cross-border transmission »[13]. In addition, the existing bilateral/multilateral agreements with third countries concerning the implementation of the Framework Decision are also excluded from its scope[14]. Finally, Article 28 of the Framework Decision[15] established that acts preceding implementation of Framework Decision[16] would not be subject to modification. Posterior acts, such as the Europol and Eurojust decisions, would be analysed on a case-by-case basis (cf. *infra*)[17].

In December 2009, the Treaty of Lisbon[18] introduced a number of significant changes which have had direct or indirect impact on the legal framework governing data protection in the EU. First of all,

[6] 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 institutions and bodies of the Community and on the free movement of such data, OJ L 8, 12.1.2001, p. 1–22.

[7] For an analysis of the EDPS, see P. De Hert and V. Papakonstantinou, «The EDPS as a Unique Stakeholder in the European Data Protection Landscape, Fulfilling the Explicit and Non-Explicit Expectations», *Data Protection Anno 2014: How to Restore Trust? Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*, H. Hijmans and H Kranenborg (ed.), Brussels, Intersentia, 2014, p. 237–52.

[8] 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, OJ L 350, 30.12.2008, p. 60–71.

[9] For a critical analysis of the relevance of this Framework Decision, see the sub-chapter « Gaps and shortcomings in Framework Decision 2008/977/JHA » - Impact Assessment, Annex 3, p. 49 – 52. See also P. De Hert and V. Papakonstantinou, *The data protection regime applying to the inter-agency cooperation and the future architecture of the EU criminal justice and law enforcement area*, Study for the European Parliament, PE 510.001, November 2014, p. 9 and sub.

[10] See Article 1 (2) (a) (b) (c) and recitals 7 and 9 of the Council Framework Decision 2008/977/JHA between Member States and Article 13 vis-à-vis third State an International organization.

[11] Impact Assessment, Annex 3, p. 50.

[12] Impact Assessment, Annex 3, p. 50 - See joined Cases C-456/99, C-138/01 and 139/01, para 42 and 43 where the European Court of Justice does not use this distinction too.

[13] Impact Assessment, Annex 3, p. 50.

[14] Article 26 of the Council Framework Decision 2008/977/JHA.

[15] « *Where in acts, adopted under Title VI of the Treaty on European Union prior to the date of entry into force of this Framework Decision and regulating the exchange of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaty establishing the European Community, specific conditions have been introduced as to the use of such data by the receiving Member State, these conditions shall take precedence over the provisions of this Framework Decision on the use of data received from or made available by another Member State*. »

[16] 19 January 2009

[17] For a critical assessment of the Framework Decision and an explanation of the political reasons which can explain the limited scope, see P. De Hert and V. Papakonstantinou, *Ibidem*, November 2014, p. 10 and 11.

[18] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007, p. 1–271.

the pillar system was abolished and there is now only a single structure[19]. The Treaty placed an individual right to data protection in the list of basic EU fundamental rights (article 16 of the Treaty on the Functioning of the European Union (hereafter "TFEU") and Article 8 of the Charter of Human rights). A specific declaration addressing the protection of personal data processed through police and judicial cooperation in criminal matters was added to the Treaty in order to recognize the specific nature of these fields[20]. Moreover, pursuant to Article 6.2 of the Treaty on the European Union (hereafter "TEU"), the EU was to accede to the European Convention on Human Rights and thus more clearly incorporate and follow the (extensive) case law of the European Court on security-related data protection[21].

The Treaty of Lisbon replayed certain cards and, thus, raised numerous questions regarding the future of former third pillar regulations concerning the protection of personal data. This case study therefore offers an analysis of those issues, with particular attention devoted to Regulation (EC) No 45/2001[22]. The application of this regulation is still the subject of much discussion and debate. With this context, and in line with the possible future amendment of Regulation (EC) No 45/2001, this case study considers (i) how and to what extent Regulation (EC) No 45/2001 has been applied in the former-third pillar context and (ii) the supervisory role of the JSBs and the EDPS, in order to foresee possible legislative options with regard to the amendment of Regulation (EC) No 45/2001. A three-pronged analysis of these issues seems most appropriate. The first section will provide an overview of the agencies, bodies, and databases involved in the area of police and judicial cooperation (1). The second section will develop an analysis through the lens of Regulation (EC) No 45/2001 (2). Finally, the third section will identify and discuss various competing scenarios for the future (3).

1.1.Overview of the legal/normative framework

This overview examines the various agencies, bodies and databases that make up the former third pillar. In this regard and given the common issues in their applicable regulatory frameworks, we shall analyse Eurojust and Europol (A), OLAF (B), and finally, the large scale IT databases: Eurodac, VIC, CIS, SIS and EU-LISA (C).

1.1.1. Eurojust and Europol: a specific normative framework

Eurojust was created by Council decision on 28 February 2002[23], and amended on 18 June 2003 and 16 December 2008[24]. Eurojust is a « judicial cooperation agency » composed of 350 individuals

[19]Article 1 (3) TEU – Some specific procedures continue to exist – see S. Van Rapenbusch, « La réforme institutionnelle du traité de Lisbonne: l'émergence juridique de l'Union européenne », *Journal de Droit Européen,* 2008, p. 577 to 581.

[20] Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation. This declaration expresses that, even if the pillar structure has disappeared, the topic of the former Third Pillar cannot be considered as a « normal area of law where just the general framework for data protection applies » - D. Alonso Blas, « Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom », *ERA*, 2010, p.2 34; in this sense see also H. Hijmans and A. Scirocco, « Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help? » *Common Market Law Review*, Vol. 46, 2009, p.1494 and sub.

[21] The European Court of Justice has recently decided (Opinion 2/13 – 18 December 2014) that the agreement negotiated between the EU and the Council of Europe on the accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms was not compatible with the Treaty of Lisbon. The accession is thus postposed *sine die*.

[22] Please note that this case study does not attempt to assess the specific data protection regulation applicable to each agency or body. References made to these *lex specialia* are solely intended for evaluation purposes of Regulation (EC) No 45/2001.

[23] Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA), OJ L 63/1, 6.3.2002 (the "Eurojust Decision").

[24] Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2009 L 138 of 2009-06-03,

including 80 magistrates. The purpose of this agency is to improve judicial coordination and cooperation between national authorities in the EU in important cross-border criminal trials,[25] and to facilitate international mutual legal assistance as well as the implementation of extradition requests.[26]

The Framework Decision 977/2008 only applies (following Recital 13 of Council Decision 2009/426/JHA), "*to the processing by Member States of the personal data shared between the Member States and Eurojust. The relevant set of data protection provisions of Decision 2002/187/JHA will not be affected by Framework Decision 2008/977/JHA and contains specific provisions on the protection of personal data regulating these matters in more detail because of the particular nature, functions and competences of Eurojust*."[27]

The processing of personal data is primarily regulated by the Eurojust Decision in Articles 14 to 28[28]. More specifically, Article 14.2 states that: "*Eurojust shall take the necessary measures to guarantee a level of protection for personal data at least equivalent to that resulting from the application of the principles of the Council of Europe Convention of 28 January 1981 and subsequent amendments thereto, where they are in force in the Member States*". In this respect, the system foresees supplementary safeguards concerning the conditions and duration of data retention for certain categories of individuals such as victims or witnesses. Related regulations are also contained therein, regarding the right of access to information as well as the system of data retention with periodic evaluations of its usefulness[29]. These provisions are further developed through the adoption of "*Rules of procedure on the processing and protection of data at Eurojust*"[30].

The application and enforcement of data protection rules is based on a two level system. The first level consists of a Eurojust independent Data Protection Officer (DPO) (Article 17), which follows the same approach as Regulation (EC) No 45/2001, and the second level consists of the Joint Supervisory Body (JSB) composed of judges or members with an equivalent level of independence (Article 23)[31]. The JSB is thus an independent supervisory body competent "to monitor all of the processing operations carried out by Eurojust" in accordance with Eurojust decision[32]. To that effect, "the JSB has full access to all files where such personal data is processed. Eurojust shall provide the JSB with all information requested from these files, and shall assist the JSB in its tasks by all other means".[33] Moreover, in this two-level structure, the JSB is a "*redress instance for the*

---

p. 14-32 - All article references with no specific references will be made with regard to its consolidated version, 5347/3/09 REV 3, 15 July 2009.

[25] « *such as terrorism, drug trafficking, trafficking in human beings, counterfeiting, money laundering, computer crime, crime against property or public goods including fraud and corruption, criminal offences affecting the European Community's financial interests, environmental crime and participation in a criminal organisation. For other types of offences, Eurojust may assist in investigations and prosecutions at the request of a Member State.* » - http://eurojust.europa.eu/about/background/Pages/mission-tasks.aspx

[26] Article 85 (1) TFEU « *Eurojust's mission shall be to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States, or requiring a prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities and by Europol* ». For an overview of the missions and amendments of the Eurojust decision in 2003 and 2008 see P. De Hert and V. Papakonstantinou, *The data protection regime applying to the inter-agency cooperation and the future architecture of the EU criminal justice and law enforcement area*, Study for the European Parliament, PE 510.001, November 2014, p. 14 and for an in-depth analysis see P. Jeney, *The Future of Eurojust, Study for the European Parliament*, PE 462.461, April 2012.

[27] For a similar interpretation, see Impact Assessment, Annex 3, p. 53.

[28] For a comprehensive analysis of the data protection at Eurojust, see D. Alonso Blas, Data protection at Eurojust – A robust, effective ad tailor-made regime, Eurojust publication, 2011, 52 pages.

29 For more details, see Sénat (France), « *Europol et Eurojust: perspectives d'avenir, Rapport d'information fait au nom de la commission des affaires européennes* », 17 April 2014, p. 38 and sub.

30 Text adopted unanimously by the College of Eurojust during the meeting of 21 October 2004 and approved by the Council on 24 February 2005,(2005/C 68/01).

31 Currently, the three members of the JSB are judges. In addition, two of them work for national Data Protection Authorities.. – for more details see http://eurojust.europa.eu/about/structure/jsb/Pages/composition-tasks.aspx

32 D. Alonso Blas, Data protection at Eurojust – A robust, effective ad tailor-made regime, Eurojust publication, 2011, p. 29.

33 D. Alonso Blas, op. cit. 2011, p. 31.

Eurojust DPO in case of non-compliance, when the College has not resolved the non-compliance of the processing within a reasonable time. The JSB also examines appeals submitted to in accordance with Articles 19.8 and 20.2 of the Eurojust Decision, and carries out controls[34]*. If the JSB considers that a decision taken by Eurojust or the processing of data by it is not compatible with the Eurojust Decision, the matter shall be referred to Eurojust, which shall accept the decision of the JSB. Decisions of the JSB shall be final and binding on Eurojust"*[35]. The JSB also provides opinions on data protection provisions in agreements and working arrangements both internal to the EU and with third states.[36]

Europol, established in 1995 by the Europol Convention[37] replaced by a Council Decision of 6 April 2009 establishing the European Police Office (EUROPOL) (the « Europol Decision »), is the European Union's law enforcement agency. « *Its aim is to improve the effectiveness and cooperation between the competent authorities of the Member States in preventing and combating all forms of serious international organized crime and terrorism* ».[38]

The Framework Decision 977/2008 is only applicable, following recital 12 of Europol Decision, « *(…) to the transfer of personal data by Member States to Europol. The relevant set of data-protection provisions in this Decision will not be affected by that Framework Decision and this Decision should contain specific provisions on the protection of personal data regulating these matters in greater detail because of the particular nature, functions and competences of Europol.* »

Data protection is a key issue in the activity of Europol. Article 27 of the Europol Decision explicitly provides that Europol shall respect the contents of Convention 108 of the European Council[39] and Recommendation No R (87) 15[40]. Furthermore, a series of provisions (in particular Articles 29, 30, and 31) establish the framework of data protection within this agency. Following Europol, the Council Decision « *reflects the same values as Directive 95/46/EC and contains detailed Europol-specific and unique provisions* »[41].These provisions are further developed through the adoption of AWF Rules[42]. Moreover, Europol observes the principles of Regulation (EC) No 45/2001 only with regard to the processing of staff data[43].

A DPO is appointed (Article 28) to supervise and monitor compliance with the regulation in accordance with data protection. The DPO's main task is to ensure lawfulness and compliance with the Council Decision as far as data protection is concerned. In cases of non-compliance the DPO may bring the matter by addressing first the Director, then the Management Board and, if necessary, the Joint Supervisory Board (hereafter « JSB »)[44]. The JSB consists of representatives of the national data protection authorities of all 28 Member States and its task is « *to review, in accordance with this Decision, the activities of Europol in order to ensure that the rights of the individual are not violated by the storage, processing, and use of the data held by Europol. In addition, the Joint*

34 See, ECJ, 25 november 2010, K, T-277/10, § 9-16.
35 D. Alonso Blas., op. cit., 2011, p. 31.
36 D. Alonso Blas, op. cit., 2011, p. 31.
37 Convention on the Establishment of a European Police Office, OJ C316 of 27.11.1995.This convention has been amended several times.
38 https://www.europol.europa.eu/content/faq/what-europols-mission-77
39 Convention for the protection of individuals with regard to automatic processing of personal data, opened for signature on 28 January 1981 in Strasbourg.
40 Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, adopted on 17 September 1987.
41 Europol, *Data Protection at Europol*, Publication Europol, 2012, p.11 available at https://www.europol.europa.eu/content/publication/data-protection-europol-1721.
42 Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files , OJ L 325, 11.12.2009, p. 14–22.
43 Art. 39 (6) of the Council Decision 2009/371/JHA.
44 Art. 28(4) loaf the Council Decision - *Data Protection at Europol*, Publication Europol, 2012, op. cit., p. 28.

Supervisory Body shall monitor the permissibility of the transmission of data originating from Europol."[45]

1.1.2. OLAF: application of Regulation (EC) No 45/2001

The European Anti-Fraud Office (OLAF) was created in 1999 by a Commission Decision[46]. OLAF is part of the Commission, although independent in its investigative functions[47]. The mission of the European Anti-Fraud Office is threefold: (i) it protects the financial interests of the European Union by investigating fraud, corruption and any other illegal activities – *external control* (ii) it detects and investigates serious matters relating to the discharge of professional duties by members and staff of the EU institutions and bodies that could result in disciplinary or criminal proceedings – *internal control* (iii) it supports the EU institutions, in particular the European Commission, in the development and implementation of anti-fraud legislation and policies[48].

In the normal course of executing its duties, OLAF often processes personal information and is therefore confronted with data protection issues. As a service of the European Commission, OLAF is fully subject to Regulation (EC) No 45/2001 and has implemented this Regulation in order to manage its specific missions. To that effect, a DPO has been designated (Article 10.4 of the OLAF regulation) for supervision and cooperation. Due to its investigatory mandate, and in order to protect its independence, OLAF is the only service of the European Commission that has appointed its own DPO[49]. Moreover, by virtue of Regulation (EC) No 45/2001, general supervision is accorded to the EDPS.

1.1.3. Eurodac - VIC, CIS, SIS: a "coordinated supervision"

Eurodac, created in 2000 by the Eurodac Regulation[50] is not an agency, but rather an EU asylum fingerprint database for asylum applicants and irregular immigrants. The database aids efficiency in application of the Dublin convention on handling claims for asylum. This widely used IT system has been in operation since 15 January 2003 and is currently used by the 28 EU Member States as well as Iceland, Liechtenstein, Norway and Switzerland.[51]

Personal data processing is a key issue for Eurodac. To this end, oversight was originally entrusted to a Joint Supervisory Authority (JSA), which was composed of two representatives from each Member State DPA.[52] Nevertheless, this system has changed since 2004 and control has effectively

[45] Article 34 (1) of the Council Decision 2009/371/JHA.
[46] Commission Decision 1999/352/EC of 28 April 1999 establishing the European Anti-Fraud Office (OLAF), OJ L 136/20 31.5.1999 (as amended by Commission Decision 2013/478/EU), subsequently complemented by Regulation 1073/1999 of the European Parliament and the Council of 25 May 1999 concerning investigation conducted by the European Anti-Fraud Office (OLAF), OJ L 136/31 31.5.1999, then replaced by Regulation 883/2013 Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248/1 18.9.2013.
[47] Information from the OLAF website, at http://ec.europa.eu/anti_fraud/policy/cooperation-with-eu-institutions/index_en.htm
[48] http://ec.europa.eu/anti_fraud/about-us/mission/index_en.htm
[49] http://ec.europa.eu/anti_fraud/about-us/data-protection/index_en.htm
[50] Council Regulation No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000, p. 1. The Eurodac Regulation will be valid until 20 July 2015 when "Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the areas of freedom, security and justice" (the "Eurodac New Regulation") becomes applicable.
[51] https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/Supervision/Eurodac
[52] See Article 20 of the Eurodac Regulation.

been handed over to the EDPS[53], which supervises the various processes, incorporates relevant findings into its annual report, and issues system-specific annual activity reports.

Eurodac Regulation predominantly makes reference to the provisions of Directive 95/46/EC,[54] while Eurodac New Regulation grants the standard-setting role to Regulation (EC) No 45/2001.[55] The model of supervision is also a two-level structure: data protection supervision of the Eurodac system is divided between a national level where DPAs take the lead, and a central (EU) level, where the EDPS is competent. Coordination between the two levels is managed by the Eurodac Supervision Coordination Group (SCG), which is composed of representatives of the DPAs and the EDPS[56]. This model of "*coordinated supervision*"[57] can also be found in the VIS, CIS and SIS systems.

The EU Visa Information System (VIS), the Customs Information System (CIS) and the Schengen Information System (SIS) are mainly databases permitting personal data exchanges among Member States. These systems each fall within the EU criminal justice and law enforcement field, they are all computer (IT) systems rather than standalone (EU) agencies, and they all apply a relatively similar data protection system.

Data protection law is similarly divided into Member State processing – where Directive 95/46/EC is applicable, and EU processing – where Regulation (EC) No 45/2001 is applicable. Moreover, VIS, CIS and SIS apply the approach of the "*coordinated model*" supervision (Member State DPAs at the national level and the EDPS at the EU level) within special coordination groups (SCGs).

The Visa Information System (VIS) is a database containing information, including biometric data, on visa applications by third-country nationals. The information is collected when a visa application is lodged with an EU consulate; the data is then used to prevent visa fraud and visa-shopping among (Schengen) Member States, to facilitate the identification of visa holders within the EU, and to ensure that the visa applicant and visa user are the same person.[58] According to the VIS Regulation, supervision of the VIS system is to be undertaken at Member State level by the respective national DPAs and at EU level by the EDPS.[59] The VIS Regulation provides that Directive 95/46/EC applies to the relevant Member State processing while Regulation (EC) No 45/2001 applies to the personal data processing performed by European institutions and bodies.[60] Cooperation between the EDPS and Member State DPAs is achieved through the VIS Supervision Coordination Group (VIS SCG).[61]

The Customs Information System (CIS) has a dual role, partially falling within former first pillar boundaries (the prevention, investigation and prosecution of actions in breach of customs and agricultural legislation), and partially serving former third pillar purposes (important contraventions of national laws). The CIS Regulation[62] provides that Member State DPAs shall "*carry out*

[53] See information on the relevant webpage, available at https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Eurodac
[54] See, for example, Article 18 or Article 2.
[55] See, for example, Article 31.
[56] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/14-05-21_Eurodac_Activity_Report_2013_EN.pdf
[57] For additional information, see the Chapter 4.2. of the EDPS annual report - A single set of rules for all: EU Data Protection Reform can support businesses and protect citizens, 2013, p. 63 - https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2013/AR2013_EN.pdf.
[58] Information from the relevant EU Commission website (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm) and the EDPS annual 2013 report, *op. cit*., p.64.
[59] Regulation No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) Articles 41 and 42 respectively, OJ L 218/60, 13.08.2008 (VIS Regulation), Articles 41 and 42 respectively.
[60] See VIS Regulation, recital 17 and 18 respectively.
[61] See the relevant EDPS webpage, available at https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/Supervision/VIS.
[62] Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure correct application of the law on customs and agricultural matters, OJ L 082/01, 22.03.1997 as amended by Regulations No 807/2003 and 766/2008 (an unofficial consolidated text may be found at:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1997R0515:20080816:EN:PDF).

independent supervision of such data included in the CIS", while the EDPS *"shall supervise compliance of the CIS with Regulation (EC) No 45/2001"*.[63] Therefore, a CIS Supervision Coordination Group has been established where the EDPS and national DPAs *"cooperate in line with their responsibilities in order to ensure coordinated supervision of CIS"*.[64] Directive 95/46/EC governs the CIS system on a Member State level and Regulation (EC) No 45/2001 governs on the EU level.[65]

The Schengen Information System (SIS)[66], currently in its second version (SIS II), is intended to allow Member State competent authorities to exchange information following the abolition of controls at internal borders within the Schengen area. As in the aforementioned systems, the Schengen legal framework[67] awards data protection supervision to Member State DPAs at the national level and to the EDPS at the EU level.[68] Cooperation takes place within the SIS II Supervision Coordination Group (whose first meeting was in June 2013).[69] Similarly, its substantive data protection law involves Directive 95/46/EC for Member State processing and the Regulation (EC) No 45/2001 for EU processing.[70]

In October 2011, EU -LISA a European Agency dedicated to the operational management of large-scale IT systems in the area of freedom, security and justice was established. EU-LISA is responsible for the operational management of the second-generation Schengen Information System (SIS II), the Visa Information System (VIS) and Eurodac.[71] Its role consist of taking all necessary measures to keep large-scale IT systems functioning in accordance with the specific provisions applicable to each of them, including responsibility for the communication infrastructure used by them.[72] EU-LISA has no power to correct or modify the data.

The agency, which has been operational since December 2013, is subject to Regulation (EC) No 45/2001 but without prejudice to the provisions on data protection laid down in the legislative instruments governing the development, establishment, operation and use of large-scale IT systems[73]. Concretely this means that the regulation is used only for (and the supervisory power of EDPS is limited to) the « *operational management* » of the large-scale IT systems in the areas of freedom, security and justice (and not for the systems themselves) [74] and, also, as regards the

63 CIS Regulation, Article 37 par. 1 and 3a respectively.
64 See the EDPS annual report for 2013, p.65.
65 See Article 43.3 of the CIS Regulation.
66 For an in-depth analysis see E. De Capitani, « The Schengen system after Lisbon: from cooperation to integration », *ERA Forum*, 2014, p. 101–118.
67 The SIS II Regulation (Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, p. 4–23) and the SIS II Decision (Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7.8.2007, p. 63–84).
68 See the SIS II Regulation, Articles 44 and 45 respectively.
69 See Article 46 of the SIS II Regulation.
70 See Preamble (18) of the SIS II Regulation.
71 Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011, p. 1–17.
72 Article 1.4 of Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. The main operational task is to ensure that these systems are kept functioning 24 hours a day, seven days a week. Its other responsibilities include adopting the necessary security measures and ensuring data security and integrity as well as compliance with data protection rules. http://ec.europa.eu/dgs/home-affairs/what-we-do/agencies/index_en.htm.
73 Article 28 of Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.
74 The provisions on data protection which regulates the large-scale IT systems (and explained *supra*) are thus still in force.

supervision of the staff files. A DPO has been appointed. Representatives of the agency participate in the various VIS, CIS II and Eurodac Supervision Coordination Group[75].

To conclude this general overview of Data protection in the areas of police and judicial cooperation in criminal matters, we observe a fragmentation in the regulatory framework. Three different types of situations may be identified:

1) **Europol and Eurojust apply their own set of data protection rules enshrined in Eurojust and Europol Decisions and follow a two-level system of supervision. In brief[76], the first level consists of a DPO to supervise and monitor compliance with the provisions of the Eurojust and Europol Decisions (Article 17 of Eurojust Decision and Article 28 of Europol Decision). The second level consists of Joint Supervisory Bodies (JSB) (Article 23 Eurojust Decision and Article 34 of Europol Decision) which also monitor compliance with the Eurojust and Europol Decisions. In addition the JSBs are responsible for upholding the rights individuals have in relation to their personal information (this includes considering the appeals of individuals who have requested access to their information but who are not satisfied with Eurojust/Europol's response)[77].**
2) **OLAF applies Regulation (EC) No 45/2001 with a general supervision of the EDPS, and**
3) **Eurodac, VIS, CIS and SIS apply Regulation (EC) No 45/2001, Directive 95/46/EC and specific regulations pertaining to these IT databases (*see above*). These large-scale IT databases are under a "*coordinated supervision*" model with DPAs and the EDPS.**

1.2. The use of Regulation (EC) No 45/2001 in the areas of police and judicial cooperation in criminal matters in a critical perspective

Before the Treaty of Lisbon came into effect, Regulation (EC) No 45/2001 did not apply to areas falling outside the scope of Community law. Nevertheless, Community institutions applied Regulation (EC) No 45/2001 in all policies.

The subsequent application of Regulation (EC) No 45/2001 to EU criminal justice and law enforcement remains a key point of controversy. As discussed *supra,* Eurojust and Europol interpret Regulation (EC) No 45/2001 (Article 3) in a literal manner that limits its use to Article 46 (f) (ii) relating to the collaboration between the EDPS and the JSBs to improve the consistency of the rules[78]. EU IT systems and agencies of the ex-third pillar, or the ones similar to police and criminal justice authorities, apply Regulation (EC) No 45/2001 and are thus under the supervision of the EDPS (OLAF, Eurodac, VIS, SIS, CIS and EU-LISA). From a regulatory perspective, the application of Regulation (EC) No 45/2001 for these bodies does not seem problematic.

[75] See the reports available at the EDPS website – for example https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/VIS/14-10-29_VIS_Supervision_Coordination_Group_EN.pdf.
[76] For a description of the system, see *supra* 1.1.1.
[77] For a description of the tasks of JSB see: for Eurojust http://eurojust.europa.eu/about/structure/jsb/Pages/composition-tasks.aspx and for Europol http://europoljsb.consilium.europa.eu/about/tasks-of-the-jsb.aspx?lang=en.
[78] In practice, the EDPS is actually not used for Article 46 (f) (ii) of Regulation (EC) No 45/2001 regarding staff files.

If Regulation (EC) No 45/2001 becomes the point of reference for Europol and Eurojust, an issue will arise as to the applicable rules, within the articulation of general data protection rules laid down in the Regulation (EC) No 45/2001, or its successor, and specific data protection rules for Europol and Eurojust. Regulation (EC) No 45/2001 contains a general data protection regime. Agency-specific texts complement those general rules with specific data protection provisions. The question will be which rules the EDPS will follow while executing its monitoring duties. It seems difficult to answer this question in a single definitive manner. A case-by-case approach seems more appropriate, whereby Regulation (EC) No 45/2001 would apply by default, but with room for the EDPS to apply heightened standards where specifically provided by texts, that is to say, when more specific rules exist. This approach would benefit those favouring maximum protection.

Before identifying the various possible scenarios, a brief discussion of the reform efforts currently underway may be necessary in order to contextualize the proposals with what is presently being discussed by European political decision-makers.

Given the above fragmented post-Lisbon context legal framework, in 2012 the European Commission presented its own approach to data protection regulation in the field of criminal justice and law enforcement through a *EU data protection reform package*.

The package contains two legislative proposals: a Regulation, the General Data Protection Regulation[79], in order to replace Directive 95/46/EC, establishing a general EU framework for data protection, and a Directive, the Police and Criminal Justice Data Protection Directive, intended to replace the 977/2008 Framework Decision on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offenses and related judicial activities. Following Article 59 of the Directive, the current criminal justice and law enforcement architecture remain unaffected.[80]. In March 2014 the European Parliament adopted its first reading on the proposals[81]. The discussions are currently pending at the Council.

In light of the new provisions of the Treaty of Lisbon regarding Eurojust (Article 86 TFEU), the Commission also presented a Reform Proposal on 17 July 2013.[82] Chapter V (Articles 27 to 37) concerns data protection. In this regard, the provision renders Regulation (EC) No 45/2001 applicable to all processing operations[83] and completes the aforementioned Regulation in the context of Eurojust[84]. The EDPS thus assumes responsibility for the supervision of Eurojust personal data processing[85]. The role of the Eurojust DPO is articulated with Regulation (EC) No 45/2001[86]. The positions on the Commission's proposal regarding both the Parliament and the Council are

[79] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), 25.01.2012, COM(2012) 11 final.

80 Some authors argue that "it appears unlikely that the draft Police and Criminal Justice Data Protection Directive will affect the agency-specific regulatory instruments in force today in the EU criminal justice and law enforcement area, at least in the foreseeable future. P. De Hert and V. Papakonstantinou, The data protection regime applying to the inter-agency cooperation and the future architecture of the EU criminal justice and law enforcement area, Study for the European Parliament, PE 510.001, November 2014, p. 29.

81 See, for the Directive, European Parliament, Report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, (COM(2012)0010-C7-0024/2012-2012/0010(COD)), A7-0403/2013, 22 November 2013.

[82] "Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust)", COM(2013) 0535 final (the "draft Eurojust Regulation") together with a "proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office (EPPO)".

[83] "*Regulation (EC) No 45/2001 shall apply to the processing of personal data by Eurojust in the context of its activities. This Regulation particularises and complements Regulation (EC) No 45/2001 insofar as personal data processed by Eurojust for its operational tasks is concerned.* » - Article 27 (5) of the proposal.

[84] See Article 28, 29, 32 and 33 of the proposal.

[85] For details see Article 35 of the proposal.

[86] Article 31 of the proposal.

currently under discussion[87]. More precisely, in March 2015, the Council reached a *general approach*[88] which will constitute the basis for discussion with the European Parliament[89]. This general approach contains several amendments regarding the provisions dedicated to data protection (Chapter IV). At the level of Parliament, the proposal is still under discussion[90].

Moreover, on the basis of Article 88 TFEU, the Commission presented a proposal for a Regulation on the European Union Agency for Law Enforcement Cooperation and Training (Europol) in 2013.[91] The draft Europol Regulation establishes a data protection system influenced by both the 977/2008 Framework Decision and Regulation (EC) No 45/2001. It strengthens the position of the DPO, abolishes the JSB, and awards supervision to the EDPS. The proposal is still currently at the "trilogue" stage[92].

By way of conclusion, and although the details of the legislative procedure render all analysis uncertain, it bears noting that through its Eurojust and Europol regulatory proposals, the Commission has moved towards an increased role of the EDPS and broader application of Regulation (EC) No 45/2001.

1.3.Scenarios

This section aims to be more forward-looking and offers a range of possible scenarios for the future of the Regulation (EC) No 45/2001 in the area of police and judicial cooperation in criminal matters.

This sub-chapter will focus particularly on the future of data protection at Eurojust and Europol since the *legal* framework of Olaf and the large-scale IT databases[93] do not seem to raise particular problems with regard to Regulation (EC) No 45/2001. In fact, according to the information collected during our discussions, the system's weaknesses do not relate to the text of the regulation as such, but to a lack of *effectiveness* in the implementation, difficulty in *translating the legal provisions* into concrete procedures and better *cooperation* with the EDPS. The lack of effectiveness is primarily due to a lack of communication concerning the importance of data protection in the European Union. This results in not making the implementation of the data protection system a priority in domestic policy. Thus, another recurrent difficulty is related to the concrete "translation" of the general provisions of Regulation (EC) No 45/2001 in diverse activities of these EU bodies as well as the fact that it is sometimes considered to be too bureaucratic. Finally, a greater availability (more on-site visits) and a better reactivity (shorter response time) from the EDPS would, it seems, be

[87] Eurojust JSB has taken a rather critical position on the texts at hand. in "*Opinion of the Joint Supervisory Body of Eurojust regarding data protection in the proposed new Eurojust legal framework*", 14 November 2013, 23 pages - http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/jsb/opinions/Opinion%20on%20the%20new%20Eurojust%20Regulation,%202013/OpinionJSB_new_Eurojust_Regulation_2013-11-14_EN.pdf

[88] 27 February 2015, Institutional file, 2013/0256, http://data.consilium.europa.eu/doc/document/ST-6643-2015-INIT/en/pdf

[89] Outcome of the Council meeting, Justice and Home Affairs Brussels, 12 and 13 March 2015, 7178/15, p 7.

[90] http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0256(COD)

[91] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final, 27.3.2013 (the "draft Europol Regulation").

[92] For a more detailed explanation, see P. De Hert and V. Papakonstantinou, *The data protection regime applying to the inter-agency cooperation and the future architecture of the EU criminal justice and law enforcement area*, Study for the European Parliament, PE 510.001, November 2014, p. 13. The Europol JSB has taken a rather critical position on the texts at hand, in three critical opinions regarding the proposal: JSB's first opinion:- http://europoljsb.consilium.europa.eu/media/257072/13-31%20jsb%20opinion%20on%20europol's%20regulation%20proposal.pdf - JSB's second opinion: http://europoljsb.consilium.europa.eu/media/259439/13-56%20second%20jsb%20opinion%20europol%20regulation%201-6-5.pdf and JSB's third opinion -http://europoljsb.consilium.europa.eu/media/266161/jsb%27s%20third%20opinion.pdf

[93] The EU-LISA situation is a particular one since this agency has only been very recently set up and the process of drawing up the data protection rules is still on going.

appreciated so that those involved would feel more EDPS presence and control and would therefore implement the Regulation more efficiently.

As a preliminary remark and before going more in-depth in these scenarios, it follows from the interviews performed, the documents provided by Eurojust and Europol[94] and the correspondence of these agencies[95], that both agencies express satisfaction with the current data protection system. They agree that the current data protection systems offer a high level of data protection. They value the constructive relationships between the DPOs, their respective hierarchies and the JSBs. In addition, according to the opinion of the defenders of the current system, the criticisms concerning the lack of independence of the JSB are unfounded in general and in particular for Eurojust. Moreover, they claim the current system works well with scarce resources and the proposed reforms would involve changes that would add an added expense to the current cost of operations and would therefore go against the principle of good administration. Finally, this *ad hoc* solution for Eurojust and Europol is based on the idea that the activities they deal with are very specific (see above) and therefore fully justifies a different treatment. This specific characteristic, according to those in favour of this scenario, is in line with Declaration 21 annexed to the Lisbon Treaty that acknowledges the existence of a differentiated status in the former third pillar.[96]

Nonetheless, it needs to be noted that the current legal framework is not free of difficulties. First of all, it maintains the long-criticised fragmentation of the legal status of data protection in the European Union. This fragmentation is less justified since the pillar system was abolished and the provisions of the Lisbon Treaty have moved in favour of a standardisation. This fragmented regulatory process gives rise to a series of questions regarding the equivalence of the protection standards between the various protection systems, the effectiveness and the legal certainty of the system given its complexity[97]. Moreover, the current legal framework poses a particular problem, in relation to the independence of the JSBs, in meeting the requirements of Article 16 TFUE. In fact, since the members of the JSB are chosen by the Member States[98], they do not give the same guarantees of independence as the EDPS which is appointed by a joint decision of the European Parliament and the Council for a term of five years, on the basis of a list drawn up by the Commission following a public call for candidates[99]. Finally, the arguments related to the low level of specialisation of the EDPS do not seem to be justified insofar as several bodies/databases of the former third pillar are under its supervision and that this collaboration, which could certainly be improved with regard to the response time and presence on site, does not pose a problem and would require, at most, some adjustments and time.

Within this context, three scenarios which rely on (i) the scope of supervision and (ii) the applicability of Regulation (EC) No 45/2001 to Eurojust and Europol could be foreseen:

1) Full supervision of the EDPS and full application of Regulation (EC)º No 45/2001 in the absence of more specific rules;

[94] D. Alonso Blas, *Data protection at Eurojust – A robust, effective and tailor-made regime,* Eurojust publication, 2011, 52 pages and *Data Protection at Europol*, Europol Publication, 2012.
[95] See the various letters sent by Eurojust and the JSB to the Commission in order to keep the system as it is - http://eurojust.europa.eu/doclibrary/Eurojust-framework/data-protection/Pages/after-lisbon.aspx
[96] Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation annexed to the final act of the intergovernmental conference that adopted the Treaty of Lisbon. This declaration expresses that, even though the pillar structure has been abolished, the topic of the former Third Pillar cannot be considered as a "normal area of law where just the general framework for data protection applies".
[97] P. De Hert and V. Papakonstantinou, *The data protection regime applying to the inter-agency cooperation and the future architecture of the EU criminal justice and law enforcement area*, Study for the European Parliament, PE 510.001, November 2014, p. 35.
[98] Article 23 Eurojust and Article 34 Europol.
[99] See Article 42(1) of Regulation (EC) No 45/2001.

2) Limited supervision of the EDPS (coordination board of national supervisory authorities with EDPS) and full application of Regulation (EC) No 45/2001 in the absence of more specific rules;
3) Limited supervision of the EDPS (coordination board of national supervisory authorities with EDPS) and Regulation (EC) No 45/2001 applicable only for staff and administrative purposes.

Given the uncertainty about the precise outcome of the various proposals in the EU data protection reform package as well as in the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust) and the Proposal for a Regulation on the European Union Agency for Law Enforcement Cooperation and Training (Europol), these scenarios are based on the currently applicable legislation (Regulation (EC) No 45/2001) as well as on the Commission proposals on Eurojust and Europol. *Please note that all the below-mentioned scenarios are based on the assumption that the JSBs would be eliminated.*

1.3.1. Full supervision of EDPS, full application of Regulation (EC) No 45/2001, unless there are more specific applicable rules

The first option relies on the generalisation of Regulation (EC) No 45/2001 in line with the position expressed by the European Commission[100] as well as a full supervision of the EDPS.

As regards the legal framework, Regulation (EC) No 45/2001 might serve as a "default" legal framework only applicable in the absence of more specific rules that would complement or particularize Regulation (EC) No 45/2001.

This scenario is in line with the Commission Eurojust proposal which stresses that Regulation (EC) No 45/2001 fully applies to the processing of personal data by Eurojust in the context of its activities. Indeed, according to Article 27.5 of the Eurojust Commission proposal, the Eurojust regulation particularizes and complements Regulation (EC) No 45/2001 in as far as personal data are processed by Eurojust for its operational tasks.

As regards supervision, the EDPS would take over the tasks of the JSBs as regards the monitoring of all data processing operations at Eurojust and Europol. This supervision scenario is in line with Commission proposals on Europol and Eurojust.

For instance, in this scenario, if a person exercises his right of access, it would fall under Article 13 of Regulation (EC) No 45/2001 and Article 32 of Eurojust Commission proposal relating to the modalities regarding the exercise of the right of access. It must be noted that the right of access can be restricted in accordance with Article 20 (1) of Regulation (EC) No 45/2001 and Article 20 (3). In case of restriction to the right of access, the EDPS shall at least inform the data subject that all necessary verifications by the EDPS have taken place. The data subject has a right to have recourse to the EDPS.

This option would fit with the prolongation of the amendments provided by the Lisbon Treaty. In fact, this would be a logical response to the elimination of the pillar structure and would therefore offer a common data protection framework for all the policies implemented. Regulation (EC) No 45/2001 would better meet the requirements of Article 16 TFUE than the current situation. Declaration 21 annexed to the Lisbon Treaty that acknowledges the existence of a differentiated status in the former third pillar ultimately only has a voluntary character and enables

[100] *"The scope of application of Regulation (EC) No 45/2001 extends automatically to all data processing activities of Union institutions within the scope of Union law. The latter now contains both former third pillar and second pillar activities. Consequently, there is no legal need to formally update Regulation (EC) No 45/2001 at present (...)"* - Impact Assessment, Annex 1, p. 10 and 11.

the use of other legal instruments but cannot lead to a reduced data protection level[101].

1.3.2. Limited supervision of EDPS (coordination board of national supervisory authorities with EDPS) and full application of Regulation (EC) No 45/2001, unless there are more specific rules

The previous scenario regarding the substantive law is retained with modification of the variable regarding *supervision*, which becomes a "coordinated supervision" in the *spirit* of that which already exists for the Eurodac, VIS, CIS and SIS systems. As such, supervision is divided between the national level where DPAs take the lead, and a central (EU) level, where the EDPS is the competent authority. Coordination between the two levels is managed by a "Supervision Coordination Group", which is composed of representatives of the DPAs and the EDPS. The "Supervision Coordination Group" might have the authority – in light of that for the VIS[102] – to enhance cooperation; to exchange relevant information; to assist supervisory authorities in audits and inspections (each acting within the scope of their respective capacities); to examine difficulties in interpretation or application of Regulation (EC) No 45/2001 and its specific rules; to analyse problems with the exercise of independent supervision or the rights of data subjects; to draw up harmonized proposals for joint solutions to problems, and; to promote awareness of data protection rights as necessary.

This scenario would ensure efficient collaboration between Member States and the EDPS, as well as the recognition of specific characteristics of the activities of Europol/Eurojust. Indeed, given that the activities of Europol/Eurojust must coincide with those actions taken on a national level, it would seem relevant to provide for a body reflecting the duality of this domain. Moreover, the mixed body would be particularly well equipped to provide adequate interpretations regarding proper application of the regulations. Moreover, the foregoing would constitute an intermediary step that would allow the EDPS to familiarize itself with data protection in specific sectors, as well as to work in collaboration with initiatives on the national level and allow for smooth transition. Indeed, in this scenario, the jurisdiction of the EDPS would be expanded because it would be required to handle specific texts regarding Eurojust/Europol data protection as well as work collaboratively with actions taken on the national level within the framework of "coordinated supervision."[103]

1.3.3. Limited supervision of the EDPS (coordination board of national supervisory authorities with EDPS), Regulation (EC) No 45/2001 applicable only for staff and administrative purposes

This situation reflects the current legal framework regarding applicable substantive law and is similar to the current practices of Eurojust and Europol. Europol/Eurojust observe the principles of Regulation (EC) No 45/2001 only with regard to the processing of staff data and data held for administrative purposes but, they continue to apply their own set of data protection rules enshrined in the Europol and Eurojust decision.

---

[101] P. De Hert and V. Papakonstantinou, *The data protection regime applying to the inter-agency cooperation and the future architecture of the EU criminal justice and law enforcement area*, Study for the European Parliament, PE 510.001, November 2014, p. 35.

[102] VIS Coordination Group adopted in April 2013 and available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/VIS/13-04-11_VIS_Supervision_Coordination_Group_RoP_EN.pdf.

[103] To that effect, a relevant source of inspiration can be found in the rules of procedure of the VIS Coordination Group adopted in April 2013 and available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/VIS/13-04-11_VIS_Supervision_Coordination_Group_RoP_EN.pdf

In this scenario, Regulation (EC) No 45/2001 would be applicable to the processing of Eurojust and Europol staff data and administrative personal data processed by both agencies. This appears in line with the Europol Commission proposal. In this regard, Recital 43 of the Europol Commission proposal provides that the processing of non-operational personal data (not related to any criminal investigations) is subject to Regulation (EC) No 45/2001. Article 48 of the Europol Commission proposal indicates that Regulation (EC) No 45/2001 applies to all personal data of Europol staff members and administrative personal data held by Europol. Specific rules are applied where Europol is exercising its activities but the proposal underlines that the set of data protection rules is, to a large extent, drawn on the rules underpinning Regulation (EC) No 45/2001 (Recital 32).

This *ad hoc* solution for Eurojust and Europol is premised on the idea that the activities they address are specific with regard to their nature and functions and therefore deserve different treatment. This specific characteristic, according to those in favour of the scenario, is in line with Declaration 21 annexed to the Lisbon Treaty, which acknowledges the existence of a differentiated status in the former third pillar.[104]

In this scenario, if a data subject exercises its right of access relating to personal data held by Europol and processed for administrative purpose (*e.g.* a staff member requests access to the personal data processed by Europol for HR purposes), this request falls under Article 13 of Regulation (EC) No 45/2001. However, if a person subject to criminal investigation requests access to his or her personal data, this request should fall under Article 39 of the Europol Commission proposal.

Supervision, for its part, would change and would follow the model of "coordinated supervision", the characteristics of which are identical to those illustrated in the second scenario.

[104] Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation annexed to the final act of the intergovernmental conference that adopted the Treaty of Lisbon. This declaration expresses that, even though the pillar structure has been abolished, the topic of the former Third Pillar cannot be considered as a "*normal area of law where just the general framework for data protection applies*".

2 Coherence of Regulation (EC) No 45/2001 with the ePrivacy Directive (as amended in 2009)

Implementation and application of Chapter IV of Regulation (EC) No 45/2001 and relevance of the provisions of the ePrivacy Directive for EU institutions and bodies.

2.1.Introduction

During the last decade, the use and management of telecommunication services in organizations and *a fortiori*, within EU institutions and bodies have largely evolved to take into account technological developments, telecommunication networks convergence and to meet users' needs.

The evolution from analogical to digital technology has facilitated the conversion of voice, data and video to the digital format. Increasingly, these are now being rendered through single networks bringing about a convergence in networks, services and also devices.

Vertical structures of independent networks (IT, fixed telecommunications, mobile telecommunications, etc.) have gradually been abandoned in favor of a horizontal structure based on the IP protocol to provide many types of content through a single network.

Regulation (EC) No 45/2001 includes in its scope the processing of personal data related to the use of telecommunications networks and equipment. The protection of personal data and privacy in the context of internal telecommunications networks is governed by Chapter IV of the Regulation (EC) No 45/2001.

Chapter IV was drawn up on the basis of the rules as stated in Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (hereinafter "Directive 97/66/EC").

In 2002, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector[105] (hereinafter "Directive 2002/58/EC") repealed Directive 97/66/EC. This text has been amended by Directive 2009/136/EC[106] (hereinafter "Directive 2009/136/EC" and together the "ePrivacy Directive").

The ePrivacy Directive complements and specifies Directive 95/46/EC so the provisions of the ePrivacy Directive will be interpreted in the light of similar provisions in Directive 95/46/EC[107].

[105] Directive 2002/58/EC of the European Parliament and of the Council *concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)* (OJ L 201 of 31.7.2002, p.37).
[106] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, *amending Directive 2002/22/EC on universal service and users' right relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws* (OJ L 337 of 18.12.2009, p.11).
[107] Case C-119/12, *Josef Probst v. mr.nexnet GmbH*, 22-11-2012.

It stems from the above that the rules found in in Chapter IV of the Regulation are outdated.

Indeed, Chapter IV of Regulation (EC) No 45/2001 translates general principles of personal data protection for the telecommunication sector. This Chapter applies to all telecommunication networks or terminal equipment operated under the control of an EU institution or body[108]. Nevertheless, Regulation (EC) No 45/2001 has never been aligned with the amendment of the ePrivacy Directive. Therefore, Chapter IV appears to be now outdated and requires a thorough review.

Within the context of the evaluation study on Regulation (EC) No 45/2001, this study aims to assess (i) the relevance of the provisions of the ePrivacy Directive within the EU institutional framework and (ii) to provide suggestions for alignment. Appendix 1 includes a comparative analysis of the provisions of Regulation (EC) No 45/2001, Directive 97/66/EC, Directive 2002/58/EC and the amendment brought by Directive 2009/136/EC.

2.2.Preliminary remarks and methodology

The purpose of this case study is to assess (i) the current implementation and application of Chapter IV of Regulation (EC) No 45/2001, (ii) the relevance of the main provisions of the ePrivacy Directive in view of the amendment of the Regulation.

Methodology

In view of the future alignment and for each main provision of the ePrivacy directive, the following methodology is applied:

- Recall of the main rules and principles provided by the ePrivacy Directive and the related provisions enshrined in Regulation (EC) No 45/2001 as they are currently implemented and applied (insofar as this information is accessible);
- A comparative analysis of the provisions aiming at assessing the relevance of the alignment.

As a preliminary remark, it should be noted that in the light of the stakeholders consulted, it is difficult to assess how Chapter IV of Regulation (EC) No 45/2001 was implemented and applied throughout EU institutions and bodies. The analysis hereinafter is based on the online consultation and the interviews conducted with DPOs and EU officials of various EU institutions and bodies.

As the same level of protection must be applied in the EU institutional framework and within Member States, this study takes as a premise that the provisions of Chapter IV should be aligned with the ePrivacy Directive, unless the provisions are not relevant in the light of the particulars of the EU institutional framework.

It should be also pointed out that Regulation (EC) No 45/2001, as the ePrivacy Directive, must provide for an equal level of protection of personal data and privacy for users of internal communication services, regardless of the technologies used. Chapter IV should remain technologically neutral as concerns the evolutive technological framework. In this regard, the relevance of this chapter within the data protection framework laid down by Regulation (EC) No 45/2001 is questioned by stakeholders. Upon consultation, stakeholders indicated that there is no

[108] Article 34 of Regulation (EC) No 45/2001.

need to provide (i) for specific rules pertaining to the telecommunication sector (ii) in any case, to specific rules pertaining to the institutional framework.

2.3.Security of processing

2.3.1. The implementation of security measures

The ePrivacy Directive - Article 4 sets out a general obligation for providers of electronic communication services to implement technical and organizational measures to safeguard the security of its services. The provision as amended in 2009 enumerates a set of minimum guarantees which must be ensured, without prejudice to the provisions of Directive 95/46/EC.

Regulation (EC) No 45/2001 - Article 35 provides for an equivalent obligation to implement technical and organizational measures, without detailing a minimum set of guarantees. It shall be nonetheless underlined that Article 22 - which is applicable to any processing of personal data - lays down a similar list of security measures.

Application of Regulation (EC) No 45/2001 –It follows from the interviews conducted that EU institutions and bodies face a growing number of attacks on their telecommunication networks or terminal equipment. It appears that the main difficulty does not lie in the interpretation of Article 35.1 of Regulation (EC) No 45/2001 but in the necessity to permanently improve technical and organizational measures in order to keep an adequate security level in front of attackers.

Conclusion: alignment and suggestion

It seems that the main issue with regard to the application of Article 35 lies in the implementation of the appropriate security measures. An alignment with the provision of the ePrivacy Directive would only have a slight impact as the rules relating to the security of the services are already in the Regulation.

2.3.2. Notification of personal data breaches

The ePrivacy Directive – The ePrivacy Directive provides for the obligation that a provider of a publicly available network give notification of personal data breach. A personal data breach is "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community*"[109].

Pursuant to Article 4.2, in case of a particular risk of breach, the provider shall inform the subscribers of the existence of the risk and of any possible remedies. The 2009 amendment introduced an obligation to notify personal data breaches to the relevant national authority (Article 4.3). The provider will also notify the person concerned, when the breach is likely to affect his personal data or his privacy unless the provider demonstrates that it has implemented appropriate technical protection measures and that those measures were applied to the data concerned by the

[109] Article 2(i) of the ePrivacy Directive.

security breach[110]. The same exception applies to the notification of personal data breaches to the subscriber.

Regulation (EC) No 45/2001 – Regulation (EC) No 45/2001 does not provide an explicit obligation to notify personal data breaches. It should nonetheless be noted that Article 35.2 provides for the obligation of EU institutions and bodies to inform users of the existence of any particular risk of a breach of the network and terminal equipment security, and of any possible remedies.

Application of Regulation (EC) No 45/2001 – Several EU institutions and bodies have already implemented an obligation to notify personal data breaches to their DPO and the data subject concerned. In most cases, it appears that the personal data breaches are notified to the DPO of the institution or the body, but not systematically to the data subject concerned or the EDPS. This notification is highly dependent on the seriousness of the breach. Indeed, current practices among certain EU institutions and bodies (such as the implementing rules on security adopted by the European Commission) include the notification of personal data breaches to the DPO. This is in line with the doctrine of the EDPS which encourage institutions to adopt internal security breach procedures that involve notification by the controller to the DPO and/or the EDPS.

Analysis and suggestions for alignment – The notification of personal data breaches is "*a key tool for increasing transparency and understanding*" and "*ensures data is fully protected throughout its lifecycle but also that users are informed if a serious incident occurs that may impact them, thus creating a sense of empowerment and individuals confidence*"[111]. The Article 29 Data Protection Working Party also considers this procedure as a way to "*increase focus and effectiveness when enforcing the obligation of service providers to take appropriate security measures*"[112]. The EDPS adds that it "*enhances the accountability of the PPECS [Providers of a Public Electronic Communications Service] regarding the information which has been compromised*"[113].

These arguments confirm the relevance of the provisions of the ePrivacy Directive for EU institutions and bodies. Furthermore, as mentioned above, several EU institutions and bodies have already implemented a personal data breach notification procedure. The question raised in this regard is to whom the notification should be made in the context of EU institutions and bodies, i.e. to the EDPS and/or the DPA.

The *ratio legis* of the ePrivacy Directive aims to introduce an obligation to notify personal data breaches systematically to an external supervisory authority (i.e. the DPA for Member States and the EDPS for EU institutions and bodies).

---

[110] On 24 June 2013, the European Commission adopted Regulation (EU) No 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.

[111] Symantec Response to Commission Communication: "A comprehensive approach on personal data protection in the European Union", p.4.

[112] Opinion 1/2009 of the Article 29 Data Protection Working Party on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy directive), 10 February 2009, 00350/09/EN, WP 159, p. 4.
Also see:
Opinion 8/2006 of the Article 29 Data Protection Working Party on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive, 26 September 2006, 1611/06/EN WP126.
Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2009/C 128/04, point 10.

[113] Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2008/C 181/01), points 9, 27 to 29.

Nevertheless, it should be stressed that the notification of each incident affecting personal data would significantly increase the administrative burden of the EDPS.

Therefore, the following could be foreseen: (i) establishment of a risk threshold above which such a breach would be notified to the EDPS[114] and (ii) notification of all personal data breaches to the DPOs. In light of the current role played by DPOs, they could constitute a first step of notification and eventually revert to the EDPS for the most significant breaches.

An alignment with the ePrivacy Directive would require introducing an obligation to notify personal data breaches to data subjects concerned by the breach.

Finally, the proposed GDPR encompasses a procedure of notification of personal data breaches. Therefore, it appears that the adoption of a breach notification procedure specific to the context of internal telecommunications networks would not be necessary.

Conclusion: alignment and suggestions

An alignment with the requirements set out by the ePrivacy Directive (and with the proposed GDPR) requires introducing an obligation to notify personal data breaches to the data subject and to the supervisory authority (EDPS).

The following could be foreseen: (i) establishment of a risk threshold above which the breach would be notified to the EDPS and (ii) notification of all personal data breaches to the DPO.

2.4.Confidentiality, cookies and similar technologies

2.4.1. Confidentiality of communications and related traffic data

The ePrivacy Directive – The ePrivacy Directive provides an obligation for Member States to ensure the confidentiality of communications and related data. Communication means "*any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information*"[115].

Pursuant to Article 5, the interception or surveillance of communications requires the prior consent of the individuals concerned (i.e. the various parties of a communication[116]). The ePrivacy Directive provides for three main exceptions:

- National security, defence, public security and governance of criminal offences or unauthorized use of the electronic communication system (Article 15.1),
- Technical storage necessary for conveyance of communications (Article 5.1)
- In case of legally authorized recording of communications and related traffic data when carried out in the course of lawful business practice (Article 5.2).

[114] For example, the threshold could depend on the seriousness of the breach, the type and volume of data involved, the numbers of data subjects affected or the location of the recipient, etc.
[115] Article 2(d) of the ePrivacy Directive.
[116] Opinion 15/2011 of the Article 29 Data Protection Working Party on the definition of consent, 13 July 2011, 01197/11/EN, WP187.

Regulation (EC) No 45/2001 - Article 36 includes a general obligation for EU institutions and bodies to ensure the confidentiality of communications in their internal networks, in accordance with general principles of European legislation. The concept of communications should be interpreted broadly and includes telephone calls, e-mail messages as well as log files and traffic data.
The provision does not specify the necessity to obtain prior consent of the users concerned and does not provide for any exception.

Article 20 of the Regulation provides an exception similar to the exception of Article 15.1 of the ePrivacy Directive. Article 20.1 relates to:

- (a) the prevention, investigation, detection and prosecution of criminal offences;
- (b) an important economic or financial interest of a Member State or the European Union;
- (c) the protection of the data subject or of the right and freedoms of others;
- (d) the national security, the public security or defence of the Member States;
- (e) the monitoring, inspection or regulatory task connected with the governance of criminal offences or economic or financial interests.

However, Article 20 of Regulation (EC) No 45/2001 does not apply to Article 36 on confidentiality of communications.

Application of Regulation (EC) No 45/2001 – In practice, EU institutions and bodies may need to intercept or oversee communications and related traffic data. The technical requirements for conveyance of communications are not different from those applicable to providers of publicly available electronic communications service according to the ePrivacy Directive.
Furthermore, certain EU institutions or bodies may also need to record calls to certain helplines, security or emergency lines or switchboards aimed at a large number of users in order, for example, to be able to verify the content of the communication afterwards and provide an accurate reply, to retain evidence, for use as a training aid, etc. In setting up such tools, EU institutions and bodies have so far referred to Article 5 of the ePrivacy Directive.

Analysis and suggestions for alignment – As mentioned above, Article 36 of Regulation (EC) No 45/2001 lays down a general obligation for EU institutions and bodies to ensure the confidentiality of communications in their internal network, in accordance with the general principles of European legislation, while the ePrivacy Directive requires an additional requirement to obtain the prior consent of users. In Regulation (EC) No 45/2001, this requirement could be considered as covered and implied by the general obligation to ensure confidentiality of communications within EU institutions and bodies**, in accordance with general principles of European legislation.** However, the "notion of general principles of EU institutions and bodies" is not defined and raises interpretation issues. It could be understood as covering the general principles of necessity and proportionality but this notion remains unclear. Therefore, in order to improve protection of data subjects, introduction of this obligation should be considered in order to obtain the prior consent of users in Article 36.

As regards exceptions, an extension of the scope of Article 20.1 of Regulation (EC) No 45/2001 to Article 36 could be considered. Indeed, Article 15.1 of the ePrivacy Directive provides an equivalent exception which explicitly applies to Article 5 relating to the confidentiality of communications.

As for the exception pertaining to technical storage, in the ePrivacy Directive, it is justified by its "*automatic, intermediate and transient*" nature and its technical "*purpose of carrying out the*

transmission in the electronic communications network"[117]. Technical requirements should also be applicable to the internal communication networks of EU institutions and bodies. Therefore, an exception of technical storage is relevant in the European institutional context in view of the alignment.

Regarding the exception for lawful business when legally authorized for the purpose of providing evidence of a commercial transaction or of any other business communication (Article 5.2.), this could seem irrelevant because of the lack of business purpose within EU institutions and bodies. Nevertheless, EU institutions may engage in "business practices", for example, the European Union Bookshop of the Publication Office of the European Union. Moreover, it follows from the consultation that EU institutions and bodies already use this exception to record calls of helplines, security or emergency lines or switchboards aimed at a large number of users.[118] It could thus be relevant to introduce this exception within the framework of Regulation (EC) No 45/2001.

Conclusion: alignment and suggestion

The general obligation for EU institutions and bodies to ensure the confidentiality of communications in their internal network, in accordance with general principles of the European legislation laid down in Article 36 of Regulation (EC) No 45/2001 could be aligned with Article 5 of the ePrivacy Directive.

An alignment would require the introduction of the obligation to obtain the prior consent of users to intercept or control a communication. The Regulation should also transpose the exceptions provided by the ePrivacy Directive. In this regard:

- Article 20.1 of Regulation (EC) No 45/2001 about "*Exemptions and restrictions*" could be extended in order to cover Article 36;
- An exception for technical storage and for legally authorized lawful business purpose should be introduced.

2.4.2. Cookies and similar technologies

The ePrivacy Directive –Article 5 of the ePrivacy Directive provides specific rules related to the storing of information or the gaining of access to information already stored in the terminal equipment of a subscriber or user. In other words, these provisions concern cookies and similar technologies. A cookie can be defined as information stored by a web page server which operates a website on a user's hard drive. Other tools may use similar technology[119] such as browser

[117] See. Recital 22 of the ePrivacy Directive.

[118] See for example, EDPS Opinions of 23 January 2006 – recording of communications made over the Security centre's telephone lines, building interphones and radios used by the General Secretariat of the Council (GSC) Security, Prevention and Medical Department (C 2005-0364); 5 May 2006 – ECB recording, storing and listening of telephone conversations in DG-M and DG-P (C 2005-0376); 8 May 2006 – EIB recording of telephone communications in trading rooms (C 2006-0102); 22 May 2006 – EC recording the line reserved for emergency and security calls in Brussels (C 2006-0002).

[119] Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2008/C 181/01), point 43.
Opinion 04/2012 of the Article 29 Data Protection Working Party on Cookie Consent Exemption, 7 June 2012, 00879/12/EN, WP 194.

fingerprints[120] or search engines when they offer an additional service that falls under the scope of an electronic communications service like "analytics"[121].

In principle, service providers need to obtain the prior consent of the user in order to store information or to gain access to information already stored in his terminal equipment.

Exceptions to this general principle are provided:

- for technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network;
- or, as strictly necessary, in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

Regulation (EC) No 45/2001 – As Regulation (EC) No 45/2001 is based on Directive 97/66/EC, there is no provision regulating the use of cookies or similar technologies in the Regulation.

Application of Regulation (EC) No 45/2001 - Today, the use of cookies and similar technologies has greatly expanded. EU institutions and bodies already use these tools and some of them have adopted internal policies mainly based on the provisions of the ePrivacy Directive. For example, the European Commission offers on its website various tools aimed at helping its services and other EU institutions and bodies to implement EU legislation on cookies (i.e. Cookie Consent Kit and templates to create cookie notice pages). The DG Connect also offers in-house interactive services available for integration in EUROPA websites. A form for each service indicates whether it uses cookies or not. The European Commission explicitly refers the ePrivacy Directive as a legal source[122]. It should be noted that, by informing users about cookies, the European Commission possibly intends to cover cookies and similar technologies but the wording used is not clear.

Analysis and suggestions for alignment – Cookies and similar technologies may raise specific privacy related risks for users[123]. Despite these risks, they also have legitimate purposes such as, for example, analysing the effectiveness of website design and advertising, counting the number of visitors of the website or verifying the identity of users engaged in on-line transactions[124]. For these reasons, the ePrivacy Directive gives providers the possibility to store information or to gain access to information already stored in users' terminal equipment only if they get prior consent, on condition of prior "*clear and comprehensive information*" in order to guarantee transparency[125].
As explained above, EU institutions and bodies already use cookies and similar technologies and have implemented internal rules based on the ePrivacy Directive. Therefore it could be necessary to align Regulation (EC) No 45/2001 on Article 5.3 of the ePrivacy Directive and to introduce an

[120] Defined as "*A set of information elements that identifies a device or application instance*" by the Internet Architecture Board (RFC6973, Cooper, 2013 - Privacy Considerations for Internet Protocols) and intended "*in a broad sense, meaning that it includes a set of information that can be used to single out, link or infer a user, user agent or device over time*" by the Article 29 Data Protection Working Party (Opinion 9/2014 of the Article 29 Data Protection Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25 November 2014, 14/EN, WP 224, p. 4).
[121] Opinion 1/2008 of the Article 29 Data Protection Working Party on data protection issues related to search engines, 4 April 2008, 00737/EN, WP 148: defines search engines as "*services that help their users to find information on the Web*". Analytics is the science of examining raw data with the purpose of drawing conclusions about that information, which can be used to customize sear engines.
[122] http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm
[123] "*Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users.*", Recital 24 of the ePrivacy Directive.
[124] Recital 25 of the ePrivacy Directive.
[125] The Article 29 Data Protection Working Party underlined the importance of transparency as "*a key condition for individuals to be able to consent to the collection and further processing of their data*" (Opinion 2/2010 of the Article 29 Data Protection Working Party on online behavioral advertising, 22 June 2010, 00909/10/EN, WP 171, p.17).

obligation to obtain the prior consent of the user in order to store information or to gain access to information already stored in his terminal equipment. This could be a way to standardize practices and specify the procedure in order for EU institutions and bodies to provide clearer information to users.

Exceptions provided in the ePrivacy Directive could also be introduced in Regulation (EC) No 45/2001.
The same reasoning can be made about the exception for technical storage to the obligation to obtain prior consent for using cookies or similar technologies, as about the exception for technical storage to the obligation to ensure confidentiality of communications. Technical requirements to establish communication for the internal networks of EU institutions and bodies should be the same as for publicly available communication services.
The notion of "*information society service*" is defined by Directive 2000/31/EC and Directive 98/34/EC[126] as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*". For example, "an information society service" may be a service consisting of the transmission of information via a communication network, providing access to a communication network, hosting information provided by a recipient of the service or providing commercial communications by e-mail. Therefore, if information society services are useful for EU institutions and bodies, such an exception seems to be entirely relevant for EU institutions and bodies.

Nevertheless, it seems that the current version of the ePrivacy Directive raises practical concerns. For example, some stakeholders seem to believe that cookies used for technical management purposes such as allowing the counting of website visitors, should be an exception and may be used without prior consent. It then follows that it is necessary to introduce the rules provided by the ePrivacy Directive on cookies and similar technologies.

Conclusion: alignment and suggestion

As EU institutions and bodies already use cookies and similar technologies, and as some of them adopted internal policies, an alignment with the ePrivacy Directive would require introducing specific provisions relating to the use of cookies or similar technologies.

It could be necessary to align with the ePrivacy Directive and provide the following:

- an obligation to obtain prior consent of the user in order to store information or to gain access to information already stored in his terminal equipment;
- the recognition of two exceptions related to (i) the technical storage for transmission purpose and (ii) for the providing of information society services.

[126] Article 2(a) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) and Article 1.2 of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998, *laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services* (OJ L 204 of 21.7.1998, p.37), as amended by Directive 98/48/EC of the European Parliament and the Council of 20 July 1998 (OJ L217 of 5.8.98, p.18).

2.5. Traffic and billing data of users processed and stored by providers of communication services

2.5.1. Traffic data

The ePrivacy Directive – The ePrivacy Directive provides a provision related to the processing and the storage of traffic data by providers of communications services. Traffic data are defined as "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*"[127]. They are personal data[128] and include the identity of persons making and receiving calls, time and duration of calls, networks used, websites visited and even sometimes geographic location of users[129].

Traffic data shall be erased or made anonymous immediately after being processed and stored by providers of publicly available electronic communications services for the duration necessary to transmit communications, except for traffic data necessary for budget and traffic management.

<u>The ePrivacy Directive provides exceptions:</u>

- After prior information of the subscriber or the user, traffic data can be processed for the purpose of billing and interconnection payments, until the bill may be challenged or the payment pursued (Article 6.2);
  It has to be noted that Directive 97/66/EC (replaced by the ePrivacy Directive in 2002) previously limited the scope of this exception to traffic data enumerated in the Annex. Such a list has been withdrawn from the ePrivacy Directive version in 2002;
- For national security, defence, public security and governance of criminal offences or the unauthorised use of the electronic communication system also covers traffic data (by reference to Article 15.1);
- Traffic data can also be processed for the purpose of marketing electronic communication services or for providing value added services, after obtaining the prior consent of the subscriber or the user (Article 6.3);
- Competent bodies may access traffic data "*with a view to settling disputes, in particular interconnection or billing disputes*" (Article 6.6).

Regulation (EC) No 45/2001 – The processing of traffic data in the area of EU institutions and bodies telecommunication networks is regulated by Article 37 which contains the same principle relating to the transmission of communications (provided by the ePrivacy Directive).

This Article also provides for an exception for "*budget and traffic management*", similar to the exception of Article 6.2 of the ePrivacy Directive. As was the case in Directive 97/66/CE, this exception should be limited to traffic data enumerated in a list approved by the EDPS. This exception is also limited to a six-month duration after which data must be erased or made anonymous, unless the data need to be kept longer to establish, exercise or defend a right in a "*legal claim pending before a court*".

[127] Article 2(b) of the ePrivacy Directive.
[128] Recital 26 of ePrivacy Directive.
[129] EDPS, Guidelines on data protection in EU financial services regulation, 26 November 2014.

Moreover, Article 20.1 is applicable to Article 37.1, meaning that, by way of exception, after the establishment of calls and other connections, instead of being immediately erased or made anonymous, traffic data can be processed and stored in order to safeguard:

- (a) the prevention, investigation, detection and prosecution of criminal offences;
- (b) an important economic or financial interest of a Member State or the European Union;
- (c) the protection of the data subject or of the rights and freedoms of others;
- (d) the national security, the public security or defence of the Member States;
- (e) the monitoring, inspection or regulatory task connected with the governance of criminal offences or economic or financial interests referred to in (a) and (b).

Application of Regulation (EC) No 45/2001 – Article 37.2 provides for an exception relating to the processing of traffic data which are necessary for budget and traffic management. This data is indicated in a list subject to agreement by the EDPS. These data can be kept for a period of six months and shall be further erased or made anonymous (Article 37.2). In practice, this traffic data may be relevant in the course of investigation of criminal offences, administrative enquiries or disciplinary proceedings. Therefore, Article 20.1 is applicable to Article 37.1, meaning that, by way of exception, after the establishment of calls and other connections, instead of being immediately erased or made anonymous, traffic data can be processed and stored in order to safeguard:

- (a) the prevention, investigation, detection and prosecution of criminal offences;
- (b) an important economic or financial interest of a Member State or the European Union;
- (c) the protection of the data subject or of the right of freedoms of others;
- (d) the national security, the public security or defense of the Member States; a monitoring, inspection or regulatory task connected with the governance of criminal offences or economic or financial interests.

Stakeholders have underlined that Article 20.1 should also cover Article 37.2. Indeed, if Article 20.1 only covers Article 37.1, it would be applicable to data which has already been erased or anonymized at the time of the investigation (insofar as Article 37.1 provides for immediate erasure or anonymisation).

The EDPS has indicated that the list provided by Article 37 (2) has never been published.

Moreover, a practical difficulty of application relates to the technical feasibility to definitively erase or anonymize traffic data in communication networks which were not all designed to offer this possibility.

Analysis and suggestions for alignment – As mentioned above, Regulation (EC) No 45/2001 already contains the principle allowing EU institutions and bodies to process and store traffic data in order to establish calls and other connections, before erasing them or making them anonymous and, also, an exception for "*budget and traffic management*".

Exception for budget and traffic management - Nevertheless, for two reasons, the exception for "*budget and traffic management*" provided by Article 37.2 appears to be more limited than the exception provided by Article 6 of the ePrivacy Directive.

- 1/ The reference in Regulation (EC) No 45/2001 to a limitative list of traffic data which may be processed, by way of exception, for budget and traffic management is more restrictive than the general exception provided for in Article 6 of the ePrivacy Directive. Moreover, it follows from our interviews with the EDPS that a list has never been published. The effective publication of a list could participate in maintaining a high level of protection. In order to reflect the practice, Regulation (EC) No 45/2001 and the ePrivacy Directive could be aligned on that point.

– 2/ Likewise, the indication of a six-month maximum duration before erasing traffic data or making them anonymous could also be seen as more restrictive. In practice, it appears that this period raises certain issues.
  This retention period was in contradiction with Article 6 of Data Retention Directive 2006/24/EC[130] (invalidated[131]) which allowed Member States to conserve data no less than six months and no more than two years from the date of communication. A solution could be to extend the maximum retention period provided in Article 37.2 of Regulation (EC) No 45/2001. For example, in the context of criminal offenses or other specific inquiries, French law provides for a one-year retention period for traffic data[132].
  As mentioned above, it is impossible to access traffic data after their erasure or their being made anonymous, within the required period of six months, on the basis of Article 20.1 of the Regulation or for administrative inquiries as provided for by internal policies.

Exception for marketing purposes and value-added services - In order to determine if the exception for marketing purposes and value-added services is relevant for EU institutions and bodies, it will be determined whether or not EU institutions and bodies have marketing purposes and propose value added services. Marketing can be defined as "*the provision of goods or services to meet customer or consumer needs*"[133] so EU institutions and bodies could use such an exception to improve their communication services. According to Article 2(g) of the ePrivacy Directive, value-added services "*means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof*". Recital 28 of the Directive gives examples: "*advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information*". They may also be ring-back tone, missed call alerts and voice mail boxes. The possibility for EU institutions and bodies to provide their users with such value-added services and, as a consequence, to align Article 37 of the Regulation with the ePrivacy Directive on this specific point has to be considered.

Exception for legal claims pending before a court - Finally, the exception for legal claims pending before a court provided for in Article 37 of Regulation (EC) No 45/2001 is also more restrictive than the ePrivacy Directive's exception for settling disputes. In order to facilitate EU institutions and bodies internal procedures, the exceptions laid down in Article 37 could be enlarged to all kinds of dispute settlements.

Conclusion: alignment and suggestion

In case of alignment with the ePrivacy Directive, Article 37 of Regulation (EC) No 45/2001 should be amended as following:

- The reference to a list of traffic data agreed by the EDPS could be deleted;
- An extension could be considered for the retention period provided for the retention of traffic data for budget and traffic management in Article 37.2 or provisions made for a general principle rather than a specific retention period;
- An exception relating to marketing purposes and value-added services could be introduced;
- The exception for legal claims already existing in Article 37 should be extended to all kinds

[130] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[131] CJEU, 8 April 2014, Digital Rights Ireland Ltd and Seitlinger and Others, joined Cases C-293/12 and C-594/12.
[132] Article L. 34-1 (III) of the Code des postes et des communications électroniques.
[133] See online Collins Dictionary.

of dispute settlement.

An exception for administrative inquiries could be introduced in Article 20.1 of the Regulation.

2.5.2. Billing data

The ePrivacy Directive – Article 7 of the ePrivacy Directive provides for a general right for subscribers to receive non-itemized bills and reminds Member states of the necessity to conciliate this right with the right to privacy of calling users and called subscribers.

Regulation (EC) No 45/2001 – The fourth paragraph of Article 37 provides for the same right for users but does not explicitly state the right to privacy.

Analysis and suggestions for alignment – A reminder of the necessity to conciliate with the right to privacy of other users does not seem to be necessary within the legal framework of Regulation (EC) No 45/201 which aims to protect "*the fundamental rights and freedom of natural persons, and in particular their right to privacy with respect to the processing of personal data*"[134].

The fourth paragraph of Article 37 of Regulation (EC) No 45/2001 does not need to be modified.

2.6. Presentation and restriction of calling and connected line identification

The ePrivacy Directive – Article 8 imposes four obligations on providers where presentation of calling and connected line identification is offered, one relates to calling users, the three others to called subscribers.
First, the possibility must be given to the calling user to prevent the presentation of the calling line identification.
Therefore possibilities must be given to the called subscriber:

- to prevent the presentation of the calling-line identification of incoming calls;
- to reject an incoming call where the presentation of the calling-line identification has been prevented by the calling user;
- to prevent the presentation of the connected line identification to the calling user.

These four rules apply to calls to third countries or incoming calls from third countries. The public must be informed of these rules.

The exception of Article 15.1 in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system applies to Article 8. This means that, for specific reasons, phone lines could be identified even if the presentation of the identification is prevented.

Regulation (EC) No 45/2001 – Article 39 of Regulation (EC) No 45/2001 provides for three main rights benefitting to users, where presentation of calling or connected line identification is offered. One right relates to the calling user, two relate to the called user.

[134] Article 1 of Regulation (EC) No 45/2001.

First, the calling user will have the possibility to eliminate the presentation of the calling-line identification.
Then, the called user will have the possibility:

- to prevent the presentation of the calling-line identification of incoming calls;
- to eliminate the presentation of the connected-line identification to the calling user.

EU institutions and bodies must inform users of their rights.

As mentioned above, Article 20.1 of the Regulation provides for exceptions similar to the exception of Article 15.1 of the ePrivacy Directive (for criminal offenses, economic or financial interest of a Member State or the European Union, protection of the data subject or of the rights and freedoms of others and national security, public security or defence of the Member States, etc.).
In Chapter IV of the Regulation, these exemptions or restrictions may only apply to Article 37.1 which allows the processing and storing of traffic data to establish calls and other connections over telecommunications networks in restrictive conditions but they could be extended to other provisions as Article 39.

Application of Regulation (EC) No 45/2001 – Several stakeholders pointed out that the provisions relating to the presentation and restriction of calling and connected line identification are irrelevant and outdated, notably in the light of BYOD (Bring Your Own Device) and mobile telephones.

Analysis and suggestions for alignment
It appears that the wording of Article 39 of Regulation (EC) No 45/2001 is slightly different from the wording of Article 8 of the ePrivacy Directive, Article 39 does not impose obligations on providers but gives rights to users. Nevertheless, Article 39 and Article 8 provide for similar rules.
The main difference is that Article 39 of the Regulation does not provide for a right for the called subscriber to reject an incoming call where the presentation of the calling-line identification has been prevented by the calling user. It does not specify either the application of the rules to calls to third countries or calls incoming from third countries.

The absence of these paragraphs in Regulation (EC) No 45/2001 seems to result from a specific choice of the European legislator, since Article 8 already contained these rules in the early version of Directive 97/66/EC. Nevertheless, in view of a general updating of Regulation (EC) No 45/2001 with the current version of the ePrivacy Directive, the missing rules in those paragraphs might be added.

Finally, an extension of Article 20.1 of Regulation (EC) No 45/2001 to Article 39 could be considered. Indeed, Article 15.1 of the ePrivacy Directive provides for an equivalent exception which explicitly applies to Article 8 relating to the phone line identification. Phone line identification uses traffic data necessary to establish communications and traffic data are already covered by Article 20.1. So an extension of the exception of Article 20.1 of the Regulation to Article 39 could be considered as well.

Conclusion: alignment and suggestion

An alignment with the ePrivacy Directive would require maintaining the existing provision and aligning Article 39 of Regulation (EC) No 45/2001 with Article 8 of the ePrivacy Directive. In this case, the following could be considered:

- modifying the wording of Article 39 of the Regulation,
- introducing an obligation for EU institutions and bodies to give the possibility to users to reject an incoming call where the presentation of the calling-line identification has been prevented by the calling user;

- introducing a paragraph on obligations related to communications with third countries.

An extension to the exception of Article 20.1 of the Regulation to Article 39 could be considered.

2.7.Location data other than traffic data

The ePrivacy Directive – The ePrivacy Directive provides for rules on the processing of location data other than traffic data. Location data means "*any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*"[135]. This definition may refer to latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and up to the time the information was recorded[136].

According to the definition of traffic data stated above, location data other than traffic data are any data indicating the geographic position of the terminal equipment of a user other than data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. They are used for value added services.

Pursuant to Article 9, location data other than traffic data can only be processed when made anonymous or with prior consent of the user or the subscriber concerned to the extent or for the duration necessary for the provision of a value-added service. Prior to obtaining consent, the provider must inform the user or the subscriber. It must also give him the possibility to withdraw its consent or temporarily refuse the processing of such data. The processing of location data other than traffic data must be restricted to persons acting under the authority of the provider of the communication network or the value added service and must also be restricted to what is necessary for the provision of the value added service only.

The exception of Article 15.1 in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system applies to Article 9.

Regulation (EC) No 45/2001 – There is no provision related to location data other than traffic data.

Application of Regulation (EC) No 45/2001 – According to the stakeholders consulted, location data are not used within EU institutions and bodies. Nevertheless, the use of value-added services requiring location data other than traffic data has become more and more common. There are currently discussions concerning the implementation of systems requiring location data as, for example, mobile device management systems.

As mentioned above, Article 20.1 of the Regulation provides for exceptions similar to the exception of Article 15.1 of the ePrivacy Directive (for criminal offenses, economic or financial interest of a Member State or the European Union, protection of the data subject or of the right of freedom of others and national security, public security or defence of the Member States, etc.).

[135] Article 2(c) of the ePrivacy Directive.
[136] Recital 14 of the ePrivacy Directive.

In Chapter IV of the Regulation, these exemptions or restrictions may only apply to Article 37.1 which allows the processing and storing of traffic data in order to establish calls and other connections over telecommunications network in restrictive conditions, but they could be extended to other provisions.

Analysis and suggestions for alignment – It follows that the introduction in Regulation (EC) No 45/2001 of a provision related to location data other than traffic data could cover future needs of EU institutions and bodies. Therefore, Regulation (EC) No 45/2001 should be aligned with the ePrivacy Directive in this regard.

As traffic data are a kind of location data and Article 15.1 of the ePrivacy Directive covers both of traffic data and location data other than traffic data, if a provision related to location data other than traffic data is introduced in Regulation (EC) No 45/2001, an extension to the exceptions of Article 20.1 to this provision could be considered.

Conclusion: alignment and suggestion

In order to cover future needs of EU institutions and bodies, a provision related to the processing of location data other than traffic data could be introduced in Regulation (EC) No 45/2001 according to the model of the ePrivacy Directive.

Moreover, if a provision related to location data other than traffic data is introduced in Regulation (EC) No 45/2001, an extension to the exceptions of Article 20.1 to this provision could be considered.

2.8.Derogations

The ePrivacy Directive – Article 10 provides for two exceptions pursuant to the "*elimination of the presentation of calling line identification*". The second one also relates to "*temporary denial or absence of consent of a subscriber or user for the processing of personal data*".

Regulation (EC) No 45/2001 – Article 40 also provides for the same exception but does not refer at all to "*temporary denial or absence of consent of a subscriber or user for the processing of personal data*".

Analysis and suggestions for alignment – Should a provision on location data other than traffic data be introduced in Regulation (EC) No 45/2001, Article 40 will have to be updated and aligned with Article 10 of the ePrivacy Directive.

In the event of the modification of Regulation (EC) No 45/2001 by a provision related to the processing of location data other than traffic data, Article 40 of the Regulation providing for exceptions should be aligned with Article 10 of the ePrivacy Directive.

2.9.Automatic calls forwarding

The ePrivacy Directive – Article 11 provides for an obligation to ensure the possibility that any subscriber may stop automatic call forwarding by a third party to their terminal equipment. For

instance, the automatic call forwarding can come from a voicemail box or another telephone number where the desired called party is available.

Regulation (EC) No 45/2001 – There is no provision related to automatic calls forwarding.

Application of Regulation (EC) No 45/2001 – It seems that, in certain EU institutions and bodies, the possibility to choose to automatically forward communications from one line to another line exists. EU institutions and bodies staff members could automatically forward calls from their professional fixed telephones to their professional cellphones or another line where they would be available.

Analysis and suggestions for alignment – In order to cover this eventuality, an equivalent provision on automatic calls forwarding should be added to Regulation (EC) No 45/2001.

Conclusion

In order to cover needs of EU institutions and bodies, it a provision related to automatic calls forwarding could be introduced according to the model of the ePrivacy Directive.

2.10. Directories of subscribers

The ePrivacy Directive – Article 12 regulates the inclusion of subscribers' personal data in public directories. In any case, subscribers will be previously informed about the purpose of directories in which their personal data can be included. They will be given the opportunity to determine whether their personal data and which of them will be included in a public directory and they will be given the possibility to verify, correct or withdraw their data. In case of any directory with another purpose than the search of contact details of persons on the basis of minimum identifiers, the subscriber must give prior consent. The Article finally stipulates the necessity to protect legitimate interests of subscribers other than natural persons.

Regulation (EC) No 45/2001 – Article 38 provides for two general rules, the obligation to limit personal data contained in public directories to what is strictly necessary and the obligation to take any necessary measures to prevent personal data contained in directories from being used for direct marketing purposes.

Application of Regulation (EC) No 45/2001 – Directories exist within certain EU institutions and bodies. There can be two kinds of directories, public directories with minimum information about staff members (for example, the public directory of the European Commission) and internal directories containing additional information available only within the EU institution or body.

Analysis and suggestions for alignment – Directories of subscribers lead to the processing of personal data (for example, first names, last names, addresses, phone numbers, professions or activities, e-mails[137]) and are widely distributed and public[138]. The provision of the ePrivacy Directive is more specific and provides for additional/further rights to subscribers. As a consequence, it could be necessary to consider the opportunity to clarify Article 38 of Regulation (EC) No 45/2001.

[137] Nathalie Campagne, *La protection « informatique et libertés » des données des personnes morales en Europe*, Lamy Droit de l'Immatériel, 2014.
[138] Recital 38 of the ePrivacy Directive.

Nevertheless, within EU institutions and bodies, the right to privacy of users must be balanced with the legitimate interest of the public to have access to public institutions and bodies. For that reason, the general rule provided for in the Regulation might be sufficient.

Please note that some of the DPOs asked for the introduction in Article 38 of a right for staff members to object the inclusion of their data in a publicly accessible directory of their institution or body on legitimate compelling grounds relating to their particular situation.

Conclusion: alignment and suggestion

There are two possibilities for Article 38 of Regulation (EC) No 45/2001 concerning directories within EU institutions and bodies:

- Article 38 could be aligned with Article 11 of the ePrivacy directive because this Article provides for a higher level of protection for data subject;
- Or Article 38 could be considered as sufficient in the context of EU institutions and bodies.

In this last case, the introduction of a minimum right for staff members to object to the inclusion of their data in a publicly accessible directory of their institution or body on legitimate compelling grounds relating to their particular situation could nevertheless be considered, but it may present an excessive administrative burden. The publicly accessible directories effectively contain minimum information anyway.

2.11. Unsolicited communications

The ePrivacy Directive – Article 13 regulates unsolicited communications for direct marketing. Communications for direct marketing (automated calling, fax or electronic mail) which are conditioned on obtaining the prior consent of subscribers or users (with the exception of contact details for electronic mail obtained in the context of the sale of a product or a service and used by the same person for direct marketing of its own similar products or services). In this last case, users or subscribers must have the possibility to object to such use of their electronic contact details.
Furthermore, the following practices related to the sending of e-mails for direct marketing is prohibited:

- disguising or concealing the identity of the sender;
- no visible valid address to which a request to cease the communications can be sent;
- contravening the obligation of information laid down in Article 6 of Directive 2000/31/EC on electronic commerce[139];
- encouragement to visit websites which contravene to this obligation of information.

In principle, the ePrivacy Directive applies to natural persons only but Article 13 sets out that the "*legitimate interests of subscribers other than natural persons*" have to be sufficiently protected.

[139] Article 6 of Directive 2001/31/EC of 8 June 2000 on electronic commerce: "*In addition to other information requirements established by Community law, Member States shall ensure that commercial communications which are part of, or constitute, an information society service comply at least with the following conditions: (a) the commercial communication shall be clearly identifiable as such; (b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable; (c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously; (d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously*."

Finally, measures must be taken in order to ensure that natural or legal persons affected by the infringement of these rules may bring legal proceedings and penalties against the providers.

Regulation (EC) No 45/2001 – There is no provision related to unsolicited communications.

Application of Regulation (EC) No 45/2001 – It appears that staff members within EU institutions and bodies may receive external unsolicited communications but also some internal unsolicited communication from other EU institutions and bodies and especially from EU trade unions, without any possibility to object to these mailings.

Analysis and suggestions for alignment – The notion of unsolicited communications for the purposes of direct marketing, as set out in the ePrivacy Directive, is not clear regarding the extent to which this provision covers non-commercial unsolicited communications, for example unsolicited communications from trade unions.

Recital 40 of the ePrivacy Directive explains the notion of unsolicited communications and the reasons why they should be limited: "*Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. (...)*" This recital specifically refers to unsolicited commercial communications.

As referred to in recital 40, should "*unsolicited communications for direct marketing*" be strictly interpreted as "*unsolicited commercial communications*", Article 13 could be considered as relevant for European institutions or bodies only in a few specific cases, when EU institutions and bodies actually have business purposes and be interested in using unsolicited communications for direct marketing purposes (for example, as stated above, the European Union Bookshop of the Publication Office of the European Union).

Nevertheless, it seems that the notion of "unsolicited communications for direct marketing" is broadly interpreted by several Member States of the European Union. For example, the French supervisory authority recommends the same level of protection for data users solicited either for commercial purposes or for political purposes[140]. Following this broad interpretation, the provision on unsolicited communications could be considered relevant for European institutions and communications for newsletters, actuality information, etc. In this case, Article 13 could be considered more relevant for EU institutions and bodies.

In both cases, Regulation (EC) No 45/2001 could be aligned with Article 13 of the ePrivacy Directive but it would be necessary to specify the scope of such a provision.

Conclusion

The level of relevance of the provision laid down in Article 13 of the ePrivacy Directive for EU

[140] Commission Nationale de l'Informatique et des Libertés (CNIL) - Deliberation n° 2006-228 of 5 October 2006 on the « *recommandation relative à la mise en oeuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques* ».

institutions and bodies depends on the interpretation of the notion of unsolicited communication for purposes of direct marketing. It remains unclear to what extent this provision covers institutional or political communications (for example, communications from trade unions).

In any case, a provision related to unsolicited communications could be considered relevant for EU institutions and bodies.

2.12. Exception for national security, defence, public security and governance of criminal offences

The ePrivacy Directive – As mentioned several times below, Article 15 allows Member States to adopt restriction measures in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system. These measures must be necessary, appropriate and proportionate within a democratic society. They can affect only enumerated provisions of the ePrivacy Directive:

- Article 5 on confidentiality of communications;
- Article 6 on traffic data;
- Article 8 on presentation and restriction of calling and connected line identification;
- Article 9 on location data other than traffic data.

Regulation (EC) No 45/2001 – Article 20.1 contains exemptions and restrictions for equivalent purposes:

- (a) the prevention, investigation, detection and prosecution of criminal offences;
- (b) an important economic or financial interest of a Member State or the European Union;
- (c) the protection of the data subject or of the right of freedoms of others;
- (d) the national security, the public security or defence of the Member States;
- (e) a monitoring, inspection or regulatory task connected with the governance of criminal offences or economic or financial interests referred to in (a) and (b).

In Chapter IV of the Regulation, these exemptions or restrictions may only apply to Article 37.1 which allows for the processing and storing of traffic data to establish calls and other connections over telecommunications network in restrictive conditions.

Analysis and suggestions for alignment – As explained above, an extension of the exceptions or restrictions of Article 20.1 of Regulation (EC) No 45/2001 to all provisions equivalent to the one covered by Article 15.1 of the ePrivacy Directive could be considered.
Article 20.1 of Regulation (EC) No 45/2001 could be extended to:

- Article 36 about the confidentiality of communications;
- Article 37.2 about traffic data processed for budget and traffic management;
- Article 38 about phone line identification;
- The eventual future provision related to location data other than traffic data.

In addition, according to DPOs' opinion, an exemption for a common security or defence of the European Union should be included in Article 20.1[141]. Introducing such an exception could be considered as it would be equivalent to the exception for national security within Member States.

Furthermore, there is no restriction for the purpose of prevention, investigation, detection and prosecution of unauthorised use of the telecommunication networks. It could be helpful for the management of telecommunication networks and the supervision of data protection rules within EU institutions and bodies, especially regarding the possible management of personal data breaches notifications, to align Article 20.1 of the Regulation with the ePrivacy Directive on that point as well.

Conclusion: suggestion and alignment

In the context of internal communication networks and especially from the perspective of Chapter IV of Regulation (EC) No 45/2001, Article 20.1 of the Regulation could be aligned with Article 15.1 of the ePrivacy Directive as following:

- The scope of Article 20.1 of the Regulation could be extended to Articles 36, 37.2, 38 and to the eventual future provision related to location data other than traffic data;
- An exception related to the common security or defence of the European Union could be introduced;
- An exception for the purpose of prevention, investigation, detection and prosecution of unauthorised use of the telecommunication networks could also be introduced.

[141] DPO Network Working Groups' Follow-up Exercise, DPO Network Proposals in light of EC General DP Regulation Proposal and Reg. 45/2001.

CONCLUSION AND MAIN RECOMMENDATIONS

As a preliminary remark, it should be noted that this case study is based on the ePrivacy Directive as it was amended in 2009. In the light of the stakeholders consulted, it is difficult to assess how Chapter IV of Regulation (EC) No 45/2001 was implemented and applied throughout EU institutions and bodies. The analysis developed above is based on the online consultation and the interviews conducted with DPOs and EU officials of various EU institutions and bodies.

As the same level of protection should be applied in the EU institutional framework and within Member States, this study takes as a premise that the provisions of Chapter IV should be aligned with the ePrivacy Directive, unless the provisions are not relevant in the light of the particularities of the EU institutional framework.

It should also be pointed out that Regulation (EC) No 45/2001, as the ePrivacy Directive, must provide for an equal level of protection of personal data and privacy for users of internal communication services, regardless of the technologies used. In this regard, the relevance of this chapter within the data protection framework laid down by Regulation (EC) No 45/2001 has been questioned by stakeholders. Those stakeholders indicated that there is no need to provide (i) for specific rules pertaining to the telecommunication sector (ii) in any case, to specific rules pertaining to the institutional framework[142].

Should the introduction of a specific chapter relating to the telecommunication sector be introduced, Chapter IV of Regulation (EC) No 45/2001 should be aligned with the ePrivacy Directive except in specific cases which rely on the context of EU institutions and bodies. Indeed, the level of protection provided by EU institutions cannot be lower than the level of protection within Member States.

Chapter IV should stay technologically neutral in order to provide for an equal level of protection of personal data and privacy for users of internal communication services, regardless of the technologies used.

Still, Regulation (EC) No 45/2001 could differ from the ePrivacy Directive in order (i) to adapt to the specific context/particulars of EU institutions and bodies (ii) if the rules are already provided for in the Regulation (but not in Chapter IV).

Comparative table of Chapter IV of Regulation (EC) No 45/2001 with the ePrivacy Directive is available in the annex.

[142] IT officials of the European Commission.

Annex 1. Comparative table of Chapter IV of Regulation (EC) No 45/2001 with the ePrivacy Directive

A. Definitions

Regulation (EC) No 45/2001	Directive 97/66/EC	Directive 2002/58/EC	Directive 2009/136/EC (Article 2)
Article 34 **Scope** (paragraph 2) For the purposes of this Chapter, 'user' shall mean any natural person using a telecommunications network or terminal equipment operated under the control of a Community institution or body. *Article 2* **Definitions** For the purposes of this Regulation: (...) (h) 'the data subject's consent' shall mean any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed.	*Article 2* **Definitions** In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive: (a) 'subscriber' shall mean any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services; (b) 'user' shall mean any natural person using a publicly available telecommunications service, for private or business purposes, without necessarily having subscribed to this service; (c) 'public telecommunications network' shall mean transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electromagnetic means, which are used, in whole or in part, for the provision of publicly	*Article 2* **Definitions** **Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) ([143]) shall apply.** **The following definitions shall also apply:** **(a) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;** **(b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;** (c) 'location data' means any data processed in an electronic communications network,	2) Article 2 shall be amended as follows: (a) point (c) shall be replaced by the following: **'(c) "location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;';** (b) point (e) shall be deleted; (c) the following point shall be added: **'(h) "personal data breach" means a breach of security leading to the**

[143] OJ L 108, 24.4.2002, p. 33.

	available telecommunications services; (d) 'telecommunications service' shall mean services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting.	indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service; **(d) 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;** (e) 'call' means a connection established by means of a publicly available telephone service allowing two-way communication in real time; **(f) 'consent' by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;** **(g) 'value added service' means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;** **(h) 'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.**	**accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.';**

B. Security of processing

Regulation (EC) No 45/2001	Directive 97/66/EC	Directive 2002/58/EC	Article 2 Directive 2009/136/EC
Article 35 **Security** 1. The Community institutions and bodies shall take appropriate technical and organisational measures to safeguard the secure use of the telecommunications networks and terminal equipment, if necessary in conjunction with the providers of publicly available telecommunications services or the providers of public telecommunications networks. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. 2. In the event of any particular risk of a breach of the security of the network and terminal equipment, the Community institution or body concerned shall inform users of the existence of that risk and of any possible remedies and alternative means of communication.	*Article 4* **Security** 1. The provider of a publicly available telecommunications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. 2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available telecommunications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.	***Article 4*** Security **1. The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.** **2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.**	4) Article 4 shall be amended as follows: (a) the title shall be replaced by the following: '**Security of processing**'; (b) the following paragraph shall be inserted: **'1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:** **—ensure that personal data can be accessed only by authorised personnel for legally authorized purposes,** **—protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,** **—ensure the implementation of a security policy with respect to the processing of personal data,** **Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.';** (c) the following paragraphs shall be added:

			'3.In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay. Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so. The notification to the subscriber or individual shall at least describe the nature of the personal data breach and

			the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach. 4. Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so. Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3.The inventory shall only include the information necessary for this purpose. 5. In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the

			Commission may, following consultation with the European Network and Information Security Agency(ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article. Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2).';

C. Confidentiality of the communications

Regulation (EC) No 45/2001	Directive 97/66/EC	Directive 2002/58/EC	Article 2 Directive 2009/136/EC
Article 36 **Confidentiality of communications** Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law.	*Article 5* **Confidentiality of the communications** 1. Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14 (1). 2. Paragraph 1 shall not affect any legally authorized recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.	*Article 5* **Confidentiality of the communications** **1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.** **2. Paragraph 1 shall not affect any legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.** 3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition	5) Article 5(3) shall be replaced by the following: '**3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying**

		that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.	**out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.';**

D. Traffic and billing data

Regulation (EC) No 45/2001	Directive 97/66/EC	Directive 2002/58/EC	Article 2 Directive 2009/136/EC
Article 37 **Traffic and billing data** (paragraphs 1 to 3) 1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection. 2. If necessary, traffic data as indicated in a **list** agreed by the European Data Protection Supervisor may be processed for the purpose of telecommunications budget and traffic management, including the verification of authorised use of the telecommunications systems. These data shall be erased or made	*Article 6* **Traffic data** 1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4. 2. For the purpose of subscriber billing and interconnection payments, data indicated in the **Annex** may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment may be	*Article 6* **Traffic data** **1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).** **2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period**	

anonymous as soon as possible and no later than six months after collection, unless they need to be kept for a longer period to establish, exercise or defend a right in a legal claim pending before a court.	pursued.	during which the bill may lawfully be challenged or payment pursued.	
	3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.	3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.	6) Article 6(3) shall be replaced by the following: '3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.';
		4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent,	

3. Processing of traffic and billing data shall only be carried out by persons handling billing, traffic or budget management.	4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own telecommunications services and it must be restricted to what is necessary for the purposes of such activities. 5. Paragraphs 1, 2, 3 and 4 shall apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection or billing disputes.	for the purposes mentioned in paragraph 3. 5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities. 6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.	

Regulation (EC) No 45/2001	Directive 97/66/EC	Directive 2002/58/EC	Article 2 Directive 2009/136/EC
Article 37 **Traffic and billing data** (paragraph 4) 4. Users of the telecommunication networks shall have the right to receive non-itemised bills or other records of calls made.	*Article 7* **Itemised billing** 1. Subscribers shall have the right to receive non-itemized bills. 2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative modalities for communications or payments are available to such users and subscribers.	*Article 7* **Itemised billing** **1. Subscribers shall have the right to receive non-itemised bills.** **2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.**	

E. Directories of subscribers

Regulation (EC) No 45/2001	Directive 97/66/EC	Directive 2002/58/EC	Directive 2009/136/EC
Article 38 **Directories of users** 1. Personal data contained in printed or electronic directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory. 2. The Community institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories, regardless of whether they are accessible to the public or not, from being used for direct marketing purposes.	*Article 11* **Directories of subscribers** 1. Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from a printed or electronic directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted in part and not to have a reference revealing his or her sex, where this	*Article 12* **Directories of subscribers** **1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.**	

	is applicable linguistically. 2. Notwithstanding paragraph 1, Member States may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved does not act as a disincentive to the exercise of this right, and that, taking account of the quality requirements of the public directory in the light of the universal service, it is limited to the actual costs incurred by the operator for the adaptation and updating of the list of subscribers not to be included in the public directory. 3. The rights conferred by paragraph 1 shall apply to subscribers who are natural persons. Member States shall also guarantee, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.	2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge. 3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers. 4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.	

F. Presentation and restriction of calling and connected line identification

Regulation (EC) No 45/2001	Directive 97/66/EC	Directive 2002/58/EC	Directive 2009/136/EC
Article 39 **Presentation and restriction of calling and connected line identification** 1. Where presentation of calling-line identification is offered, the calling user shall have the possibility via a simple means, free of charge, to eliminate the presentation of the calling-line identification. 2. Where presentation of calling-line identification is offered, the called user shall have the possibility via a simple means, free of charge, to prevent the presentation of the calling-line identification of incoming calls. 3. Where presentation of connected-line identification is offered, the called user shall have the possibility via a simple means, free of charge, to eliminate the presentation of the connected-line identification to the calling user.	*Article 8* **Presentation and restriction of calling and connected line identification** 1. Where presentation of calling-line identification is offered, the calling user must have the possibility via a simple means, free of charge, to eliminate the presentation of the calling-line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis. 2. Where presentation of calling-line identification is offered, the called subscriber must have the possibility via a simple means, free of charge for reasonable use of this function, to prevent the presentation of the calling line identification of incoming calls. 3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the called subscriber must have the possibility via a simple means to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber. 4. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user. 5. The provisions set out in paragraph 1 shall also apply with regard to calls to third countries originating in the Community; the	*Article 8* **Presentation and restriction of calling and connected line identification** **1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.** **2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.** **3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.** **4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling**	

4. Where presentation of calling or connected-line identification is offered, the Community institutions and bodies shall inform the users thereof and of the possibilities set out in paragraphs 1, 2 and 3.	provisions set out in paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries. 6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.	user. 5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries. 6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.	

G. Exceptions

Regulation (EC) No 45/2001	Directive 97/66/EC	Directive 2002/58/EC	Directive 2009/136/EC
Article 40 **Derogations** Community institutions and bodies shall ensure that there are transparent procedures governing the way in which they may override the elimination of the presentation of calling-line identification: (a) on a temporary basis, upon application of a user requesting the tracing of malicious or nuisance calls; (b) on a per-line basis for organisational entities dealing with emergency calls, for the purpose of answering such calls.	*Article 9* **Exceptions** Member States shall ensure that there are transparent procedures governing the way in which a provider of a public telecommunications network and/or a publicly available telecommunications service may override the elimination of the presentation of calling line identification: (a) on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls; in this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public telecommunications network and/or publicly available telecommunications service; (b) on a per-line basis for organisations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.	*Article 10* **Exceptions** Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override: (a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service; (b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.	

H. Other provisions of the ePrivacy Directive

	Directive 97/66/EC	Directive 2002/58/EC	Directive 2009/136/EC
		Article 9 Location data other than traffic data 1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time. 2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication. 3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the	

		public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.	
	Article 10 **Automatic call forwarding** Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber's terminal.	*Article 11* **Automatic call forwarding** **Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.**	
	Article 12 **Unsolicited calls** 1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.	*Article 13* **Unsolicited communications** 1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. 2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused	7) Article 13 shall be replaced by the following: '*Article 13* **Unsolicited communications** **1. The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.** **2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly**

	2. Member States shall take appropriate measures to ensure that, free of charge, unsolicited calls for purposes of direct marketing, by means other than those referred to in paragraph 1, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls, the choice between these options to be determined by national legislation. 3. The rights conferred by paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also guarantee, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited calls are sufficiently protected.	such use. 3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation. 4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited. 5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.	and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use. 3. Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user. 4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive2000/31/EC, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited. 5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons.

			Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected. 6. Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.';

3 Access to documents vs data protection

This section presents the case study relating to the articulation between access to documents and data protection. This case study has been conducted on the basis of a thorough documentary review as well as a set of interviews with EU officials from the Council of the EU, the EU Commission and the EDPS.

This case study explores and systematises the interface between the protection of personal data and the right to privacy on the one hand, with the right of access to documents under European Union (EU) law on the other.

When assessing the potential conflict between access to documents and data protection, it is imperative to first establish the legal status of both of these rights as fundamental rights of the EU. [144] In the European Convention on Human Rights[145] the right to private life is enshrined in Article 8 and has been interpreted by the Strasbourg Court[146] to also cover a right to data protection.[147] Both rights are deeply rooted in the constitutional order of the Member States[148] and are cornerstones of democracy and the rule of law.[149] As neither the right of data protection[150] nor that of access to information[151] is absolute, both are being subject to exceptions that need to be taken into account. In particular, the right to access documents belongs to a broader principle, that of openness, [152]which has progressively been integrated in European law[153]. Currently enshrined in Article 1 TEU ('decisions are taken as openly as possible to the citizen') and Article 15 TFEU ('EU's institutions shall conduct their work as openly as possible'), this principle expresses the precepts of good governance and, as such, is instrumental to the enjoyment of the newly Treaty-sanctioned right to participate in the democratic life of the Union[154].

3.1. The relationship between Regulation (EC) No 45/2001 and Regulation (EC) No 1049/2001

These fundamental rights have respectively been implemented in Regulation (EC) No 45/2001, which regulates and guarantees the protection of individuals' data by the EU institutions[155], and

[144] The Treaty on the functioning of the Union establishes the right to data protection (Art. 16 TFEU) and the right to access documents (Art. 15(3) TFEU). The Charter protects the right to privacy (Art. 7) and the right to data protection (Art. 8), whereas also granting a right of access to documents (Art. 42).
[145] European Convention on Human Rights, CETS No. 005, 1950.
[146] European Court of Human Rights.
[147] See e.g. ECtHR, Amann v. Switzerland, App. no. 27798/95, ECHR 2000-II, para 65; ECtHR Rotaru v. Romania [GC] App. No. 28341/95, ECHR 2000-V, para 43.
[148] H. Kranenborg & W. Voermans, Access to information in the European Union – A comparative Analysis of EC and Member State Legislation, (Groningen: European Law Publishing, 2005).
[149] Opinion AG Sharpston, Case C-28/08 P European Commission v. Bavarian Lager Co. Ltd., [2010] ECR I-6055, para. 1.
[150] As the Court held in Schecke and Eifert, the right to the protection of personal data is not absolute, but 'must be considered in relation to its function in society'. See Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063, paras 47-48.
[151] Opinion of Advocate General Geelhoed, Case C-266/05 P Sison v. Council [2007] I-1233, point 24.
[152] A. Alemanno, Unpacking the Principle of Openness in EU Law: Transparency, Participation and Democracy, European Law Review, 1/2014.
[153] The first appearance of the concept of openness goes back to the Maastricht Treaty. See Article 1(2) TEU. See, on this point, B. Bugaric, "Openness and Transparency in Public Administration: Challenges for Public Law" (2004) 22 Wisconsin International Law Journal 487 and for a national perspective on the principle, see J. Ziller, "European Models of Government: Towards a Patchwork with Missing Pieces" (2001) 54 Parliamentary Affairs 102.
[154] See Article 10 TEU.
[155] The Regulation implements Article 286 of the Treaty establishing the European Communities which requires the application of data protection rules to Community institutions and bodies, as well as the establishment of an independent

Regulation (EC) No 1049/2001, which recognizes the right to access EU documents that might contain those data[156]. However, the contradicting aims of the two regulations are evident: whereas the objective of Regulation (EC) No 1049/2001 is to provide 'the fullest possible effect to the right of public access to documents'[157] ensuring transparency of the public decision-making process; Regulation (EC) No 45/2001 focuses on the protection of personal data and delimits their disclosure.[158] Therefore, a conflict may arise in cases where a document subject to an access to documents request contains data such as the names and other details of participants in a meeting organised by a Union institution or information on persons employed by the institutions.[159]

Although Regulation (EC) No 45/2001 and Regulation (EC) No 1049/2001 were adopted very close in time, their relationships and ensuing potential conflicts were not sufficiently addressed and clarified in their respective texts. Regulation (EC) No 45/2001 does not contain any provision governing the impact of the protection of personal data in access to documents procedures.[160] The access to documents Regulation, however, does list the protection of personal data amongst the exceptions to the access to documents[161]. The core provision is to be found in the mandatory exceptions to the right to access to documents in Art. 4 (1) (b) Regulation (EC) No 1049/2001:

'*The institution shall refuse access to a document where disclosure would undermine the protection of privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data*'.

Still, the interpretation of Article 4(1) (b) remains unclear as the provision raises the question whether it is all personal data that is subject to the exception and the consequential application of the data protection rules or whether this exception only applies where the data would infringe upon the privacy of the data subject.

This question whether and to what extent data protection rules as enshrined in Regulation 45 (EC) No 45/2001 apply in an access to documents request is crucial insofar as the leeway to grant access to documents becomes delimited once that Regulation applies. Under data protection rules, processing must be fair and lawful[162]. Moreover, the data subject has a right to object to such processing.[163] Additionally, Article 8 of Regulation (EC) No 45/2001 on the transfer of data to recipients other than EU institutions and bodies only allows disclosure where it is (a) necessary to perform a task in the public service or (b) where the requesting party can establish the necessity and, additionally, no legitimate interest of the data subject prevents such transfer.

---

supervisory authority. 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, OJ L 8, 12 January 2001, at 1- 22; (hereinafter: Data Protection Regulation).

[156] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31 May 2001, at 43-48; (hereinafter: Access to Documents Regulation).

[157] Access to Documents Regulation, Preamble 4.

[158] Case T- 194/04 Bavarian Lager v. Commission, [2007] ECR- II 4523, para 98.

[159] Although the debate on the conflict of access to documents and the protection of personal data already arose before the adoption of Regulation (EC) No 45/2001 and Regulation (EC) No 1049/2001, as shown by the events preceding the Bavarian Lager Case (Ombudsman Case 713/98/IJH, available via: http://www.ombudsman.europa.eu/en/cases/specialreport.faces/en/380/html.bookmark), this analysis will focus on these two Regulations as providing the current legislative framework for the debate.

[160] The only reference to access to documents to be found in Regulation (EC) No 45/2001is Preamble (15):
'*Access to documents, including conditions for access to documents containing personal data, is governed by the rules adopted on the basis of Article 255 of the EC Treaty the scope of which includes Titles V and VI of the Treaty on European Union*.'

[161] Access to Documents Regulation, Preamble 11 and Art. 4(1) (b). Yet it fails to provide enough time to the relevant EU institution to balance the two conflicting rights.

[162] Data Protection Regulation, Art. 4.

[163] Data Protection Regulation, Art. 18.

3.2. Interpretation of Article 4(1) (b) Regulation (EC) No 1049/2001: threshold vs renvoi

In September 2002, the European Ombudsman openly criticized an arising institutional practice of applying data protection rules to undermine the principle of openness in public activities.[164] In a letter to the European Commission, the Ombudsman expressed concern that data protection was *"misinterpreted as implying the existence of a general right to participate anonymously in public activities"*.[165]

In July 2005 the European Data Protection Supervisor (EDPS)[166] stepped in to clarify the scope of the privacy exception in the access to documents Regulation[167], introducing what has been referred to as the 'threshold theory'. The EDPS argued that the exception only applies where the privacy of an individual is harmed by the release of a document. Thus, even if a document contains personal data, the exception only applies where this data affects the privacy and integrity of an individual.[168] This understanding, by relying on a distinction between the right to privacy and the right to data protection, argues that not all personal data necessarily fall within the right to privacy.[169] The question whether the data concerned affect the right to privacy becomes the threshold for the application of data protection law (threshold theory).

Institutional practice in many cases, especially on the side of the Commission did, however, reflect a different approach. The Commission interpreted the provision to act as a general exception for all data in a document subject to access to document request and leads to the automatic application of data protection rules.[170] Art. 4(1)(b), in this sense, is understood to constitute a 'renvoi' to the data protection rules (renvoi theory).

3.3. The Bavarian Lager rulings

The interpretation of Art. 4(1) (b) Regulation (EC) No 1049/2001 was referred to the Court in a case considering the minutes of a Commission meeting, for which the Commission refused an application for access to documents insofar as the names of the participants in the meeting were concerned. In November 2007, the Court of First Instance (CFI, now General Court) in its judgment,

[164] European Ombudsman, The misuse of data protection rules in the European Union, Case 713/98/(IJH)GG, 25 September 2002, available via: http://www.ombudsman.europa.eu/de/cases/correspondence.faces/en/3538/html.bookmark.

[165] European Ombudsman, Letter from the European Ombudsman to the President of the European Commission regarding data protection, Case 713/98/(IJH)GG, 30 September 2002, available via: http://www.ombudsman.europa.eu/en/cases/correspondence.faces.

[166] The position of the European Data Protection Supervisor (EDPS) was created in 2001 through the data protection regulation. The mandate of the EDPS is to ensure that the European institutions and bodies correctly adhere to the data protection requirements when processing data and protect privacy rights accordingly. The EDPS cooperates with Data Protection Officers in the institutions and with data protection authorities in the Member States. In addition, the EDPS provides advice to the institutions and bodies. Moreover, the EDPS can receive complaints about alleged breaches of the data protection though EU institutions and bodies and can also investigate potential violations on own initiative. For more information see: https://secure.edps.europa.eu.

[167] EDPS, Public access to documents and data protection, Background Paper Series No.1, July 2005, available via: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/05-07_BP_accesstodocuments_EN.pdf.

[168] Ibid., p. 12.

[169] Ibid., p. 15: For example: Whereas the mentioning of a name in a document, according to the EDPS does not trigger the privacy exemption, an access to documents could be denied in cases where for example the reputation of an individual is at stake. (p. 36- 37).

[170] See e.g. the reflection of the Commission reply in European Ombudsman, Decision of the European Ombudsman on complaint 1368/2004/GG against the European Commission, 15.12.2005, available via: http://www.ombudsman.europa.eu/cases/decision.faces/en/2193/html.bookmark.

adhered to what was above introduced as the 'threshold' theory.[171] It denied the applicability of Art. 8 (b) of Regulation (EC) No 45/2001 to access to documents requests, arguing that this would contradict the objective of Regulation (EC) No 1049/2001.[172] Moreover, it also denied the data subjects' right to object under Article 18 of the data protection Regulation.[173] The Court continued by examining whether the disclosure of the names would amount to an infringement of their right to privacy and integrity, mainly under the framework of Article 8 ECHR, and came to the conclusion that this was not the case.[174] The threshold approach was also relied on in 2009 in the *Borax* cases,[175] where the CFI again assessed whether the access to documents which in this case would reveal the identity and opinions voiced by experts, supported the Commission in the context of chemicals classification. Also in this case, the Court denied that the Commission proved that the access to documents would undermine privacy. This approach advocated by the CFI received support in the literature.[176]

The Commission supported by the Council, however, successfully appealed the *Bavarian Lager* ruling of the CFI in a judgment from June 2010 of the Court of Justice of the EU (CJEU).[177] Although the Court clarified that no provision in the Regulation would establish the primacy of one regulation over the other,[178] it ruled that where a request based on Regulation (EC) No 1049/2001 seeks to obtain documents including personal data Regulation (EC) No 45/2001 applies in its entirety.[179] Thus, whenever the document contains personal data, the rules of the data protection Regulation and specifically also Article 8 governing the transfer of data and the right of the data subject to object enshrined in Article 18 become applicable.[180] The Court ruled that the Commission correctly tried to verify whether the data subjects had given their consent to a publication.[181] Importantly, the Court also emphasized that, in the context of the data protection Regulation Article 8(b), an access to documents request must provide 'express and legitimate justification or any convincing argument in order to demonstrate the necessity for those personal data to be transferred'[182]. The institution in question then must balance the interests of the parties and establish that the legitimate interests of the subject are not prejudiced.[183] The Court of Justice thus fundamentally overruled the reasoning of the Court of First Instance and established that the relationship between Regulation (EC) No 45/2001 and Regulation (EC) No 1049/2001 is governed by the renvoi theory.

[171] Case T- 194/04 Bavarian Lager v. Commission, [2007] ECR- II 4523, para 98.
[172] Ibid. paras 107 and 138.
[173] Ibid. para 106.
[174] Ibid. paras 125 and 131.
[175] Case T-121/05 Borax Europe v. Commission, [2009] ECR II-27; Case T-166/05 Borax Europe v. Commission, [2009] ECR II-28.
[176] H. Kranenborg, Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data, 45 Common Market Law Review (2008), pp. 1079-1114, I. Harden, Openness and Data Protection in the European Union, Queen's Papers on Europeanisation No, 9/2001. Still, criticism was raised with regard to the remaining ambiguity of the application of Art. 4 and 5 of Regulation (EC) No 45/2001 once an access to documents request indeed came within the remit of the privacy exemption and the denial of the right to object by the data subject. (See: H. Kranenborg, Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data, 45 Common Market Law Review (2008), pp. 1079-1114, p. 1102) Moreover, it was criticised that the narrow interpretation of the exception in Art. 4(1) (b), requiring actual harm does not correspond with the interpretation the Court took in the similarly worded public interest exception 4(1) (a) of Regulation (EC) No 1049/2001 where only reasonable foreseeability is required. (See: D. Adamski, How wide is "the widest possible"? Judicial interpretation of the exceptions to the right of access to official documents revisited, 46 Common Market Law Review (2009), pp. 521-549, p. 529).
[177] Case C-28/08 P, European Commission v. Bavarian Lager [2010] ECR I-6055.
[178] Ibid. para 56.
[179] Ibid., paras. 59-61.
[180] Ibid., para. 68.
[181] Ibid., para. 74.
[182] Ibid., para 78.
[183] Ibid. para. 78.

3.4.Criticism of the Bavarian Lager

The renvoi theory and its application by the Court of Justice in *Bavarian Lager* have been met with disapproval in the literature. Some authors even claimed that the differences in the judgments of the CFI and CJEU in the *Bavarian Lager* cases are more inspired by the outcome the respective courts favoured then the actual interpretation of the law.[184]

The renvoi approach has been criticized insofar as it might pose a risk in leading to a possible misuse of data protection arguments to restrict public access to documents.[185] The balance the Court strikes between the protection of privacy and the right to access to documents is perceived as unsound. While the Court announces that both regulations are equally applicable in the case, its approach is perceived as disregarding the access to documents regulation and its underlying Treaty enshrined principles of transparency and openness.[186] It entails the danger that the rights of data protection and privacy are expanded into a right to anonymously participate in public activities.[187] Thus, the EDPS expressed *in tempore non suspecto* (i.e. before the CJEU judgment) with reference to the *renvoi theory*: *"This solution may respect the right to data protection, but does not respect the right to public access."*[188]

The critique especially relates to the requirement that, where the data subject has not given the explicit consent to a publication of documents containing personal data, the general right of access to documents becomes dependent on the ability to demonstrate that the transfer of this personal data is necessary. This might entail a risk of undermining the general nature of the access to documents right, which according to Art. 6(1) Regulation (EC) No 1049/2001 and previous case law[189], does not have to be supported by any reasoning on the side of the applicant.[190] Whereas in the CFI ruling Art 6(1) of the access to documents Regulation serves as the core argument against the application of the data protection Regulation,[191] the judgment of the CJEU does not address the inherent conflict. The need to legitimize an access to documents request, however, is argued to touch upon the very substance of the right to access to documents.[192] It might, therefore, be in contradiction with the doctrine regarding the balancing of fundamental rights, which requires the

[184] D. Curtin 'The role of judge-made law and EU supranational government: a bumpy road from secrecy to translucence' in M. Dougan, N.N. Shuibhne & E. Spaventa (Eds.), Empowerment and disempowerment of the European citizen (Modern studies in European law, 35) (Oxford: Hart, 2012), p. 101-127, p.119.
[185] S. Peers, The New Regulation on Access to Documents: A Critical Analysis, Yearbook of European Law (2001) 21 (1): 385-442; I. Harden, Openness and Data Protection in the European Union, Queen's Papers on Europeanisation No, 9/2001, p. 19.
[186] P. Leino, 'Just a little sunshine in the rain: the 2010 case law of the European Court of Justice on access to documents', 48 Common Market Law Review 48 (2011), pp. 1215-1252, p. 1238.
[187] European Ombudsman, Letter from the European Ombudsman to the President of the European Commission regarding data protection, Case: 713/98/(IJH)GG, 30.09.2002, available via: http://www.ombudsman.europa.eu/en/cases/correspondence.faces/en/3539/html.bookmark; P. Leino, 'Just a little sunshine in the rain: the 2010 case law of the European Court of Justice on access to documents', 48 Common Market Law Review 48 (2011),pp.. 1215-1252, p. 1239; D. Curtin 'The role of judge-made law and EU supranational government: a bumpy road from secrecy to translucence' in M. Dougan, N.N. Shuibhne & E. Spaventa (Eds.), Empowerment and disempowerment of the European citizen (Modern studies in European law, 35) (Oxford: Hart, 2012), p. 101-127, p.121.
[188] EDPS, Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents O.J. 2009, C 2/03, para. 37.
[189] Joined cases C-174/98 P and C-189/98 P Netherlands and van der Wal v Commission [2000] ECR I-1 para 27; Case T 211/00 Kuijer v. Council [2002] ECR II-485, para 55; Joined Cases T-391/03 and T-70/04 Franchet and Byk V. Commission [2006] ECR II-2023, para 84; Case T-174/95, Svenska Journalistförbundet v. Council, [1998] ECR II-2289, § 110.
[190] H. Labayle, Openness, transparency and access to documents and information in the EU, Note, European Parliament, DG for Internal Policies, Policy Department C – Citizen's Rights and Constitutional Affairs, 2013, p. 21.
[191] Case T- 194/04 Bavarian Lager v. Commission, [2007] ECR- II 4523, para. 107.
[192] H. Kranenborg, Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data, 45 Common Market Law Review (2008), pp. 1079-1114, p. 1099.

weighing of the protected interests, in order to come to a proportionate outcome without harming the substance of the rights in questions.[193]

The Court insisted however that "*according to Article 1(1) of Regulation (EC) No 45/2001, the purpose of that Regulation is to 'protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. That provision does not allow cases of processing of personal data to be separated into two categories, namely a category in which that treatment is examined solely on the basis of Article 8 of the ECHR and the case-law of the European Court of Human Rights relating to that article and another category in which that processing is subject to the provisions of Regulation (EC) No 45/2001*". In its view, "*it is clear from the first sentence of recital 15 of Regulation (EC) No 45/2001 that the Union legislature has pointed to the need to apply Article 6 EU and, by that means, Article 8 of the ECHR, '[w]here such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation, in particular those laid down in Titles V and VI of the [EU Treaty in its version prior to the Treaty of Lisbon]'. By contrast, such a reference was not found necessary for processing carried out in the exercise of activities within the scope of that Regulation, given that, in such cases, it is clearly Regulation (EC) No 45/2001 itself which applies*". Therefore, it would follow that"*where a request based on Regulation No 1049/2001 seeks to obtain access to documents including personal data, the provisions of Regulation (EC) No 45/2001 become applicable in their entirety, including Articles 8 and 18 thereof*".[194]

3.5. The case- law post Bavarian Lager

The subsequent case law provided further detail on the protection of personal data in the context of access to documents. In the *Valero Jordana* case, the General Court confirmed the CJEU *Bavarian Lager* ruling.[195] However, the Court made clear that the Commission's argument that the applicant had to file a request under Regulation (EC) No 45/2001 instead of Regulation (EC) No 1049/2001 where an access request concerns documents containing personal data, was invalid. Thus, a separate request under the data protection Regulation is not required, as the institution concerned needs to automatically apply the data protection rules in access to documents requests whenever personal data might be affected.[196]

The Court, furthermore, clarified in *Internationaler Hilfsfond* that the privacy exception does not extend to data that concern the applicant of an access to documents request; however, the exception then still prevents a disclosure to the general public.[197] Moreover, it was established that institutions may not simply exclude a whole category of data – like the identity of former MEP assistance – from access, but needs to assess, in every case, if this would *"specifically and effectively undermine the right to privacy."*[198]

Most interesting is however the Courts' further analysis of the requirements under Article 8(b) of the data protection regulation. Overall, the *Bavarian Lager* appeal ruling still leaves open the question of how to attain a proportionate balance between access to documents and personal data.

[193] See Case C-112/00 Eugen Schmidtberger, Internationale Transporte und Planzüge v. Republik Österreich, [2003] ECR I-5659.
[194] An early interpretation of the relationship between the two regulations can be found in C. Naômé, The Case-Law of the Court of Justice and of the Court of First Instance of the European Communities on Transparency: From Carvel to Hautala II (1995-2001), in V. Deckmyn, Increasing Transparency in the European Union, 2002.
[195] Case T-161/04 Gregorio Valero Jordana v. European Commission, [2011] ECR II-215, para. 87.
[196] Ibid., para. 99-103.
[197] Case T-300/10 Internationaler Hilfsfond v. Commission, published in the electronic Report of Cases, para. 107 and 108.
[198] Case T-190/10 Egan & Hackett v. European Parliament, published in the electronic Report of Cases, Paras. 93- 94 and 101.

Where an access to documents applicant under Article 8(b) tries to legitimize a request no guidance is provided in the judgment on how to assess such justification.[199]

An insight in the balancing exercise under Article 8(b) is provided by the *Dennekamp* case in which a journalist asked the Parliament to provide the names of MEPs that benefited from an additional pension scheme.[200] The applicant tried to justify his request through the inherent interest of the public, and the accountability and transparency with regard to the spending of public funds.[201] The General Court, however, established a very high standard for the reasoning required under Art. 8(b) data protection Regulation and found that the applicant was not able to demonstrate the necessity of a data transfer.[202] The Court specifically held that the applicant failed to prove not only that the data was necessary for the purpose he pursued but also to establish that it was necessary and proportionate to the public interest invoked..[203] The judgment has been met with criticism based on the fact that it remains unclear how necessity and proportionality should be proven.[204] Moreover, arguments have been advanced that the Court's findings will seriously impair on the accountability function carried out by journalists.[205]

A similar logic to the reasoning in *Dennekamp* was applied in a case involving the rejection of an NGO request of access to documents by the European Food Safety Authority (EFSA). The NGO wanted information on participants of an expert meeting linked to statements made at that meeting, but - according to the Court - it failed to prove necessity of the data transfer.[206]

In the meantime, Mr Dennekamp brought another action against a new decision of the Parliament not to grant him access to the requested data on 22 February 2013.[207] The case is not yet decided, but the EDPS has again intervened arguing in favour of the applicant and for the preservation of a watchdog function of the press.[208]

Recently, in *Strack v. Commission*, the Court also explicitly clarified that a claim that access to documents would always be in the public interest and would justify a disclosure under Art. 8(a) data protection regulation has been deemed unjustified.[209] Reliance on the general principle of transparency as providing an overriding public interest was similarly disregarded by the Court, which ruled instead that '*such general considerations cannot provide an appropriate basis for establishing that, in the present case, the principle of transparency was in some sense especially pressing and capable, therefore, of prevailing over the reasons justifying the refusal to disclose the documents in question*.'[210]

---

[199] EDPS, Public access after Bavarian Lager, Background Paper, 24.03.2011, available via: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf, p. 6.
[200] Case T-82/09 Geert-Jan Dennekamp v. European Parliament [2011] ECR II-00418.
[201] Ibid, para 32-33.
[202] Ibid, para 31.
[203] Ibid, para 34.
[204] D. Adamski, 'Approximating a Workable Compromise On Access to Document: The 2011 Developments in the European Courts', 49 Common Market Law Review 521-558 (2012), p. 545.
[205] Ibid.; D. Curtin 'The role of judge-made law and EU supranational government: a bumpy road from secrecy to translucence' in M. Dougan, N.N. Shuibhne & E. Spaventa (Eds.), Empowerement and disempowerement of the European citizen (Modern studies in European law, 35) (Oxford: Hart, 2012), p. 101-127, p.121.
[206] Case T-214/11 ClientEarth and PAN v. EFSA, Not yet published. Currently an appeal is pending before the Court of Justice (Case C-615/13 P).
[207] Case T-115/13 Dennekamp v European Parliament, pending.
[208] EDPS, Pleading before the General Court Case T-115/13 Dennekamp v European Parliament Luxembourg, 19 November 2014, available via: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2014/14-11-17_EDPS_pleading_Dennekamp_II_EN.pdf.)
[209] Case C-127/13 P Strack v. Commission, not yet published, para. 108.
[210] Ibid., para 131.

Additionally, when applicants tried to substantiate the necessity of a data transfer not on a more general reasoning regarding transparency and accountability but by claiming that the documents requested are required in ongoing court proceedings, these claims were also denied.[211]

3.6. Proposed solutions for the resolving the conflict

Given the current persisting uncertainties and the criticism directed against the judicial solution of the conflict between privacy and access to documents, there have been calls in the literature for express legislative rules of conflict to be enshrined either in the access to documents Regulation or the data protection Regulation.[212]

3.6.1. The EU Commission's approach: staff vs other personal data

One proposal for a conflict rule has been advanced by the European Commission entailing the possible disclosure of names, titles and function of civil servants and holders of public offices as well as interest representatives in the context of their professional activities, while maintaining the applicability of the data protection legislation for other personal data.[213] The EU Commission in its current practice relating to the requests for access to documents containing the names of its staff, such as emails, seems to have largely operationalized such an approach. Those requests are no longer automatically granted, but subject to a proof of the need for disclosure, which once established has to be balanced against the interest for privacy of the staff members concerned. In particular, within the framework of this examination, the test of necessity is very narrowly interpreted and, in any event, the applicant must prove that 'no data subjects' legitimate interests might be prejudiced' in the light of Article 8(b). Should the test not be satisfied, the personal data are erased and a redacted version of the document, i.e. email/correspondence, could be disclosed. It must however be underscored that this policy applies only to staff members below senior manager positions, i.e. below the level of Director-General and Deputy Director-General.

3.6.2. The EP's proposed approach: an overriding public interests clause

Another approach, which was originally advanced by the EDPS[214], backed up the literature[215] and eventually reflected in the proposal of the European Parliament[216] for the revision of the access to documents regulation, is to include an overriding public interests clause. This would allow for the

[211] Case T-300/10 Internationaler Hilfsfond v. Commission, published in the electronic Report of Cases; Case T-190/10 Egan & Hackett v. European Parliament, published in the electronic Report of Cases.
[212] H. Kranenborg, Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data, 45 Common Market Law Review (2008), pp. 1079-1114, p. 1103.; see also EDPS, p. 8.
[213] European Commission, Proposal for a Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents, (COM (2008) 229 final).
[214] EDPS, Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents O.J. 2009, C 2/03, para. 50.
[215] H. Kranenborg, Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data, 45 Common Market Law Review (2008), pp. 1079-1114, p. 1110; D. Curtin 'The role of judge-made law and EU supranational government: a bumpy road from secrecy to translucence' in M. Dougan, N.N. Shuibhne & E. Spaventa (Eds.), Empowerement and disempowerement of the European citizen (Modern studies in European law, 35) (Oxford: Hart, 2012), p. 101-127, p. 122.
[216] European Parliament, Proposal for a regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (recast), OJ C 87E , 1.4.2010, p. 362–380.

publication of otherwise protected data where such public interests weigh more than the interests of the data subject.

A recent, highly publicized judgment on data protection, not in the remit of Regulation (EC) No 45/2001 but of Directive 95/46/EC[217] which harmonizes the data protection rules of the Member States, might provide a useful insight on balancing the right to data protection with other rights. In *Google Spain*[218] a Spanish citizen successfully claimed a right to remove a link containing personal information from the results displayed in a search engine upon searching his name. The Court of Justice introduced a right to deletion of such information ('right to be forgotten'), where such information is inaccurate, inadequate, irrelevant or excessive in relation to the processing purpose.[219] However, the Court acknowledged that this right is not absolute and must be balanced with other rights such as the legitimate interest of the public.[220] The balancing then needs to take into account *"the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life*."[221] Thus, in this context, the Court acknowledged that a public interest in the private data might overrule the protection awarded to the data subject.

In addition to the introduction of an overriding public interest, the Parliament's proposal also deletes the reference to the data protection legislation from the proposed privacy exception, which would entail that privacy as opposed to data protection again becomes the central trigger for the exception and that the fundamental right to privacy will be used to assess whether access can be granted.

3.6.3. The EDPS' proposal: proactive approach

In the absence of a legislative conflict rule, the EDPS advocated a 'proactive approach' of the institutions in addressing potential conflicts between data protection and access to documents.[222] In essence, the EDPS encourages the institutions to provide information to data subjects regarding the potential public disclosure of their data before or during the collection of such data. Moreover, the EDPS envisages the possibility for the EU institutions – in the light of the Treaty based values of openness, good administration and good governance – to create general policies with regard to openness of data concerning e.g. public persons in official capacity. This is what the EU Commission has done in the framework of its new policy in relation to requests for access to documents involving the personal data of its staff members (below senior manager positions). A proactive disclosure of documents would also be possible on the basis of Article 5(a) Regulation (EC) No 45/2001, which allows the processing where it is necessary for the performance of tasks carried out in the public interest.[223] Such proactive disclosure would then still need to be subject to an exception where the legitimate interest of data subject prevents disclosure. Furthermore, the collected data needed to be necessary and proportionate in relation to the aim pursued.[224]

[217] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).
[218] Case C-132/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, [2014] not yet published.
[219] Para 93.
[220] Para 99.
[221] Para 81. See also para 97 & 99.
[222] EDPS, Public access after Bavarian Lager, Background Paper, 24.03.2011, available via: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.
[223] Ibid., p.9.
[224] Ibid., p.10.

The challenge represented by the implementation of a proactive approach to publishing data is exemplified in the context of the publication of declarations of interest (DOIs) by many institutions and bodies in the EU to manage and demonstrate the independence and objectivity of staff members and experts. Since such declarations per definition will reveal personal data such as former employers or financial interests, a careful balancing of transparency and privacy needs to be ensured. The EDPS has in this case recently provided guidance for the publication of DOIs, with distinguished rules depending on factors such as the legal basis for requiring a DOI, the various positions within the institutions and bodies, and the means of publication (e.g. internet).[225] The level of detail in this guidance document shows that general rules are difficult to formulate, as the delicate balance between privacy and transparency is influenced by a large array of factors and needs to be assessed on a case-by-case basis.

In this regard, the EDPS proposal published after the *Bavarian Lager* ruling also fails to provide detailed rules required by the institutions when balancing the right to access documents with the right to privacy.[226] To address this concern, a follow-up document providing further guidance is expected to be published by the EDPS in 2015.

The rapid digitalization of the regime governing the access to EU documents may provide a chance to make the proactive approach operational at more reasonable costs than would currently be the case. Should the EU institutions embrace case management systems – defining *ex ante* what should be part of the file – this would significantly facilitate the task of determining what could be disclosed and what should not. The pilot project Public Access to the EU by the European Parliament aims at incorporating and testing such an approach.

3.6.4. The revision of Regulation (EC) No 45/2001 as an opportunity to address the tension between access to documents and data protection

Although the case of the Court of Justice strived to identify a *modus vivendi* in the application of Regulation 1049/2001 and Regulation (EC) No 45/2001, this does not entirely address the tension existing between these two regulations. The source of this tension lies in the textual conflict between Article 6(1) of Regulation 1049/2001 – which explicitly states that applicants for access to documents are not obliged to state reasons for the application – and Article 8(b) of Regulation (EC) No 45/2001 – which states that the recipient must establish the necessity of having the data transferred.

Hence, today the question arises whether the revision of Regulation (EC) No 45/2001 might provide the EU legislator with an opportunity to explicitly address - and possibly solve - this textual conflict. Therefore, to tackle the current problem of reconciling Article 8(b) of Regulation (EC) No 45/2001 with Article 6(1) of Regulation 1049/2001, one should explore whether there is a way to deal with this via a specific provision in the new, revised Regulation (EC) No 45/2001.

In so doing, it must first be observed that it appears most likely that in the case law of the Court of Justice on the relations between access to documents and data protection (*Bavarian Lager*) the renvoi theory will continue to prevail over the threshold one. As a result, the new, revised Regulation (EC) No 45/2001 could start from the premise that under Regulation 1049/2001 – as

[225] EDPS, Guidelines on the processing of personal data with regard to the management of conflicts of interest in EU institutions and bodies, 8.12.2014, available via: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-12-08_CoI_Guidelines_EN.pdf.

[226] EDPS, Public access after Bavarian Lager, Background Paper, 24.03.2011, available via: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

interpreted by the Court in *Bavarian Lager* – data protection rules can limit the access to documents (Article 4–1-b) and that the applicant must comply with Article 8 (b) of Regulation (EC) No 45/2001 and justify the necessity to obtain the personal data.

Given this set of premises, this case law could be codified in the revised regulation along these lines so as to solve the existing tension between the two regulations.

To this purpose a recital could be inserted into the preamble of the revised Regulation so as to provide for specific provisions relating to the processing of personal data and public access to documents.[227]

The text of the revised regulation might in turn contemplate a provision – entitled '*Processing of personal data and public access to documents*' –embracing the Court's approach (renvoi theory). This new provision would address and solve the current problem of reconciling Article 8(b) of Regulation (EC) No 45/2001 with Article 6(1) of Regulation 1049/2001 at its roots.

Yet, doubts remain as to whether such an approach could entirely address the existing tension. This is true insofar as the suggested revision of Regulation (EC) No 45/2001 would entail – in essence – to reverse the burden of proof in providing the necessity for disclosing personal data. This might go against the spirit of the access to documents regime as it is enshrined in EU primary law

The EU legislator might therefore consider that Regulation 1049/2001 could possibly be better placed to address the existing tension with Regulation (EC) No 45/2001. This appears all the more true should one consider that, besides Article 6(1), the protection of personal data is expressly mentioned in it as one of the grounds to refuse public access - Article 4(1)(b). More critically, the EU framework protecting personal data implies a certain level of 'protection', which suggests that establishing a higher threshold in terms of possible public access might contrast with other legal frameworks interfering with the rules on public access to documents, such as for instance Regulation (EC) N° 1367/2006. Thus, Article 6 of the latter clearly establishes that an overriding public interest shall be deemed to exist for all information related to 'emissions in the environment', thus lowering the threshold for public access with regard to this type of information/documents.

This set of both textual and systemic considerations would rather suggest maintaining the principle that is the recipient of the personal data who has to determine the necessity for the transfer in the revisions of the Data Protection Regulation (notably Articles 7-9). In other words, Regulation (EC) No 45/2001 might not be the best legislative instrument capable of addressing the tension existing access to documents and data protection.

3.7.Conclusion

Although the case law of the Court did contribute to clarifying the application of Art. 4(1)(b) of Regulation (EC) No 1049/2001, several ambiguities and points of dissatisfaction remain with regard to the conflict between the rights to privacy and data protection and the right to access documents. A legislative rule addressing the conflict could clarify the situation.

In this regard, Regulation (EC) No 1049/2001 appears to be the privileged instrument to foresee instances to deny access to documents and *a fortiori*, to lay down the conflict rule. *The question of the possible amendment of Regulation (EC) No 45/2001 to address this issue shall however – as*

[227] The text of the recital might possibly read along those lines: 'In order to ensure that public administrations can operate transparently, and that a balance can be struck between the protection of personal data and the right of access to documents, this Regulation foresees specific provisions relating to the processing of personal data and public access to documents'.

demonstrated above – be addressed by the EU Commission in the framework not only of its review, but also in the framework of the EU broader legal regime for data protection.

While awaiting such a conflict rule, EU institutions and bodies seem – as illustrated above – increasingly being called upon to establish proactive policies with regard to potential publication of personal data. Yet the question remains how to actually operationalize such an approach in a consistent fashion across time and within the existing statutory and resource constraints.

Although tempting, it might be risky to envisage and adopt a one-size-fits-all solution across EU institutions and policy areas. This appears to be the case as the weight and role of personal data differ considerably depending on whether these are included in documents related to legislative making or in other activities such as enforcement, inspection or advisory.

4 Data retention within the HR context

This section presents the case study relating to the conservation of staff members' personal data by the institutions and bodies of the European Union (hereinafter the "EU") in the human resources context.

The case study was conducted on the basis of the results of the e-survey on Regulation (EC) No 45/2001, specific interviews[228] *performed with the staff members of the European Commission (with members of the Directorate-General for Human Resources and Security and of the Directorate-General for Informatics (hereinafter "DG HR" and DG DIGIT")), a selection of EU institutions and bodies and a thorough review of documents such as EU legislation, internal rules of EU institutions and bodies and abstracts of registers of Data Protection Officers (hereinafter "DPOs").*

4.1.Introduction

Pursuant to Article 4(1) (e) of Regulation (EC) No 45/2001, "*Personal data must be kept in a form which permits identification of data subjects for* ***no longer than is necessary for the purposes for which the data were collected or for which they are further processed****. The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes*."

This provision lays down the general principle of limited retention period of personal data, i.e. retention limited to the period of time necessary for the purposes for which the data have been collected or for which they are further processed.

The application of this principle is a source of concern, as some EU institutions have difficulties with properly estimating the periods in which retention is *de facto* necessary. In some cases, the European Data Protection Supervisor (hereinafter "EDPS") openly criticised the long retention periods it detected.[229] Therefore, after a preliminary section on the difficulties raised by data retention within the EU institutional framework (4.2), this case study aims at analysing the applicable rules and the current data retention practices of EU institutions and bodies relating to processing operations carried out in the human resources context (4.3).

4.2.General remarks on data retention within the EU institutional framework

4.2.1. Preliminary remark: focus on archiving

Within the EU institutions and bodies, staff members' documents may be retained for long period of time by invoking the necessity to constitute public archives.

[228] Interviews performed are confidential, in this respect no names or sources are reported here.
[229] See the letter from Sophie Louveaux (EDPS Head of Unit Supervision and Enforcement) and Hielke Hijmans (EDPS Head of Unit Policy and Consultations) to Marie-Hélène Boulanger (European commission, DG Justice) dated 2 October 2013, where EDPS spoke about "an administrative tradition of the EU institutions to keep data for an indefinite period".

In this regard, Article 15 of the Treaty on the Functioning of the European Union (TFEU) provides for any citizen of the Union and any natural or legal person residing or having its registered office in a Member State the right to access documents of the European Parliament, the Council of the European Union and the European Commission.

The purpose of archiving is two-fold: (1) to enable the exercise of the rights of citizens, organisations, states and European authorities and (2) to constitute historical, statistical and scientific legacy.

The articulation between regulations on archives and data protection regulation may appear difficult, especially on the topic of data retention and the exercise of rights of data subjects *(on this specific point please also refer to part of the final report regarding Coherence).* Several of the consulted stakeholders have stressed the operational difficulties faced notably by documentalists.

It is interesting to note that, under French law, three levels of public archives have been identified[230]:

- **Standard archives**: documents remain available for the daily activities for which they were constituted;

- **Intermediate archives:** after closure of the file, case or activity for which they were constituted, documents remain available for administrative needs (i.e. administrative management, legal actions).

Administrative retention periods correspond to standard and intermediate archives, governed by data protection law.

- **Definitive archives: at the end of the administrative retention period, administrative documents have no more interest for direct administrative purposes, but some of them may have a historical, scientific or patrimonial interest, or a general interest because of their legal value. These interests justify the retention of some documents containing personal data for a longer period. Making them anonymous would be a way to respect personal data protection rules but it could also eliminate the historical, scientific, patrimonial or legal interest of the document. As a consequence, systematically making them anonymous is not an option. Instead appropriate protection measures should be taken for their storage. Access to these documents should be limited. These definitive archives are governed by regulations on archives.**

This classification could apply to administrative documents and archives of EU institutions and bodies. In order to distinguish documents that should be destroyed at the end of the administrative retention period from documents which should be conserved as definitive archives, clear administrative retention periods should be identified and effective sorting procedures should be taken.

The analysis of the Common Commission-Level Retention List for European Commission's Files[231] (hereinafter the "CRL"), an internal document which establishes the retention periods for the different types of Commission files, highlights that such procedures already exist within the European Commission. For each type of file, this schedule identifies an administrative retention

[230] See Françoise BANAT-BERGER, « *Archives et protection des données personnelles* », Revue Lamy Droit de l'Immatériel 2013/95, n°3177.
CNIL, Deliberation n°88-052 of 10 May 1988 on « adoption d'une recommandation sur la compatibilité entre les lois n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et n°79-18 du 3 janvier 1979 sur les archives ».
[231] Common Commission-Level Retention List for European Commission Files – First Revision, adopted on 17 December 2012, SEC(2012)713, first version adopted on 4 July 2007, SEC (2007) 970.

period during which the department in charge is required to keep a file, depending on its usefulness for administrative purposes and the relevant statutory and legal obligations. This schedule also identifies the action to be taken by the department in charge at the end of the administrative retention period. Three different actions are possible:

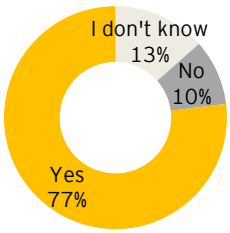
- Direct transfer to historical archives;
- Choice of a group of files for preservation and destruction of the remainder, transfer of preserved documents to historical archives;
- Destruction.

4.2.2. Existence of internal policies

A major part of the EU's institutions and bodies have implemented internal procedures on data retention.

77% of the data controllers interviewed through the online survey confirmed the existence of internal procedures on data protection in their institutions:

Q130: Are you aware of any procedures/internal rules that define storage / retention periods according to the nature of data processing operation?



It seems the European Parliament issued a Common Retention List and specific retention lists at the level of each directorate-general, internal regulatory documents setting up administrative retention periods for European Parliament's documents[232].

The most common procedure cited by data controllers is the Common Commission-Level Retention List for European Commission. The first version of this list is dated 2007 but it was modified in 2012.

Within the European Commission, the second version of the CRL dated 2012 regulates data retention issues. The CRL recommends administrative retention periods for different kinds of files, starting from the closure of the file. Where there is no duration indicated, the data controller chooses reasonable retention periods in consultation with the DPO and eventually with the EDPS. The CRL can be applied by the agencies and is considered a reference document for many EU institutions and bodies.

The European Commission also established retention lists at the level of certain directorates general or offices. For instance, the Commission established a specific retention list for the European Commission's Office for the Administration and Payment of Individual Entitlements or Pay Master Office (hereinafter "PMO") which identifies administrative retention periods of documents in the field of administration, calculation and payment of financial entitlements of the staff of the European Commission and certain other EU institutions and bodies (i.e. salaries and allowances, reimbursement of experts and mission expenses, health insurance and accident cover, pensions, unemployment)[233].

[232] Rules on document management in the European Parliament, Bureau Decision of 2 July 2012.
[233] « *Liste spécifique de conservation PMO* », European Commission, Ref. Ares(2011)1049880 – 04/10/2011.

However, even if data retention periods may be defined in certain EU institutions and bodies, there may still be inconsistencies in proportionality and application of these periods.

4.2.3. Difficulties highlighted by stakeholders

Despite the existence of internal policies on data retention, EU institutions and bodies face considerable difficulties when it comes to implementing and applying provisions on data retention of Regulation (EC) No 45/2001. Many of the stakeholders interviewed emphasised the great inconsistencies of practices in data retention. They highlighted numerous issues:

(i) the complexity of data retention procedures in the field of human resources because of the quantity and the diversity of collected data and necessary processing operations;
(ii) the lack of sufficiently operational guidance available;
(iii) conflicts between existing sources;
(iv) the inappropriateness of EDPS guidance when it comes to addressing operational requirements. Indeed, they emphasize the point that guidelines or opinions recall general principles without providing clear practical recommendations on applicable data retention periods and starting dates of these periods;
(v) difficulties to conciliate data retention periods and technical possibilities of IT systems used by EU institutions and bodies.

These issues result in a great loss of efficiency and effectiveness as (i) data controllers and DPOs lose a considerable amount of time in determining applicable retention periods and as (ii) data retention periods are not systematically applied. Moreover, there are inconsistencies in data retention periods applicable to data processing operations pursuing the same purposes across EU institutions and bodies.

4.2.4. Methodology followed to conduct the analysis of the EU institutions and bodies current practices concerning data retention within a Human Resources context

As a complete and exhaustive study of all applicable and applied data retention rules and practices in each EU institution and body appears unrealistic, the case study covers three HR purposes: processing related to recruitment management, disciplinary proceedings and staff evaluations in order to clearly show the shortcomings and inconsistencies in the retention period applied and operational difficulties faced by EU institutions and bodies.

For each purpose, the same method has been applied to challenge current practices on data retention of EU institutions and bodies. As explained below, this method relies on the comparison of data retention periods from different sources:

- EDPS thematic Guidelines;
- EDPS Opinions issued in the course of the prior checking procedure;
- The Common Commission-Level Retention List;
- DPOs Registers of selected EU institutions and bodies;
- Interviews performed.

Firstly, the study identifies the relevant provisions of EU Staff Regulations of Officials[234] (hereafter the "Staff Regulations") and of the Conditions of Employment of Other Servants[235] (hereafter the "CEOS") for the identified purposes.

Staff Regulations do not explicitly provide any time limit for the storage of EU staff members' personal data. Therefore, references to the relevant provisions of Staff Regulations are solely made in order to determine the legal basis on which data processing operations are carried out for each specific purpose.

Consequently, the present case study is based mainly on interpretative/administrative documents such as Guidelines and Opinions of the EDPS issued in the course of the prior checking procedure.

The EDPS provided for thematic Guidelines regarding the processing operations carried out by the EU institutions under the provisions of the Staff Regulations. This guidance is based on previous EDPS Opinions rendered in the course of prior checking. These Guidelines have however only been issued for specific fields of human resources activities, such as staff recruitment, staff evaluation and disciplinary proceedings. These guidelines are an essential tool for EU institutions and bodies to determine data retention periods. Nevertheless, these guidelines do not cover all fields of human resources. Where no guidelines have been published, data controllers need to refer to the opinions of the EDPS[236].

Indeed, the Opinions of the EDPS issued under Article 27 of Regulation (EC) No 45/2001 (which sets out the prior checking procedure) provide rich guidance on the recommendations of the EDPS to the EU institutions and bodies in order to carry out data processing operations in full compliance with the provisions of Regulation (EC) No 45/2001. It should be recalled that the prior checking procedure set out in Article 27 of Regulation (EC) No 45/2001 requires the EU institutions and bodies to notify the EDPS to make a prior check of processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, scope or purpose. Sections 27 (2) a) and b) specify that the processing of data relating to health and to suspected offences, criminal convictions or security measures as well as processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct, present such risk and must then be notified to the EDPS. Therefore, these Opinions constitute a solid basis to conciliate the principles set out in Regulation (EC) No 45/2001, and in particular the principle of data retention for no longer than necessary, with the data processing operations carried out under the Staff Regulations[237].

This study also relies on the analysis of internal procedures on data retention of the European Commission, which mainly refers to the Common Commission-Level Retention List for European Commission's Files.

Finally, in order to have a clear view on the data retention periods effectively implemented within EU institutions and bodies, the study evaluates certain data retention periods declared in DPOs Registers of a selection of EU institutions and bodies (European Commission, European Parliament,

[234] See the last consolidated version (1962R0031 – EN - 01.01.2014 - 011.001) of the Regulation (EEC) No 31, 11 (EAEC) laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community, (OJ 45, 14.6.1962, p. 1385), as amended in 2014.
[235] *Idem*.
[236] See for example the areas of staff mobility or salaries.
[237] On the basis of this opinion, the EPDS issued thematic Guidelines in different areas such as recruitments, staff evaluations and disciplinary proceedings, but also leave and flexitime, anti-harassment procedures and health data at work (available on the EDPS website: https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/Supervision/Guidelines).

Council of the European Union, OLAF). It should be pointed out that many DPO's registers of EU institutions and bodies are not available on the Internet[238].

For the purposes of the analysis, it is assumed that the data retention length indicated in the DPO's registers and in the procedures is the data retention period applied within the relevant institution. **Nonetheless, it should be noted that several of the stakeholders consulted have indicated that the retention periods indicated in the registers are not respected.**

4.2.5. Staff members' e-mails management

E-mail management

Staff members' e-mails may contain personal data and will therefore be subject to specific retention periods pursuant to the purpose. The stakeholders consulted indicated that EU institutions and bodies are using software for e-mail management (*e.g*. outlook).

EU institutions have developed IT tools in order to ensure regular and automatic deletion of e-mails on both the terminal equipment of staff members and the global IT network. However, it appears that some EU agencies face difficulties in erasing the e-mails from terminal equipment of the staff (inbox).

Such tools are already in place in the European Parliament and the Ombudsman where e-mails in personal mailboxes are automatically deleted after 3 months. Within the European Commission, such a tool will be put in place by the DG DIGIT on 1 July (automatic deletion after 6 months) and it seems that it is also planned by the European Central Bank.

The main issue in this regard is the necessity to raise awareness of EU staff members on the prior selection of important e-mails which will be registered for a longer period as these e-mails may contain crucial information.

Guidelines

In order to ensure the enforcement of rules relating to documents by staff members, certain EU institutions and bodies issued guidelines and internal policies on document management[239]. The main goal of most of these guidelines is to ensure the registration and filing of documents containing important information relating to the EU institution or body's activity. These are key steps to facilitating access to documents by other staff members and future archiving. Such guidelines set good practices relating to registration of e-mails before their automatic deletion.

According to these guidelines, e-mails should be registered as other documents; criteria for their registration are the same as criteria for all other documents. For instance the European Commission's Guidelines on document management[240] recommend registering "*e-mail that contains important information, involves action or follow-up, or may later be needed as proof*".

---

[238] According to Article 26 of Regulation (EC) No 45/2001: "*the [DPO] registers may be inspected by any person* ***directly*** *or indirectly through the European data Processing Supervisor*";
See also Article 46(i) of Regulation (EC) No 45/2001: "*The European Data Protection Supervisor shall: (...) (i) keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the data Protection Officers under Article 26*".

[239] Commission Decision 2002/47/EC, ECSC Euratom of 23 January 2002 amending its Rules of Procedure (OJ L21/23 of the 24.1.2002).
SEC(2009)1643 Implementing rules for Decision 2002/47/EC, ECSC, Euratom on document management and for Decision 2004/563/EC, Euratom on electronic and digitised documents, adopted on 30.11.2009.
Ares(2015)182108 Guidelines on document management and access to documents, 16.01.2015.
Rules on document Management in the European Parliament, Bureau decision of 2 July 2012.

[240] Ares(2015)182108 Guidelines on document management and access to documents, 16.01.2015.

Registration of selected e-mails in personal equipment of staff members is not sufficient to ensure their integrity and preservation; they are also registered in the IT network of the EU institution and body.

It should be stressed that even important e-mails must be deleted when they are no longer necessary.

Recommendations (in line with the current practices of certain EU institutions)

- Once e-mails are sent or received, staff members should determine whether or not they should be registered for long-term safeguard depending on their nature and the level of importance of their content in relation with activities of EU institutions and bodies;
- These should register selected e-mails in the global IT networks used by EU institutions and bodies. After a period of time, these e-mails should be deleted;
- Unselected e-mails should be deleted after a short-term period (as soon as they are no longer necessary) and automatic deletion of these e-mails should be foreseen.

4.3. Overview of practices regarding the conservation of personal data in HR context

The analysis of current practices on data retention of EU staff members' personal data by the EU institutions and bodies focuses on the three following purposes: data processing related to (2.1) recruitment management, (2.2) disciplinary proceedings and (2.3) staff evaluations.

4.3.1. Data retention practices in the area of recruitment management

Recruitment procedures of EU staff members according to the staff Regulations or the CEOS involves the implementation of personal data processing operations regarding candidates.

For the purpose of the present case study, the scope of recruitment covers the whole process, from the selection of candidates to the effective decision of recruitment or dismissal.

Please note that the European Commission considers that the selection process and recruitment are different data processing operations, the first being handled by the European Personnel Selection Office (EPSO) while recruitment is a data processing operation carried out by the DG HR. However, the EDPS[241], the Council of the European Union[242] and the European Parliament[243] do not always

[241] See EDPS Guidelines concerning the processing operations in the field of staff recruitment, October 2008, accessible at the following address: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines.
[242] See General Secretariat of the Council of the European Union, DPO Register, No 153N02 of 19-09-2014, « Sélection du personnel permanent et temporaire au Secrétariat général du Conseil de l'Union Européenne » (http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/data-protection/details/?detailsId=292).
[243] See European Parliament, Data Protection Registry, Notification No 117 of 09-05-2007, for "Sélection et recrutement des fonctionnaires et transferts interinstitutionnels". (http://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do?output=pdf&lang=FR&id=594) or Notification No 72 of 01-08-2006, for "Recrutement des agents contractuels" (http://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do;jsessionid=BCE05FC97D562D83F9D478335AC7216A?output=pdf&lang=FR&id=593).

distinguish these steps and sometimes encompass selection and recruitment in the same processing operation.

Moreover, hereinafter, data subjects should be taken as being candidates in recruitment procedures for permanent, temporary and contractual staff, national experts and trainees[244].

4.3.1.1. Overview of legal basis for data processing operations performed for recruitment purpose

As they involve an evaluation of the applicants' ability to perform the job for which they have applied and for which they are being evaluated, recruitment procedures, as set out in the Staff Regulations for permanent[245], contractual and temporary[246] staff involve personal data processing operations by the EU institutions and bodies falling under Article 27 of the Regulation. EU institutions and bodies have implemented internal recruitment procedures. Internal decisions of the EU institutions and bodies lay down admittance procedures for trainees[247] and national experts[248].In this context, candidates in the recruitment procedures for permanent staff, temporary agents and contractual agents, as well as the national experts and trainees who join the institutions and bodies are data subjects.[249] Processed personal data may be, for instance, the name, surname, date of birth, e-mail address, and curriculum vitae. The processing of sensitive data (namely data related to health as well as to criminal offences) may also be involved.

Staff Regulations do not provide any time limit for the storage of this information. However, deadlines and criteria for retention could be deduced from certain provisions of Staff Regulations (like Article 85), coupled with the relevant case law. Moreover, the Opinions and Guidelines of the EDPS provide clear guidance to enable the institutions and bodies to determine a data retention period in compliance with Article 4 (1) of Regulation (EC) No 45/2001.

4.3.1.2. Interpretation of the EDPS

In the recruitment field, the EDPS established thematic guidelines[250] summarizing the overall Opinions issued in the course of the prior checking procedure. These guidelines have proven to be an effective instrument.

These Guidelines dated October 2008 are applicable to the recruitment of any type of staff member (permanent staff, temporary agents and contractual agents). These Guidelines are also applicable to national experts and trainees. They provide a very detailed and concise view on the data retention period that may be adopted within the EU institutions and bodies. Indeed, the EDPS specified that such a data retention period is to be differentiated in accordance with the status of the candidate (permanent staff, temporary, contract and trainee on the one hand, and recruited, non-recruited applicants or applicants on reserve list on the other hand) and the type of data processed (i.e. sensitive data or not).

---

[244] For a similar position, see EDPS Guidelines concerning the processing operations in the field of staff recruitment, October 2008, accessible at the following address: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines.
[245] Article 27 to 34 of the Staff Regulations.
[246] Article 12 to 15 and 82 to 84 of the CEOS.
[247] For example, for the European commission: *Rules governing the official traineeships scheme of the European Commission* – Commission decision of 2.03.2005 – C(2005)458.
[248] For example, for the European Commission: *Rules on the secondment to the Commission of national experts and national experts in professional training* – Commission decision of 12.11.2008 – C(2008) 6866.
[249] Auxiliary conference interpreters (ACIs) of the European Commission are recruited by the SCIC or DG Interpretation with specific requirements (see. Opinion on a notification for Prior Checking received from the Deputy Data Protection Officer of the European Commission on the "Management of personal data of Auxiliary Conference Interpreters (ACI) stored in Signalétique (application of the central database CORALIN)", Brussels, 22 December 2006 (Case 2006-364).
[250] EDPS Guidelines concerning the processing operations in the field of staff recruitment, October 2008, accessible at the following address: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines.

Please note that these Guidelines explicitly mention that only data in an anonymous form should be stored for statistical purposes.

Data retention period related to the recruitment of officials, contract and temporary staff, and admittance of national experts

The EDPS Guidelines provide guidance to enable the EU institutions and bodies to determine a data retention period complying with the principle set out in Article 4(1) of Regulation (EC) No 45/2001.

With regard to recruited applicants, the EDPS indicates that their data should be stored in the personal file constituted for each staff member in accordance with Article 26[251] of the Staff Regulations, for a period of ten years as of the termination of employment or as of the last pension payment.

In its Opinions, the EDPS encourages reducing this period and reiterates the necessity for long-term data storage in order to provide for appropriate guarantees for transmission and storage[252]. In other Opinions, the EDPS took the position that a retention period of 10 years is too long if there is no specific justification for it. Data of a purely informative nature no longer necessary for administrative reasons (address, telephone number, etc.) can be disposed of after a minimum period of 5 years[253].

For non-recruited applicants, the time limit should be determined by the EU institutions or body in relation to:

(i) the time limits established for the possible review of the decision taken in the selection procedure; for instance, a two-year period following the recruitment procedure has been deemed acceptable as that period is derived from the length of time during which a complaint may be brought to the European Ombudsman[254];

(ii) the time limits for budgetary and audit purposes in accordance with Article 49 of the Implementing Rules to the Financial Regulations[255]; and

(iii) the validity of the respective (reserve) lists. The EDPS stated that the retention period must be determined in accordance with the validity and the actual extension of the respective reserve lists.

The EDPS seems to accept a retention period of 2 or, at the most, 3 years following the end of the procedure.[256] Some stakeholders argue that this period is too short, in light of the 5-year limitation period for legal action for damages (non-contractual liability) under Article 340 (2) TFEU.

[251] It is worth reminding that under Article 26 of the Staff Regulations, the personal file of an official shall contain:
(a) all documents concerning his administrative status and all reports relating to his ability, efficiency and conduct;
(b) any comments by the official on such documents.

[252] EPDS Opinion on the « *notification d'un contrôle préalable reçue du Délégué à la protection des données du Conseil de l'Union européenne à propos du dossier "Procédure d'embauche des fonctionnaires et autres agents du Secrétariat général du Conseil"* », Brussels, 25 January 2008 (Case 2007-194); EDPS Opinion EDPS concerning recruitment of permanent, temporary and contract agents at European Maritime Safety Agency (EMSA), Brussels, 7 January 2008, (case 2007-566).

[253] Opinion on the notification for prior checking from the Data Protection Officer of the European Maritime Safety Agency regarding the "Recruitment of permanent, temporary and contract agents", Brussels, 7 January 2008 (case 2007-566) and EDPS Opinion on a notification for prior check on the system of "Recruitment, by competition, of permanent staff for the European institutions or for Community bodies, offices and agencies", Brussels, 24 February 2006 (Case 2004-236).

[254] EDPS Guidelines concerning the processing operations in the field of staff recruitment, October 2008, accessible at the following address: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines.

[255] Article 49 provides that "Personal data contained in t supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes".

[256] EDPS Opinion concerning the selection of the Chair of the Supervisory Board of the European Central Bank, Brussels, 20 September 2013, (Case 2013-1007).

Data retention period related to the admittance of trainees

With regards to the admittance of trainees, the EDPS specified the starting period for the storage of their personal data.

For pre-selected but unsuccessful candidates, the starting date should be the immediate official starting date of the traineeship period and not the final date of the traineeship period to which the candidacy relates. According to an EDPS Opinion issued in the course of a prior checking procedure, recommendations on data retention laid down for non-recruitment candidates for staff positions were applicable to trainees. Indeed the EDPS again states that the personal data of unsuccessful applicants may be kept for up to two years following the recruitment procedure, as two years is the time during which a complaint may be brought to the European Ombudsman[257].

For successful candidates, personal data necessary for discharging the budget may be retained for up to 5 years after the traineeship budget is discharged in accordance with the Financial Regulation.

Once the 5-year period is completed, only the data necessary for providing a copy of the trainee certificate should be stored (namely information on the duration of the traineeship, the department to which the trainee was assigned, the name of the supervisor and the nature of the work performed).[258] These data could be stored for a period of 50 years.

Please note that in an Opinion dated June 2007, the EDPS welcomed the fact that data relating to non-validated applicants would be erased no later than one week after the deadline for submitting applications[259].

Data retention period of sensitive data

Sensitive data such as health data and criminal records may be processed in the course of the recruitment procedure in order to verify the suitability of the candidate for the position. Therefore, the EDPS Guidelines provide specific recommendations regarding the retention period of such data.

With regards to the retention period of the criminal record, police records and certificates of good conduct, the EDPS insisted on the fact that these documents cannot be stored as such by the agency but should rather be returned to recruited or non-recruited candidates immediately after the selection and (possible) recruitment. However, a "standard form" stating that the person could be suitable for the performance of his duties and that he enjoys his full rights as a citizen should be established and may be stored. The EDPS does not specify any duration as regards such a form.

Nevertheless the EDPS further explained specificities of the retention of sensitive data such as criminal records in an Opinion and validated the accuracy of a 2-year retention period for criminal records of candidates to the Court of Auditors justified by specific reasons linked to the tasks of the Court[260].

Similarly, according to the EDPS Guidelines, the retention period of other special categories of data (such as health and disability data) should immediately be deleted, either once they are no longer necessary for recruitment or reimbursement purposes, or following the date when a follow-up procedure has been completed. Yet, with regards to successful applicants, such data can be forwarded to the personal file in case special arrangements are required throughout the entire

[257] EPDS Opinion on a notification for prior checking received from the Data Protection Officer of the European Union Agency for Fundamental Rights on the « the processing of personal data in the context of internships », Case 2013-0654.
[258] EDPS Guidelines concerning the processing operations in the field of staff recruitment, October 2008, accessible at the following address: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines.
[259] EDPS Opinion on a notification for prior checking received from the Data Protection Officer of the Council on the "Selection procedure for trainees at the General Secretariat of the Council of the European Union", Brussels, 12 June 2007 (Case 2007-217).
[260] Letter from the EDPS to the DPO of the Court of Auditors, Brussels, 23 July 2012, C 2011-0482.

period of employment. The European Union Civil Service Tribunal confirmed this point in a judgment dated 5 July 2011[261].

4.3.1.3. Current practices among EU institutions and bodies

Having set-up the data retention time-limit recommended by the EDPS, it is then possible to challenge the data retention period currently applied within the EU institutions and bodies in accordance with the various categories of applicants identified in these Guidelines.

Data retention period related to the recruitment of officials, contract and temporary staff, and admittance of national experts

According to the Common Retention List of the European Commission

According to the Common Retention List of the European Commission, the personal data processed in the course of the recruitment procedure of permanent staff (officials) are stored for 10 years[262]. The CRL makes a difference between files for the organization of the competition[263] (among which there are minutes and references to disputes) and proper files on candidates eliminated during the procedure or entered on the reserve list.

The CRL refers to the related Opinion of the EDPS[264], by which it may be understood that:

(i) This 10-year administrative retention period applies to non-recruited candidates' paper files.
(ii) If the candidate is recruited, the EPSO transfers the application form, copies of diplomas or degrees and document proving previous professional experience into the personal file of agent for an indefinite period. The EPSO keeps all the other documents relating to the competition in which the applicant was successful (among which the applicant's written papers and any administrative correspondence exchanged during the competition) also for an indefinite period.
(iii) All on-line data are only stored for twelve months after the successful applicant has been appointed or until the reserve list expires if the person concerned has not been recruited.

The EDPS recommended applying a 10-year retention period after termination of employment or last pension payment to recruited candidates paper files.

The EDPS validated all other retention periods but recommended covering data by adequate measures for transmission and storage. It also recommended disposing data of a purely informative nature no longer necessary for administrative reasons after a minimum period of 5 years.

With regard to the procedures for the selection of contract staff and temporary agents, the CRL recommends a retention period of 5 years[265]. The EDPS Opinion referred to by the CRL is not available but it could be assumed that this retention period, as for permanent staff, only refers to non-recruited candidates' files. Recruited candidates' files would be transferred to personal files of the agent and governed by the above mentioned related retention period.

---

[261] F-46/09, *V. v. European Parliament*, 5.07.2011.
[262] See CRL, Annex 1: CRL Management Schedule, 12.3.4.A and 12.3.4.C.
The CRL also sets out a 10-year retention period specific for files regarding the organization of competitions for officials (CRL, Annex 1: CRL Management Schedule, 12.3.4.A) and a 10-year retention period for files concerning the selection of heads of unit, directors and senior posts (CRL, Annex 1: CRL Management Schedule, 12.3.3).
[263] The CRL specifies that "For computer-based tests, where the questions are contained in a database set up by the department and regularly updated, the 10-year ARP does not apply to the database." but it only relates to updated questions and not answers.
[264] EDPS Opinion on a notification for prior check on the system of "Recruitment, by competition, of permanent staff for the European institutions or for Community bodies, offices and agencies", Brussels, 24 February 2006 (Case 2004-236).
[265] See CRL, Annex 1: CRL Management Schedule, 12.3.4.D.

Moreover, for data relating to recruitment stored in personal files of staff members, users should refer to the general retention period recommended by the CRL for personal files of staff members within the European Commission, which is "*8 years after the extinction of all rights of the person concerned and of any independents; and for at least 120 years after the date of birth of the person concerned*". The CRL specifies that the retention period of these files is independent of the date on which the file is closed (i.e. the date of termination of service of the staff member)[266].

EU institutions and bodies justify this long-length retention period by the possible existence of staff members' beneficiaries (for example, a case of a handicapped child depending on an official, who could receive benefits until his or her death). The European Commission found further justification for this 120 years retention period:

(i) The possibility of legal action: for instance, even if the administration is not aware of possible beneficiaries, such persons may be in a position to claim benefits or damages long after the official left the service.
(ii) The need to reconstruct events of the career: for instance, in legal action on non-contractual liability (e.g. in order to be able to determine places of work in asbestos cases).

However, the position of the EDPS regarding this recommendation is clear. In its comments on the draft of the Common Retention List dated 2007, the EDPS already asked for a justification of this duration[267]. Later on, and in several opinions on a notification for prior checking, the EDPS expressly stated that the duration of 120 years is excessive and disproportionate[268]. Especially in the context of selection and recruitment of EU agents, the EDPS wrote: "*As the EDPS highlighted in previous cases and in its Guidelines, the retention period of 120 years of the data in the personal file is excessive and disproportionate to the purpose for which the data are collected, namely recruitment and hence staff member's rights under Staff Regulations. The EDPS reiterates his position that data of successful candidates (...) should be kept in the personal file for a retention period of ten years as of the termination of employment or as of the last pension payment. Such period is considered to be reasonable in light of Article 4 (1) (e) of the Regulation.*"[269] EU institutions and bodies could provide for specific administrative retention periods regarding documents necessary in the context of the exceptional cases referred to.

Finally, please note that the CRL recommends a retention period of two years for unsolicited applications.

According to Data Protection Registers

In the DPO Registers of the European Commission, the European Parliament and the General-Secretariat of the Council of the European Union, there are several processing operations concerning the recruitment of officials, contract agents and temporary agents recorded, as well as for national experts.

[266] See CRL, Annex 1: CRL Management Schedule, 12.3.7.
[267] In its Comments on the draft of the Common Retention List (Brussel, 7 May 2007, the EDPS already wrote that: « *As already mentioned, the EDPS would like the Commission to justify its keeping personal files for up to eight years after the extinction of all rights of the person concerned and of his dependants but until at least 120 years after his date of birth.* ».
[268] EDPS Opinion on prior-checking notification on the processing operations related to renewal of contracts for temporary and contract agents in the Innovation and Networks Executive Agency, Brussels, 12 June 2014 (case 2013-1288); EDPS Opinion on a notification for prior checking on selection procedures for officials, temporary and contract agents and trainees at the Office for Harmonization in the Internal Market ("OHIM"), Brussels, 26 March 2014 (case 2012-0852).
[269] EDPS Opinion on a notification for prior checking of the processing of personal data in the context of the selection and recruitment of Seconded National Experts ("SNEs"), trainees and interim agents the European Research Council Executive Agency, Brussels, 28 February 2013 (case 2012-0997).

- **DPO Register of the European Commission**

EPSO and DG HR data processing operations relating to recruitment procedures are recorded by the DPO of the European Commission in the register.

➢ *Data processing operations carried out by EPSO*

The register of the European Commission includes a processing operation for the "*Selection, by competition, of permanent staff for the European institutions or for Community bodies, offices and agencies*"[270], controlled by the EPSO. Processed data would relate to competition notice, on-line application, admission tests, assessment and leading to the inclusion of name on reserve list. The DPO reported several retention periods:

- For on-line data:
  - For recruited applicants: 12 months after the recruitment of the selected successful candidate;
  - For non-recruited applicants: 12 months after the closure of the applicant's last candidacy or until the closure of the reserve list;
- For paper data: 10 years;
- For non-recruited applicants: 1 year after closure.

The processing operation for the selection and recruitment of contract agents for EU institutions, bodies, offices and agencies[271] is recorded in the register. Processed data would be the same as for the precedent processing operation described. The register reported a general retention period of 3 years, which could vary according to selection procedures of contract agents. In this case, the retention period is specified in the competition notice. No difference is made between recruited and non-recruited candidates.

The processing operation for the selection and recruitment of temporary agents for EU institutions, bodies, offices and agencies[272] is also recorded in the register. Processed data would be the same. Without any apparent difference with the selection procedure of temporary agents, the register reported a general retention period of 10 years and specified that, after the selection procedure, files of candidates are sent to DG HR but EPSO conserves a copy. No difference is made between recruited and non-recruited candidates.

➢ *Data processing operations carried out by DG HR*

The register of the European Commission includes a specific processing for the "*Selection of Senior Staff in the Commission and in the Agencies*"[273]. Processed data relate to the professional and personal profile of candidates (i.e. CVs, motivation letters, copies of certificates, references, etc.), performance and integrity of internal candidates, and results of evaluations. The register reported that selection files stored in paper form are destroyed 10 years after the end of the selection procedures. This duration could be extended by one year after the final decision in case of legal action against the appointment decision. There is no specific retention period reported for

[270] European Commission, DPO Register, DPO-336.5 Selection, by competition, of permanent staff for the European institutions of Community bodies, offices and agencies, EPSO, 2011-06-16 (http://ec.europa.eu/dpo-register/details.htm?id=25277).
[271] European Commission, DPO Register, DPO-884.3 Sélection d'agents contractuels en vue de leur recrutement par les institutions européennes et le cas échéant, par les organismes, les organes ou les agences communautaires, EPSO, 2009-11-19 (http://ec.europa.eu/dpo-register/details.htm?id=25506).
[272] European Commission, DPO Register, DPO-885.3 Sélection d'agents temporaires en vue de leur recrutement par les institutions européennes et le cas échéant, par les organismes, les organes ou les agences communautaires, EPSO, 2009-11-19 (http://ec.europa.eu/dpo-register/details.htm?id=25509).
[273] European Commission, DPO Register, DPO-920.6 Selection of Senior Staff in the Commission and in the Agencies, DG HR, 2012-06-01 (http://ec.europa.eu/dpo-register/details.htm?id=27190).

non-recruited applicants so it seems that this period concerns recruited applicants as well as non-recruited applicants. No specific retention period is reported either for selection dossiers stored in electronic form but there may be no files stored in electronic form.

The register of the European Commission includes the processing of documents provided by candidates for their recruitment, including criminal report extracts and/or certificates of good life and morality[274]. This notification is not up to date. A new version is pending for prior checking with the EDPS. In principle, these documents are stored for the duration which is strictly necessary for the recruitment procedure, until the recruited candidates sign their contracts or the appointment act. After the end of the procedure:

- documents relating to recruited candidates are transferred into the personal file of the staff member and criminal report extracts are redacted; here the DPO reverts to the processing operation related to personal files and also registered;
- documents relating to non-recruited candidates are stored for 5 years but, in this case, contrary to recommendations of the EDPS about retention of sensitive data, criminal report extracts remain legible.

There are several personal data processing operations reported, relating to personal files in general:

- For personal files of the European Agency for Reconstruction by the DG HR, the register states that the data retention period is the same as the one for other personal files already sent to historical archives (i.e. 120 years)[275].
- For management of personal files by the DG HR, the DPO reported that scanned files are stored until the termination of all rights of the agent or its beneficiaries and the termination of any deadline for appeal. Paper documents scanned are transferred to the historical archives according to the usual procedure and destroyed together with electronic documents. There is no information about the coherence between the usual procedure for storage in the historical archives (i.e. the 120-year retention period) and the destruction of paper files together with the electronic file[276].
- For the management of personal files of employees from Luxembourg by the DG HR of the European Commission, the DPO reported a 3-year retention period after the end of service of the employee or until legal proceedings have been fully terminated including any appeal cases, whichever is the longer[277]. However, this category of staff falls under Luxembourgish labour law and is therefore incommensurable with staff falling under the Staff Regulations.

- **DPO Register of the European Parliament**

The register of the European Parliament includes the processing of personal data for selection and recruitment of agents, and inter-institutional transfers by the directorate for the Human Resources Strategy[278]. He reported the following retention periods:

[274] European Commission, DPO Register, DPO-2667.1 Traitement des documents fournis par le candidat pour son recrutement, y compris les extraits de casiers judiciaires et les certificats de bonne vie et moeurs, DG HR, 2011-05_27 (http://ec.europa.eu/dpo-register/details.htm?id=26545).
[275] European Commission, DPO Register, DPO-2796.3 Dossier personnels de l'Agence Européenne de Reconstruction (AER), DG HR, 2010-08-27 (http://ec.europa.eu/dpo-register/details.htm?id=26622).
[276] European Commission, DPO Register, DPO-230.3 Gestion des dossiers personnels, DG HR, 2010-08-27 (http://ec.europa.eu/dpo-register/details.htm?id=25222).
[277] European Commission, DPO Register, DPO-2930.2 Gestion des dossiers personnels des salariés luxembourgeois, DG HR, 2015-05-05 (http://ec.europa.eu/dpo-register/details.htm?id=39239).
[278] European Parliament, Data Protection Registry, Notification No 117 of 09-05-2007, for "Sélection et recrutement des fonctionnaires et transferts interinstitutionnels" (http://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do?output=pdf&lang=FR&id=594).

- For non-recruited candidates: 3 years after the end of the selection procedure;
- For recruited candidates: 10 years after the recruitment procedure for recruitment files or 10 years after "extinction" of beneficiaries for personal files.

The register of the European Parliament includes the processing for the Recruitment of national experts[279] without reporting any retention period and **the processing for the recruitment of interim agents** with a reported general retention period of 2 years[280].

- **DPO Register of the Council of European Union**

As for the register of the Council, it includes an operation relating to the selection of permanent and temporary agents of the General Secretariat of the Council of the European Union[281]. Processed data would relate to the identity of candidates, administrative information (address, phone number, etc.), data provided by the candidates for selection (language, diploma, etc.) and test results. The DPO recorded several retention periods:

- For selected but non-recruited candidates: 2 years in paper form;
- For non-recruited candidates of the reserve list: 2 years from the closure of the reserve list;
- For recruited candidates: 10 years from the termination of employment or the last pension payment in the personal file;
- For unsolicited applications: 6 months in electronic form or no storage at all, depending on the reception mailbox.

The processing for the "Selection procedure of members of the Management Board of the European Medicines agency (EMA)"[282] **is also recorded in the register.** The duration reported is a general retention period of 3 years, corresponding to the entire duration of the mandate according to Regulation (EU) No 726/2004 for data on all candidates.

Data retention period related to the admittance of trainees

According to the Common Retention List of the European Commission

Concerning files on trainees, the CRL recommends several retention periods[283]:

- For files on trainees, grant holders or short and long term visitors: 50 years for the "*sheet established for the reconstruction of one's career*" but only 5 years for all other documents;
- For files on unsuccessful candidates: 2 years.

The 2-year retention period recommended for files of unsuccessful candidates corresponds to the time limit to refer the case to the European Ombudsman, as recommended by the EDPS.

[279] European Parliament, Data Protection Registry, Notification No 6 of 1-07-2006, for "Recrutement des experts nationaux detachés auprès du PE" (http://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do?output=pdf&lang=EN&id=591).
[280] European Parliament, Data Protection Registry, Notification No 313 of 11-04-2013, for "Recrutement des agents interimaires" (http://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do?output=pdf&lang=FR&id=599).
[281] General Secretariat of the Council of the European Union, DPO Register, No 153N02 of 19-09-2014, « Sélection du personnel permanent et temporaire au Secrétariat général du Conseil de l'Union Européenne » (http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/data-protection/details/?detailsId=292).
[282] General Secretariat of the Council of the European Union, DPO Register, No 238N00 of 21-02-2014, "Selection procedure of members of the Management Board of the European Medicines agency (EMA)" (http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/data-protection/details/?detailsId=408).
[283] See CRL, Annex 1: CRL Management Schedule, 12.3.8.C & D.
The CRL also sets out a 5-year retention period specific for files regarding the adoption and application of rules on Commission traineeship, grants and short or long term visits programmes (CRL, Annex 1: CRL Management Schedule, 12.3.8.A) and a 5-year retention period for files concerning the invitations to apply, procedure, selection panels, etc. for traineeships, grants and short or long term visits (CRL, Annex 1: CRL Management Schedule, 12.3.8.B).

Likewise, it seems that the retention periods recommended by the CRL regarding files on trainees, grant holders or short and long-term visitors correspond to the retention periods recommended by the EDPS in its Guidelines. The sheet established for the reconstruction of one's career mentioned by the CRL would be the data necessary for providing a copy of the trainee certificate as referred by the EDPS.

According to Data Protection Registers

In the DPO Registers of the European Commission and the European Parliament, there are several processing operations concerning admittance of trainees.

The register of the European Commission included the processing operation for scholarship trainees in Luxembourg, controlled by the DG HR[284]. He reported the following retention periods:

- For admitted trainees: 1 year after completion of the traineeship;
- For unsuccessful trainees: 3 months after the starting date of the planned traineeship, except for data entered into the general database which follows the retention policy of that processing.

The register of the European Parliament includes the processing for selection, recruitment and management of trainees of the European Parliament[285]. Processed data relate to evaluation of personal aspects of the data subject, data subject's family, data subject's career, expenses and medical benefits but not to data relating to suspected offenses, offenses, criminal convictions or security measures. Concerning unsuccessful candidates, data should be stored for a maximum of 2 years. Concerning successful candidates, data should be stored indefinitely.

Conclusion

As a consequence, it follows from the analysis of the personal data processing operations selected, that EDPS Guidelines recommendations and CRL's recommendations are not systematically followed in practice. Retention periods reported by DPOs for recruitment of staff members are highly variable:

(i) In many cases, it appears that no distinction is made between recruited and non-recruited candidates[286], and there is no particular remark about any transfer of data into personal files of agents after their recruitment[287].
(ii) Occasionally, no retention period is reported[288].
(iii) It appears that in certain cases no distinction is made between permanent staff and temporary staff[289].

[284] European Commission, DPO Register, DPO-2750.2 Stagiaires scolaires à Luxembourg, DG HR, 2015-05-05 (http://ec.europa.eu/dpo-register/details.htm?id=26587).
[285] European Parliament, Data Protection Registry, Notification No 114 of 20-03-2007, for "Sélection, recrutement et gestion des stagiaires auprès du PE" (http://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do?output=pdf&lang=EN&id=592).
[286] See for example: European Commission, DPO Register, DPO-884.3 Sélection d'agents contractuels en vue de leur recrutement par les institutions européennes et le cas échéant, par les organismes, les organes ou les agences communautaires, EPSO, 2009-11-19 (http://ec.europa.eu/dpo-register/details.htm?id=25506); European Commission, DPO Register, DPO-885.3 Sélection d'agents temporaires en vue de leur recrutement par les institutions européennes et le cas échéant, par les organismes, les organes ou les agences communautaires, EPSO, 2009-11-19 (http://ec.europa.eu/dpo-register/details.htm?id=25509).
[287] See for example: idem and European Commission, DPO Register, DPO-336.5 Selection, by competition, of permanent staff for the European institutions of Community bodies, offices and agencies, EPSO, 2011-06-16 (http://ec.europa.eu/dpo-register/details.htm?id=25277).
[288] See for example: European Parliament, Data Protection Registry, Notification No 6 of 1-07-2006, for "Recrutement des experts nationaux detachés auprès du PE" (http://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do?output=pdf&lang=EN&id=591).

(iv) In several cases, the European Personnel Selection Office (as regards data processing operations incorporated in the DPO Register of the European Commission) does not follow the CRL recommendations either. For example, the European Commission recorded a general 3-year retention period for data relating to the selection of contract agents[290] and a 10-year retention period for data relating to the selection of temporary agents[291], where the CRL recommends a 5-year retention period for personal data relating to both recruitment procedures.

(v) Finally, where the CRL does not follow the EDPS Opinion[292], it is recommended (i) that EU institutions and bodies collaborate with the EDPS in order to identify an appropriate retention period (ii) to ensure the follow up of the implementation of the recommendations of the EDPS formulated in its opinions.

4.3.2. Data retention practices regarding staff evaluation

Career management of the EU staff members involves the implementation of specific procedures required under Staff Regulations relating mainly to the evaluation of the EU staff members.

For the purpose of this case study, promotion will be considered part of the evaluation process insofar as it is the consequence and one of the objectives of such process.

4.3.2.1. Overview of legal basis for data processing operations performed for evaluation purposes

In accordance with the provisions of the Staff Regulations, staff members are subject to a number of evaluation procedures for the management of their career. As indicated by the EDPS in its general Guidelines concerning staff evaluation,[293] an EU staff member is to be evaluated in the course of staff performance assessment through the establishment of career development reports.[294]

At the beginning of his career, any staff member is subject to a probationary evaluation, leading to the establishment of a probationary report.[295] When officials are appointed head of unit, director or director-general, they also are subject to a probationary period, which leads to the establishment of a management probationary report[296]. In the course of their career, officials will be annually assessed; some categories of contract agents will be assessed in view of the renewal of their contract for an indefinite term[297], as well as temporary agents in view of their re-grading[298]. In addition, some officials may also be subject to a certification procedure[299] which allows the

[289] See for example: General Secretariat of the Council of the European Union, DPO Register, No 153N02 of 19-09-2014, « Sélection du personnel permanent et temporaire au Secrétariat général du Conseil de l'Union Européenne » (http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/data-protection/details/?detailsId=292).
[290] European Commission, DPO Register, DPO-884.3 Sélection d'agents contractuels en vue de leur recrutement par les institutions européennes et le cas échéant, par les organismes, les organes ou les agences communautaires, EPSO, 2009-11-19 (http://ec.europa.eu/dpo-register/details.htm?id=25506).
[291] European Commission, DPO Register, DPO-885.3 Sélection d'agents temporaires en vue de leur recrutement par les institutions européennes et le cas échéant, par les organismes, les organes ou les agences communautaires, EPSO, 2009-11-19 (http://ec.europa.eu/dpo-register/details.htm?id=25509).
[292] See for example: European Commission, DPO Register, DPO-336.5 Selection, by competition, of permanent staff for the European institutions of Community bodies, offices and agencies, EPSO, 2011-06-16 (http://ec.europa.eu/dpo-register/details.htm?id=25277) and European Parliament, Data Protection Registry, Notification No 117 of 09-05-2007, for "Sélection et recrutement des fonctionnaires et transferts interinstitutionnels" (http://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do?output=pdf&lang=FR&id=594).
[293] EDPS Guidelines concerning the processing of Personal Data in the area of staff evaluation, July 2011.
[294] Article 43 of the Staff Regulations and 15(2) of the CEOS.
[295] Article 34 of the Staff Regulation as well as Articles 14 and 84 of the CEOS (for temporary Staff).
[296] Articles 44 to 46 of the Staff Regulations.
[297] Article 85(3) of the CEOS.
[298] Articles 10(3) and 15 of the CEOS.
[299] Article 45 (a) of the Staff Regulations.

appointment of an official in function group AST (Assistant) from grade 5 to a job in function group AD (Administrator) by means of a compulsory training programme at the European Administrative School.

Each of these procedures involves data processing operations which generally lead to the establishment of a report that will be added to and stored in the personal file of the Staff member in accordance with Article 26 of the Staff Regulations (together with Article 11(1) and 81 of the CEOS).

In the absence of any time limit for the storage of the information processed for evaluation purposes, the EDPS issued a number of Opinions summarized in the general Guidelines concerning the processing of Personal Data in the area of staff evaluation dated July 2011.

4.3.2.3. Interpretation of EDPS

As indicated previously, the EDPS issued Guidelines concerning the evaluation of EU staff[300]. The scope covers the evaluation procedures described above and all their related documents (such as probationary reports, career development reports[301], as well as various decisions adopted in the course of the respective procedure) which are stored in the personal file of the relevant staff member.

In its Guidelines, the EDPS questioned the existing practice of keeping all related documents containing personal data in a personal file for up to ten years after the termination of employment or the last pension payment as this does not correspond to the specific purposes for which the data was collected and/or further processed, such as the accomplishment of the respective evaluation exercise.

Documents concerned are: career development reports, probation reports, promotion/re-grading decisions as well as letters confirming the final award of the respective points, certification files of successful applicants (applications without the supporting documents that should be destroyed within one month after the publication of the list of successful applicants, training attendance and exam results), and attestation decisions.

The EDPS also provided clear guidance on retention periods which should be considered appropriate for other documents. Accordingly:

(i) **evaluation reports** may be kept for up to five years as the evaluator needs to consult previous reports in order to assess the progress made by the staff member but does not necessarily need to have access to all previous reports. Therefore, in one of its opinions, the EDPS stated that a time limit of up to five years is deemed appropriate as to how far the reports can go[302];

(ii) **documents relating to promotion, certification, and attestation decisions** may be kept during the entire career of the staff member but there is no need to keep all related documents;

(iii) **some other documents** such as lists published on the Intranet within promotion and certification procedures may be kept for up to five years for further audit purposes;

(iv) **files of unsuccessful applicants for certification and attestation** may be kept until all appeal channels have been exhausted including the time limits for appeal before the Civil Service Tribunal.

[300] EDPS Guidelines concerning the processing of personal data in the area of staff evaluation, July 2011.

[301] The career development reports is the annual report which examines the ability, efficiency and conduct in the service of the relevant staff member.

[302] See EDPS Opinion on a notification for prior check on the "staff assessment procedure" of the European Defense Agency, Brussels, 16 October 2013 (case 2013-0744).

In an Opinion on the underperformance procedure of the European Central Bank (hereafter the "ECB")[303] anchored in the condition of Employment for Staff of the ECB and contained in the ECB Staff Rules, the EDPS welcomed the 5 and 3-year retention periods reported for the conservation of data related to performance appraisal in the personal file of the assessed agent and the 6-month retention period before destruction of other documents (i.e. recording of hearings, etc.).

In another Opinion on the annual appraisal procedure of the European External Action Service[304], the EDPS rejected a 10-year retention period from the end of service of the agent (i.e. termination of contract or retirement of the active service) because there was no sufficient evidence demonstrating the necessity of a conservation policy extending to the whole career of the agent.

Similarly, as regards the procedure of assessment and reporting on probationary periods of the Community Plant Variety Office, the EDPS stated that the existing retention period which extends to the entire career of the data subject is not necessary for the initial assessment of staff. The EDPS recommended a maximum storage period of five years after the end of a particular evaluation exercise[305].

4.3.2.4. Current practices among EU institutions and bodies

Having set-up the data retention periods recommended by the EDPS, it is then possible to confront them with the data retention periods currently applied within the EU institutions and bodies.

According to the Common Retention List of the European Commission

The Common Retention List does not recommend a specific retention period for data relating to staff evaluation stored in the personal file of staff members. As for data relating to recruitment stored in the personal file of staff members, users should refer to the general retention period recommended by the CRL for personal files (i.e. eight years after the extinction of all rights of the person concerned and of any dependents, and for at least 120 years after the date of birth of the person concerned)[306].

In this specific context, the EDPS requested justifications of the retention period for personal files which are meant to be kept for up to eight years after extinction of all rights of the person concerned and of his dependents but at least 120 years after his date of birth[307]. The EDPS wrote: "*The EDPS would like to comment on the retention period of personal files. INEA foresees a retention period for the personal files of 120 years. In light of Article 4(1) (e) of the Regulation, the EDPS has always considered this retention period as* <u>*excessive and unnecessary*</u> *to the purpose for which personal data are collected and further processed. As the EDPS recommended in his Guidelines on Staff recruitment, personal data should be stored in personal files (Article 26 of the Staff Regulations), for a period of ten years as of the termination of employment or as of the last pension payment. The EDPS highlights that the issue of the retention period of personal files is a pending issue subject to on-going discussions between the EDPS and the EU institutions. The EDPS invites INEA to re- consider this issue in light of the agency's practical needs and experiences*".[308]

[303] EPDS Opinion on the notification for prior checking received from the Data Protection Officer of the European Central Bank concerning the ECB's Underperformance Procedure, Brussels, 30 August 2013 (case 2013-0892).
[304] EDPS Opinion on the notification for prior checking from the Data Protection Officer of the European External Action Service concerning annual appraisal, Brussels, 23 May 2013 (case 2013-0206).
[305] Opinion on the notification for prior checking from the Data Protection Officer of the Community Plant Variety Office concerning "Assessment and reporting on probationary periods" Brussels, 19 October 2011 (case 2011-0298).
[306] See CRL, Annex 1: CRL Management Schedule, 12.3.7.
[307] EDPS comments on the draft CRL of 5 July 2012 (EDPS 2007-0222) as well as EDPS comments on the draft revised CRL of 17 October 2012 (EDPS 2012-0804).
[308] EDPS Opinion on prior-checking notification on the processing operations related to renewal of contracts for temporary and contract agents in the Innovation and Networks Executive Agency, Brussels, 12 June 2014 (case 2013-1288).

According to DPO Registers of selected EU institutions and bodies

The DPO of the European Commission registered several personal data processing operations relating to staff evaluation:

- For data processing operations concerning staff promotions controlled by the DG HR, the DPO reported a ten-year retention period from the last pension payment, in the related electronic database[309];
- The notification on evaluation has been updated and is pending for prior checking with the EDPS;
- For all human resources reports established for management purposes by the Directorate-General for Economic and Financial Affairs, the DPO reported a ten-year retention period. He specified, "*This long conservation period is necessary in order to prepare reports/statistics on long term evolution of staff in the DG.*" In the case of promotion, data seem to be stored for the last five exercises in order to produce relevant statistics[310].

For data processing operations concerning staff promotion, the DPO of the Council of the European Union reported a five-year retention period, in electronic or paper form. The register specifies that most of the paper documents are destroyed at the end of the assessment procedure[311].

The DPO Register of the European Parliament reports processing operations for a certification procedure. Data should be stored for five years after the end of the procedure[312].

Conclusions

It would appear that CRL is not consistent with the recommendations of the EDPS. Pursuant to the CRL, data controllers should refer to the general 120-year administrative retention period recommended for personal files of staff members which the EDPS on various occasions considered as excessive. On the other hand, in case of the European Commission, all its HR processes, including relevant retention periods have been duly notified. Despite numerous comments and Opinions of the EDPS on various files (from its Comments on the Common Retention List dated 2007 to Opinions in the contexts of staff recruitment and evaluation namely dated 2013 and 2014[313]), the European Commission did not modify the CRL.

Finally, retention periods effectively reported by DPOs for storage of documents related to staff evaluation vary from ten years after the last pension payment to five years after the end of the procedure. These differences could be explained by the fact that the five-year retention period recommended by the EDPS has been criticized as too short/inappropriate according to data controllers.

[309] European Commission, DPO Register, DPO-472.5 SYSPER 2 - Promotion, DG HR, 2012-04-19 (http://ec.europa.eu/dpo-register/details.htm?id=30066).
[310] European Commission, DPO Register, DPO-1051.5 Human resources (HR) reports, DG Economic and Financial Affairs, 2015-19-03 (http://ec.europa.eu/dpo-register/details.htm?id=38972).
[311] General-Secretariat of the Council of the European Union, DPO Register, 162N02 (08/10/2013), « Exercice de promotion » (http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/data-protection/details/?detailsId=301).
[312] European Parliament, DPO Register, No 107, 10-01-2007, « Procédure d'attestation » by the staff and career management Unity (http://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do?output=pdf&lang=FR&id=618).
[313] Comments on the draft of the Common Retention List (Brussel, 7 May 2007); EDPS Opinion on prior-checking notification on the processing operations related to renewal of contracts for temporary and contract agents in the Innovation and Networks Executive Agency, Brussels, 12 June 2014 (case 2013-1288); EDPS Opinion on a notification for prior checking on selection procedures for officials, temporary and contract agents and trainees at the Office for Harmonization in the Internal Market ("OHIM"), Brussels, 26 March 2014 (case 2012-0852); EDPS Opinion on a notification for prior checking of the processing of personal data in the context of the selection and recruitment of Seconded National Experts ("SNEs"), trainees and interim agents the European Research Council Executive Agency, Brussels, 28 February 2013 (case 2012-0997).

4.3.3. Data retention practices in the area of administrative investigations and disciplinary proceedings

Staff Regulations provide for rules on administrative investigations and disciplinary proceedings which involve the processing of personal data. The CEOS are referring to those proceedings for temporary staff, contract staff and parliamentary assistants.

4.3.3.1. Overview of legal basis for administrative investigations and disciplinary proceedings

According to Staff Regulations, staff members are liable for any failure to comply with their obligations under these Regulations, intentionally or through negligence. If a staff member fails to comply, his Appointing Authority or the European Anti-Fraud Office (OLAF), independent office within the European Commission responsible for internal investigations including investigations relating to EU staff, may launch administrative investigations which may be followed by disciplinary proceedings as laid down in Annex IX to the Staff Regulations[314]. These procedures involve data processing operations.

During the investigation phase, an investigation report is established. On this basis, the Appointing Authority determines the follow-up to be given to the investigation, whether to initiate disciplinary proceedings or not[315].

The Appointing Authority may decide to send a written warning or a reprimand without consulting the Disciplinary Board of the Institution[316]. In all other cases, the Appointing Authority must submit a report to the Disciplinary Board in order for the Board to deliver an opinion[317]. The Appointing Authority will make the final decision[318]. If the Authority decides to close the case without imposing any disciplinary penalty on the staff member, it informs the staff member in writing without delay and the staff member may request that this decision be inserted in his personal file.

Staff Regulations do not provide for any time limit for the storage of the information processed during administrative investigations or disciplinary proceedings, but Article 27 of Annex IX specifies that a staff member may submit a request for the deletion from his personal file of all reference to the disciplinary measures after a period of three years in case of a written warning or reprimand or after a period of six years in the case of any other penalty. This right is not granted to officials against whom a removal from post has been ordered.

The EDPS issued Guidelines offering practical guidance and suggesting best practices to European institutions and bodies on the processing of personal data in administrative inquiries and disciplinary proceedings by European institutions and bodies[319].

4.3.3.2. Interpretation of the EDPS

The EDPS Guidelines concerning administrative inquiries and disciplinary proceedings, based on 14 EDPS Opinions previously issued, cover the data retention issue.

The EDPS differentiates between the conservation of data in personal files and the conservation of data in disciplinary files. All information collected and documents related to the administrative investigations or disciplinary proceedings should be stored in a disciplinary file relating to the

[314] Article 86 to the Staff Regulations; Articles 50a, 119 and 139.3 CEOS.
[315] Article 3 of Annex IX to the Staff Regulations.
[316] Article 11 of Annex IX to the Staff Regulations.
[317] Articles 12 and 18 of Annex IX to the Staff Regulations.
[318] Article 22 of Annex IX to the Staff Regulation.
[319] EDPS Guidelines concerning the processing of personal data in administrative inquiries and disciplinary proceedings by European institutions and bodies, 23 April 2010.

staff member concerned, separate from the personal file. A copy of the final decision should be kept in his personal file, only if the Appointing Authority imposes disciplinary penalties on him. In those cases when no disciplinary charges are imposed, there should be no trace of the procedure in the personal file.

As regards data retention in personal files, the EDPS explains that, according to Article 27 of Annex IX, the copy of the final decision on disciplinary measures may be removed from the personal file of the staff member on his request. This decision is at the discretion of the Appointing Authority which must justify any refusal. This means that personal data concerning disciplinary proceedings may be erased from the personal file of a staff member three or six years after the decision, depending on the content of the decision. However, in case of refusal, no time limit for retention is specified. The EDPS advises European institutions and bodies to set up a maximum retention period, for example the same as the retention period for disciplinary files, in order to ban parallel files according to the case law of the Court of Justice of the European Union[320].

As regards the data retention in disciplinary files, the EDPS recommends that European institutions and bodies set up an adequate retention period, taking into account the time limit for appeal and the obligation to keep "*in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed*"[321].

In any case, the EDPS rejects the argument of the necessity to take into account the recurrence of a staff member's action or behaviour and conduct throughout the course of his career in order to determine disciplinary penalties. This argument has been raised to justify a long retention period for disciplinary data in personal or disciplinary files[322]. It appears from various EDPS Opinions on prior checks, that this argument has been invoked by several European institutions and bodies in order to justify the retention of disciplinary data in the personal file of staff members after the end of their careers until the age of 70. The EDPS considered this duration not justified[323].

In several Opinions, the EDPS considered as proportionate the following retention periods[324]:

- A 20-year retention period for all data in disciplinary files related to administrative inquiries and disciplinary proceedings, from the date of the disciplinary decision or the date on which the inquiry is closed;
- A 5-year retention period for all data related to administrative inquiries without a disciplinary follow-up from the date of closure of the inquiry;
- The same retention period for the copy of the disciplinary decision stored in the personal file of the staff member as for the data related to administrative inquiries and disciplinary proceedings stored in the disciplinary file, namely a 20-year retention period from the date of the disciplinary decision.

[320] CJEC, 11 October 1995, *Baltsavias v. Commission,* Cases T-39/93 and T-553/93.
[321] Article 4(1)(e) of Regulation (EC) No 45/2001.
[322] Article 10(h) and (i) of annex IX to the Staff Regulations.
[323] EDPS Opinion on the notification for prior checking from the Data Protection Officer of the European Economic and Social Committee regarding the EESC internal administrative investigations and disciplinary proceedings, Brussels, 9 November 2009, Case 2008-569 and EDPS Opinion on the notification for prior checking from the European Ombudsman's Data Protection Officer regarding the "disciplinary proceedings and administrative investigations" dossier, Brussels, 17 October 2007, Case 2007-0413.
[324] EDPS Opinion on the notification for prior checking relating to internal administrative inquiries and disciplinary procedures within the European Commission, Brussels, 20 April 2005, Case 2004-187; EDPS Opinion on the updated notification concerning administrative inquiries and disciplinary proceedings within the Court of Justice of the EU, Brussels, 12 September 2011, Case 2011-0806 and EDPS Opinion on notifications for prior checking from the Data Protection Officers of certain EU agencies concerning the "processing of administrative inquiries and disciplinary proceedings", Brussels, 22 June 2011, Case 2010-072.

4.3.3.3. Current practices among EU institutions and bodies

In view of the data retention time limit recommended by the EDPS through its Guidelines and Opinions on notifications for prior checking, it is interesting to compare them with the practices of EU institutions and bodies on data retention for administrative inquiries and disciplinary proceedings.

Data retention period according to the Common Retention List of the European Commission

Within European institutions and bodies, administrative inquiries and disciplinary proceedings are conducted by OLAF or the Appointing Authority of the EU institutions and bodies. In the European Commission, the Commission's Investigation and Disciplinary Office (IDOC) conducts administrative inquiries and disciplinary proceedings for the Appointing Authority.

The CRL, in its section on "*Professional conduct and discipline*", recommends administrative retention periods for each step of administrative inquiries and disciplinary proceedings[325]:

- For files that have not given rise to administrative investigations:
  - A 2-year retention period regarding procedures coordinated by IDOC for the DG Human Resources and Security;
  - A 5-year retention period regarding procedures coordinated by OLAF;
- For administrative investigations without disciplinary consequences files:
  - A 5-year retention period regarding procedures coordinated by IDOC;
  - A 10-year retention period regarding procedures coordinated by OLAF;
- For administrative investigations with disciplinary consequences files, a 20-year retention period, by reference to the EDPS Opinion 2004-187[326], whether the investigation is coordinated by IDOC or OLAF;
- For disciplinary procedures files, once again in reference to the EDPS Opinion 2004-187, there is a 20-year retention period.

The Common Retention List does not recommend a specific administrative retention period for data relating to administrative investigations or disciplinary proceedings stored in the personal file of a staff member. The administrative retention period for these data must be the general period recommended for personal files, **namely 8 years after the extinction of all rights of the person concerned and of any dependents, and for at least 120 years after the date of birth. As the personal file may contain a copy of the final decision of the Appointing Authority when a disciplinary penalty is imposed on the EU official, an appropriate retention period needs to be identified. It is important to underline that this 120 years period cannot apply to all documents enshrined in the personal file; each type of document should be submitted to a specific retention period according to their purposes.**

Moreover, the administrative retention periods recommended for files related to disciplinary proceedings (i.e. investigations with disciplinary consequences files and disciplinary procedures files) refer to periods recommended by the EDPS in its Opinion dated April 2005 which are the same as the retention periods recommended by the EDPS in its Guidelines. As for retention periods for files only related to administrative investigations (i.e. files that have not given rise to administrative investigations and investigations without disciplinary consequences files) conducted by IDOC for the

[325] See CRL, Annex 1: CRL Management Schedule, 12.4.
Please note that the Common Retention List recommends retention periods regarding files created by the Secretariat General of the European Commission or Directorates General cooperating during investigations and disciplinary procedures. It states a 15-year retention period for files created by the Secretariat General and a 5-year retention period for files created by Directorates General.
[326] EDPS Opinion 2004-187: see above.

DG Human Resources and Security, they also seem to be proportionate in view of retention periods recommended by the EDPS in its Guidelines and above mentioned.

Please note that administrative retention periods for files related to administrative investigations conducted by OLAF are longer than administrative retention periods recommended by the EDPS and the CRL for files related to administrative investigations conducted by IDOC. This retention period must be justified by legitimate reasons.

Data retention period according the registers of EU institutions and bodies

In the OLAF Personal Data Register, OLAF notified a processing for "*administrative investigations within the EU institutions, bodies, offices and agencies for the purpose of detecting (…) serious matters relating to the discharge of professional duties; maintaining investigation files*."[327] OLAF may keep investigation files for up to 15 years after the closure of the investigation where recommendations have been made, and up to 8 years where no recommendations have been made.

OLAF notified another processing related to administrative investigations, for operational analysis[328]. In this case, OLAF made the difference between incoming information which does not result in the opening of an investigation and will be retained for a maximum of 5 years and investigations files which will be retained for a maximum of 15 years, provided recommendations have been made upon conclusion of the investigation, and 8 years, provided no recommendations have been made.

In the European Commission Personal Data Register, there is a notification concerning a processing operation for internal European Commission administrative investigations and disciplinary proceedings, notified by the DG Human Resources and Security[329]. The administrative retention periods set forth concerning data stored in disciplinary files are the same as the periods recommended by the CRL. However, even if the form makes it clear that only disciplinary decisions are stored in the personal files of staff members, it does not register any maximum retention period. The form only refers to Article 27 of Annex IX to the Staff Regulations and the possibility for staff members to request the removal of disciplinary decisions from their personal files (see above).

It appears that the data retention periods registered by the DG Human Resources and Security follow the Common Retention List recommendations for professional conduct and reflect the problematic absence of a specific data retention period recommended for the storage of the disciplinary decision in staff members' personal files.

As for OLAF, it does not follow the Common Retention List recommendations and declares longer administrative retention periods for investigation files where recommendations have been made. These retention periods may be valid if they are justified.

Conclusions

An analysis of the European Commission register shows that the recommendations of the EDPS relating to the retention period applying to disciplinary files are being followed. Nevertheless, a distinction must be made between (the) conservation of data in personal files an conservation of data in disciplinary files. In this regard, Article 27 of Annex IX of the Staff Regulations offers staff members a limited right for deletion of disciplinary decisions from their personal files though there

[327] OLAF Personal Data Register, DPO-176.1 Internal investigations, Publication 2014.07.24 (http://ec.europa.eu/anti_fraud/olaf-and-you/data-protection/olaf-register/index_en.htm).
[328] OLAF Personal Data Register, DPO-89.1 Operational Analysis, Publication 2015-02-19 (http://ec.europa.eu/anti_fraud/olaf-and-you/data-protection/olaf-register/index_en.htm).
[329] European Commission Personal Data Register, DPO-63.8 Enquêtes administratives et procédures disciplinaires internes de la commission européenne, Publication 2012-06-01 (http://ec.europa.eu/dpo-register/details.htm?id=27176).

is no specific maximum retention period set up in case of refusal of the Appointing Authority. In practice, however, the Appointing Authority never refuses the deletion.

Furthermore, the duration of 120 years after the date of birth for disciplinary decisions included in personal files may be deemed excessive. Therefore, it is important to differentiate between the retention periods of each of the documents encompassed in personal files.

Conclusion

- EU institutions and bodies refer to the guidelines of the EDPS in order to determine appropriate retention periods pursuant to the purpose of the processing. When guidelines are not adopted by the EDPS, data controllers refer to the opinions of the EDPS rendered in the course of prior checking. This exercise of prior checking opinions may be burdensome and time consuming for EU institutions and bodies.
- There are inconsistencies between the retention periods applied by EU institutions and bodies. Although some of the retention periods applied in the HR context appear excessive at the outset (e.g. a 120-year retention period for personal files), similar retention periods can be found in comparable international organisations (Council of Europe: 120 years, United Nations: 30 years after termination of service) and Member States (France: up to 80 years after birth, UK: up to 100 years after birth, Germany: until all possible claims are extinguished or 110 years after birth). Justifications for such retention periods correspond to those relied upon by the European Commission[330].
- While conducting our research, we came across cases of non-application of the retention periods. Some of them can be explained by old IT systems that may hinder the erasure of personal data.
- Certain stakeholders have stressed that the retention periods recommended by the EDPS are inappropriate with regard to their operational needs (*e.g.* the six-month retention period for logs).

Main recommendations

- The guidelines of the EDPS are a very useful tool in order to determine and apply appropriate data protection retention periods. Therefore, the evaluator encourages the adoption of further guidelines in order to assist data controllers in determining the appropriate data retention periods.

- The existing guidelines could be further improved by identifying clear retention periods (where possible) and/or giving clear criteria aimed at helping stakeholders to identify the various kinds of data and documents concerned. Nevertheless, the evaluator acknowledges that this identification of retention periods applicable to all EU institutions and bodies (without differentiation) is difficult as the retention periods are to be identified on a case by case basis.

- The EDPS should continue to follow up on the implementation of the recommendations provided to EU institutions and bodies in the course of prior checking. Indeed, it appears that certain recommendations of the EDPS are not followed by certain EU institutions and bodies.

- Raise awareness of stakeholders as regards:
  - the necessity to conserve personal data no longer than necessary;
  - the purposes for which the data were collected and processed;
  - the automatic deletion of personal data;
  - the distinction between retention for administrative purposes regulated by data protection law and retention for public archives.

[330] See above.

5 Articulation between the supervisory and advisory roles of EDPS

This section presents a case study relating to the articulation between the supervisory and advisory roles of the EDPS. This case study has been conducted on the basis of a thorough documentary review, interviews with the EDPS and DPOs from various EU institutions and bodies and a survey targeting DPOs, DPCs, data controllers and IT staff involved in data protection issues.

The European Data Protection Supervisor (hereinafter the "EDPS") is an independent European Union (hereinafter "EU") body created by Regulation (EC) No. 45/2001[331] on the basis of article 286 of the Treaty establishing the European Community[332].

Today, article 16 of the Treaty on the Functioning of the European Union[333] (hereinafter "TFEU") empowers the EDPS:

"1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. ***Compliance with these rules shall be subject to the control of independent authorities.***

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."

5.1. Assessment of the powers provided to the EDPS

5.1.1. Recall of the roles of EDPS

Pursuant to the fifth Recital of Regulation (EC) No 45/2001 and Article 41 of Regulation (EC) No 45/2001, an independent supervisory authority shall be established and shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies.

To this end, Article 41 of the Regulation specifies the two roles assigned to EDPS including:

- **a supervisory role**: the monitoring and ensuring of the application of the provisions of this Regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body;
- **an advisory role**: i.e. advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data.

[331] 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.
[332] Consolidated version of the Treaty establishing the European Community, OJ No 321 of 29 December 2006, p. 171.
[333] Consolidated version of the Treaty on the Functioning of the European Union, Official Journal No. C 326/47 of 26 October 2012, p.0001 – 0390.

The evaluation question relating to effectiveness explores the quality of the supervisory and advisory roles of the EDPS. The following sections provide a synthesis of the answer to the evaluation question on effectiveness.

Supervisory role: in order to perform its duties relating to its supervisory role (namely, investigate complaints, conduct inquiries, monitor and ensure the application of the provision of the Regulation, monitor relevant ICT developments, keep a register of processing operations, carry out prior checks of notified processing), EDPS has developed guidance and tools to facilitate the implementation of each duty and simplify the application of the Regulation.

The implementation and application of each of its supervisory tasks are effective and efforts have been made to gain efficiency. Some of these tasks are still very time-consuming, both for DPOs and EDPS (prior checks), and cause big delays in processing. In order to monitor and ensure the application of the provisions of the Regulation in each EU institution and body, the EDPS conducts a biannual survey and performs inspections as well as compliance visits. More recently, in order to address institutional criticism of the complexity of the guidance for non-specialists, the length in replying to DPOs and data controllers' concerns as regards data protection, a data protection hotline has been set up to increase support capacity for institutions on a daily basis.

Advisory role: as a EU specialist on data protection matters, **it is the responsibility of** the EDPS to advise institutions and bodies on all matters concerning the processing of personal data. Pursuant to Article 28.2 of Regulation (EC) No 45/2001, one of the main tasks of the EDPS in this regard is to examine the data protection and privacy impact of proposed new legislation even though the Regulation does not set out explicit details on the consultation procedure. The EDPS has increasingly provided formal and informal comments as well as legislative opinions. However, the evaluation pointed out that the EDPS is not systematically consulted in the legislative process: if cooperation with the European Commission and the European Parliament is satisfactory, in spite of the absence of formal procedures to involve the EDPS in the legislative process, the EDPS estimates that it is not, by itself, sufficiently involved in the discussions on data protection policy that take place at the Council of the European Union.

In addition to these tasks, the EDPS is also involved with linked responsibilities such as cooperating with national supervisory authorities[334] established in EU Member States, participating in the activities of the Article 29 Working Party on the Protection of Individuals with regard to the processing of personal data, providing secretariat to Coordinated Supervision Groups as set forth under specific legal basis (VIS, SIS II, CIS, Eurodac and IMI), as well as participating in international cooperation. Moreover, the EDPS provides day-to-day advice to EU institutions and bodies on data protection matters and also deals with litigation matters.

5.1.2. A list of powers mainly focusing on the supervisory activity of the EDPS

Article 47 of the Regulation lists the powers of the EDPS as the following: give advice to data subjects, support data controllers, warn them about or prevent a data processing if necessary, order data rectification or destruction, refer the matters to the relevant institutions, intervene in actions brought to the Court of Justice. To this end, EDPS also has the power to access all personal data and premises.

The list entitles the EDPS to authority over data controllers performing personal data processing in EU institutions and bodies, as well as a right to access the data and to order the rectification, blocking, erasure or destruction of data. This authority allows for a satisfactory level of

[334] As referred to in the Article 28 of the Directive 95/46/EC.

enforcement of the Regulation within EU institutions and bodies, since the EDPS has the necessary powers to perform this supervisory role. Nonetheless, its sanctioning power is limited to warning the controllers or imposing a ban on data processing operations.

As regards their powers relating to an advisory role on the legislative process, the list of powers of Article 47 of the Regulation does not refer to this role. The list of duties enshrined in Article 46 of the Regulation refers to the advisory role in paragraph (d) which provides for the responsibility to advise all Community institutions on all matters relating to the processing of personal data. This provision could however be interpreted as a role limited to advice pertaining to the elaboration of internal rules regarding data processing within European institutions and bodies.

As a conclusion, the EDPS is assigned two roles: a supervisory role and an advisory role. The analysis of the effectiveness of governance highlighted the fact that the EDPS' organization of work allows for a satisfactory performance of these activities, although some of the supervisory tasks (prior checks) are very time-consuming and cause delays in the overall process of data processing for data controllers. The advisory role on the legislative process is highly dependent upon the quality of the relationship with the relevant institutions (European Commission, European Parliament and European Council) and their needs to get support from EDPS. This is especially true since the Regulation does not describe the EDPS consultation procedures[335].

In order to perform these activities, the Regulation foresees a list of duties and powers for the EDPS. A matching analysis highlights the limited number of duties relating to the EDPS' advisory role. This explains why the EDPS is highly dependent on the will of the institutions to consult it during the legislative process. On the other hand, the list of duties and powers enshrined in Articles 46 and 47 of the Regulation illustrate the weigh given to the supervisory role of the EDPS by the Regulation.

5.2. Allocation of resources between all the tasks of the EDPS

The articulation of the supervisory and advisory roles of the EDPS must be analysed in light of the time spent on each activity and the allocation of resources.

5.2.1. Total resources allocated by EDPS

Annual reports provide information on the staff allocation per unit and the evolution of these figures over time. The overall budget and number of official staff both increased regularly between 2004 and 2012 and have remained stable since then, although the 2015 budget has slightly increased in comparison with the 2014 budget.

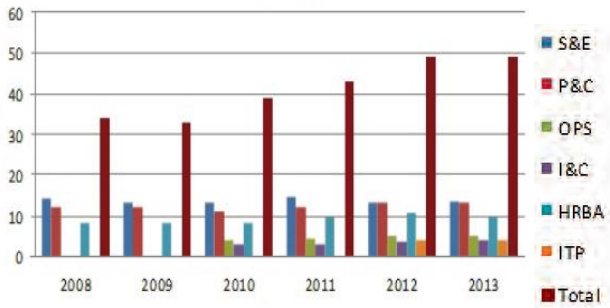
[335] Article 28 of the Regulation only provides for the consultation of the EDPS by the Commission when adopting a legislative proposal relating to the protection of individual's rights and freedoms with regard to the processing of personal data.

5.2.2. Comparison of resource allocation between supervisory and advisory roles

A similar number of staff in the supervision and enforcement unit and in the policy and consultation unit, stable since 2008

The analysis of the staff allocation per unit clearly shows that the number of official staff has remained stable since 2008 in the following units: supervision and enforcement (S&E), policy and consultation (P&C), human resources and business administration (HRBA), whereas other units have been set up in the meantime (Information and Communication sector, Information technology policy sector and Records management group), notably to provide support to the work done by the others.

Figure 1 - Evolution of EDPS official staff by unit since 2008 (source: EDPS Annual report)



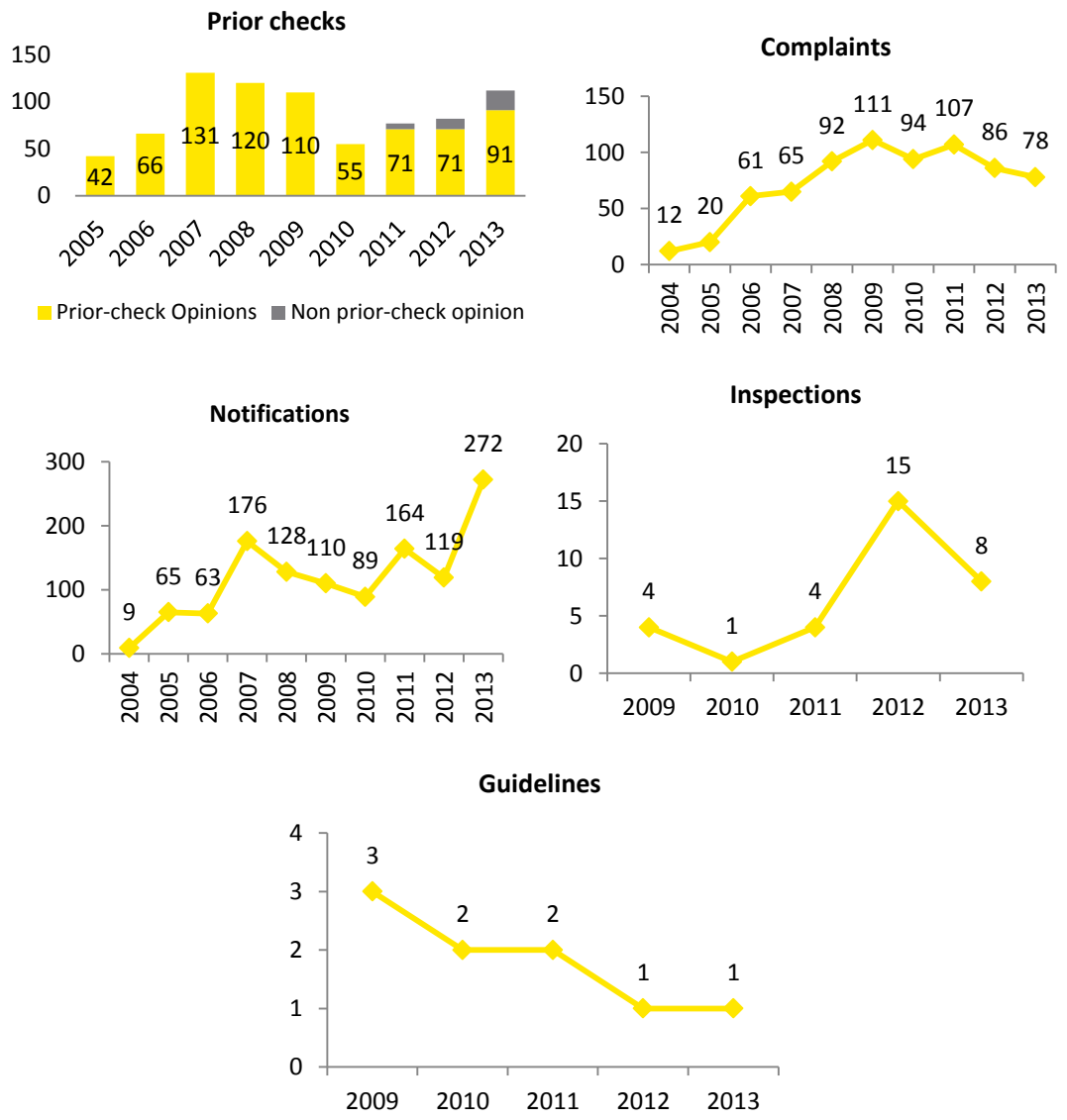
The supervision and enforcement unit accounts for one quarter of the staff costs which is equivalent to the allocation of staff costs to the policy and consultation units. Together with the human resources and business administration units, they make up two thirds of the staff costs.

Efficiency gains in both units since 2008

Supervision and enforcement

When considering the number of activities performed by the S&E unit since 2008, the stable number of staff members reflects the important gain in efficiency in this unit, in particular with regard to the increase in the number of notifications received, inspections performed and the implementation of new tools to improve the support to Institutions and bodies such as compliance visits and the hotline for DPOs and data controllers. In particular, the regular development of guidelines has contributed to limiting the need for EDPS support for data controllers and DPOs. Although the time spent on each activity can vary a lot between two cases, these figures clearly illustrate the level of activity of the unit.

Figure 2 - Evolution of S&E unit activities since 2004 (source: EDPS annual reports)

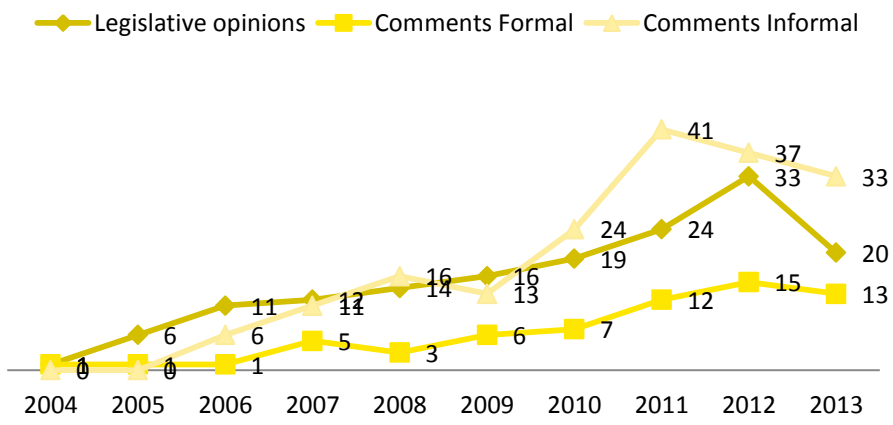


Policy and consultation

As regards the policy and consultation unit, the number of comments and opinions provided since the establishment of the EDPS regularly increased between 2004 and 2011 and has been fairly stable since then (although the 2013 reduction in activity corresponds to the large amount of time dedicated to the reform of the GDPR[336]). The 2008 level represents roughly half of the 2013 activity, although the number of staff has been fairly stable since 2008. This effort reflects the increased efficiency of the unit, based mainly on the improved skills of the unit members.

[336] General Data Protection Regulation.

Figure 3 - Evolution of legislative opinions and comments provided by the EDPS since 2004 (source: EDPS annual reports)



Our assessment of the allocation of resources between both units in comparison with the weight given to each underpinning task in the Regulation

When comparing these figures to the importance given to each role (i.e. supervisory and regulatory roles) in the Regulation as presented above, it appears that the S&E unit performing most of the supervisory tasks and the P&C unit performing most of the advisory tasks occupy the same level of staff although priority seems to be given to the supervisory role of the EDPS in the Regulation.

This statement must be balanced by the fact that the information technology policy sector composed of 4 official staff members in 2013 and 6 in 2015 also supports the supervisory and advisory roles of the EDPS and the S&E unit which also performs advisory tasks (art 28.1 & 46 (d)). In addition, other support or transversal services (I&C, HRBA and OPS) also provide support to the two policy units (S&E and P&C). The P&C unit also performs tasks that go beyond the Regulation (EC) No 45/2001, including the provision of Secretariat to Coordinated Supervision Groups as set forth under specific legal bases (VIS, SIS II, CIS, Eurodac and IMI), as well as international cooperation for instance.

5.2.3. The new EDPS strategy: priority given to increased cooperation and advisory role

The new EDPS strategy for 2015-2019 is structured across three axes:

- **Data protection goes digital**: the role of digital technologies to ensure data protection;
- **Forging global partnerships**: cooperation at an international level on data protection issues;
- **Opening a new chapter for EU data protection**: evolution of EU data protection rules.

This new strategy highlights the commitment of EDPS to improve its supervisory role on data protection with the help of new digital technologies. The third axis focuses on the will to promote dialogue on new EU rules for data protection and to support the policy making process corresponding to its advisory role. The second axis highlights the role the EDPS wants to play in international discussions on data protection. This role has been assigned to the recently appointed European Data Protection Supervisor in the *Vacancy Notice for the European Data Protection Supervisor "COM/2014/10354"* [337] *(representing the EDPS at the highest levels and developing and*

[337] Vacancy notice for the European Data Protection Supervisor COM/2014/10354 (2014/C 163 A/02), OJ C 163 A/6 28.5.2014.

maintaining effective relationships with a diverse community of stakeholders in other EU institutions, Member States, non-EU countries and other national or international organisations).

While the primary role of the EDPS, as per the Regulation,(being) is the supervision of EU institutions and bodies, the allocation of resources as well as the EDPS' strategy do not seem to fully reflect this. This is partially linked to the fact that the EDPS' activities embrace other tasks than those provided by Regulation (EC) No 45/2001. An allocation of resources in favour of the supervision and enforcement unit could be foreseen in order to (1) intensify the existing supervision activities of the EDPS (inspections, compliance visits, guidelines) and (2) better reflect the weight given to supervision in the regulation (subject to our above-mentioned comment). The implementation of the activity-based cost project (on-going) will facilitate the monitoring of resources with regard to the assigned objectives of the EDPS.

5.3. Legal feasibility of providing the EDPS with the power to impose financial sanctions (in the light of the GDPR)

One of EDPS' main tasks is the supervision and enforcement of personal data processing operations carried out by the European institutions and bodies under Regulation (EC) No. 45/2001. In order to fulfill this task, the EDPS has been granted several supervisory powers listed in Article 47 of Regulation (EC) No. 45/2001 (e.g. possibility to give advice, to make proposals for remedying a breach, to warn or admonish, to order to rectify, block, erase or destroy data, etc.). In particular, it should be noted that article 47.1 (f) of Regulation (EC) No. 45/2001 grants the EDPS with the power to "*impose a temporary or definitive ban on processing*".

Concerns have been expressed by DPOs about the inefficiency of the range of sanctioning powers granted to the EDPS. It has been stressed that granting the EDPS a power to impose financial fines could contribute to better enforcement of the Regulation (and thus, respect of the data controllers). As a consequence, this document aims to analyse the possibility of granting the EDPS the power to fine EU institutions and bodies in order to strengthen its supervisory authority.

In this context, it is important to address questions of legal (I) and policy (II) feasibility in the EU context.

To determine the legal feasibility of granting the EDPS power of financial sanction on EU institutions and bodies, our analysis begins with a comparative study of the EPDS with other EU institutions and bodies. Specific attention must be paid to the powers of the Court of Justice of the European Union.

5.3.1. Comparison with other European supervisory authorities

First, a comparison with the powers entrusted to other major EU supervisory authorities provides us with a general overview of the EU institutional architecture as well as a glimpse into the possibility of granting to grant the EPDS power of financial sanction.

The EU is composed of three main institutions empowered to make European laws and policies:

- The European Parliament is elected by the European citizens and represents them;
- The Council of the EU (also called the Council of Ministers) represents the governments of the European Union's State Members;

- The European Commission represents the interests of the Union.

Many other independent institutions and bodies gravitate around those three institutions. Among them, we identified three main authorities whose task it is to supervise activities of other EU institutions and bodies:

- The European Ombudsman;
- The European Court of Auditors;
- The European Anti-Fraud Office.

A study of those three, main European supervisory institutions and bodies (would) allows us to obtain a precise overview of the situation of the major EU supervisory institutions and bodies.

The European Ombudsman

The European Ombudsman is a European body, established by Articles 20 and 228 TFEU, in order to investigate maladministration in European institutions and bodies.

After an inquiry is opened once a complaint is made or on its own initiative, the Ombudsman has various options[338]. It can:

- propose a friendly amicable solution that will satisfy the complainant;
- issue a draft recommendation in which the Ombudsman asks the institution to correct the maladministration;
- issue critical remarks;
- notify competent national authorities of facts relating to criminal law and, if appropriate, apprise the EU institution with authority over the official or servant concerned[339].

In settling a case of maladministration, the Ombudsman has no power to adopt an injunction on other European institutions and bodies. It can only make proposals, recommendations or remarks. So the Ombudsman does not enjoy any power to take financial sanctions.

The European Court of Auditors

- The European Court of Auditors (hereinafter the "ECA") is a European institution established by Articles 285 to 287 TFEU.
- The ECA is the EU's independent external auditor and has the responsibility "*to carry out the Union's audit*" (Article 285 TFEU).
- Article 287 TFEU describes the ECA different tasks and its functioning is regulated by Rules of procedure[340].

According to Article 287.1 TFEU:

*"The **Court of Auditors** shall provide the European Parliament and the Council with a **statement of assurance as to the reliability of the accounts and the legality and regularity of the underlying transactions** which hall be published in the* Official Journal of the European Union. *This statement may be supplemented by specific assessments for each major area of Union activity."*

According to Article 287.2 TFEU:

[338] Annual report of the European Ombudsman, 2013 (www.ombudsman.europa.eu).
[339] Decision 94/262/ECSC, EC, Euratom of the European Parliament of 9 March 1994 on the regulations and general conditions governing the performance of the Ombudsman's duties, JO L 113 of the 4.5.1994.
[340] Rules of procedure of the Court of Auditors of the European Union, JO L 103/1 of the 23.4.2010.

"The Court of Auditors shall examine the accounts of all revenue and expenditure of the Union to improve financial management and report to the citizens of Europe on the use made of public funds by the European authorities."

To perform its duties, the ECA has authority to carry out an audit of revenue and an audit of expenditure the conditions of which are described in article 287.3 TFEU.

Lastly, according to Article 287.4 TFEU, the ECA issues an annual report at the close of each financial year. The report is shared with other EU Institutions which can reply to the Court of Auditors. The report and the replies are published in the Official Journal of the European Union. The ECA may also submit observations on specific questions and deliver opinions at the request of one of the other institutions or bodies of the Union.

The Court of Auditors has no power to impose financial sanctions.

The European Anti-Fraud Office

Established in 1988 as part of the Secretariat-General of the European Commission, the European Anti-Fraud Office (hereinafter the "OLAF") became an independent entity within the European Commission in 1999[341].

It has various missions among which the fight against "*fraud, corruption and any other illegal activity affecting the financial interest of the Union*" (article 1.4 of Regulation (EU, Euratom) No. 883/2013[342]).

To this End, the OLAF can undertake internal investigations within the EU institutions, bodies, offices and agencies, regarding serious matters relating to the discharge of professional duties by members and staff of the EU institutions and bodies that could result in disciplinary or criminal proceedings (article 4 of Regulation (EU, Euratom) No. 883/2013). After each investigation, the Office has to issue an investigation report which must be accompanied by recommendations made by the Director-General as to the action that should or should not have been taken in response to the findings. The recommendations may consist of: disciplinary (such as a reprimand, demotion or dismissal), administrative (such as amendments to contracts, changes in rules or improvements to recruitment procedures), financial (such as recovery of disbursed funds, imposition of financial penalties or exclusion from procurement procedures) or judicial actions (such as a report to the competent public prosecutor's office) by the institutions, bodies, offices and agencies concerned (article 11 of Regulation (EU, Euratom) No 883/2013).

Since such measures are taken by the relevant EU institutions or by the competent authorities of the relevant Member State, OLAF has no power to impose sanctions or to take any action against persons under investigation or persons who, in the light of the facts, are shown to bear some degree of responsibility.

It follows from the above that none of these three major EU supervisory authorities have been empowered to impose financial sanctions on other European institutions and bodies, including the authority to impose financial sanctions.

5.3.2. Powers of the Court of Justice of the European Union

At a second step, it is important to explore whether, and under which conditions, the Court of Justice of the European Union (CJUE) is legally vested with the power of financial sanction, bearing

[341] Commission decision 1999/352/EC, ECSC, Euratom of 28 April 1999 establishing the European Anti-fraud Office (OLAF), JO L 136/20 of the 31.5.1999.

[342] Regulation (EU, Euratom) No. 883/2013 of the European Parliament and of the Council, of 11 September 2013, concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999.

in mind that the EDPS cannot go beyond the CJEU's prerogatives. This will enable us to determine whether it is legally possible to grant the EDPS the power to take financial sanctions on EU institutions and bodies.

The CJEU is the judicial institution of the European Union. The CJEU consists of three courts:

- the Court of Justice;
- the General Court;
- the Civil service Tribunal.

Overview of the jurisdiction of the CJEU

According to article 256 TFEU, the main jurisdiction of **the General Court** is to hear and determine, at first instance:

- actions for annulment of measures adopted by EU institutions and bodies (article 263 TFEU);
- actions for failure to act against an EU institution or body (article 265 TFEU);
- actions for damages against EU institutions and bodies (article 268 TFEU referring to article 340 TFEU).

The General Court also has jurisdiction to hear and determine actions against decisions of specialized courts and, as a matter of principle (but this option has yet to be implemented), to hear and determine questions referred for a preliminary ruling in specific areas (article 256.3 TFEU) such as an exception to the principal jurisdiction of the Court of Justice.

The Court of Justice has jurisdiction:

- to hear and determine actions for failure to fulfill obligations against EU Member States (articles 258 to 260 TFEU describe the main procedure), at first and last instance;
- to hear and determine the references for preliminary rulings (article 267 TFEU), on both the interpretation and the validity of EU law;
- to hear and determine actions brought against decisions of the General Court;
- to hear and determine annulment of a measure adopted by a European institution or actions for failure to act against a European institution, in specific areas, at first instance (article 263 TFEU; article 51 of the Statute of the Court of Justice of the European Union which provides for exceptions[343]).

The Civil Service Tribunal is the first specialized court created by the Council of the European Union in 2004[344], on the basis of article 257 TFEU. It has jurisdiction to hear and determine all actions between a European institution and body and its staff (article 270 TFEU). There are two types of actions before the Civil Service Tribunal: actions regarding the legality of an act affecting a staff member and actions for damages[345].

[343] Protocol (No. 3) on the Statute of the Court of Justice of the European Union, annexed to the Treaties, as amended by Regulation (EU, Euratom) No 741/2012 of the European Parliament and of the Council of 11 August 2012 (OJ L 228, 23.8.2012, p. 1) and by Article 9 of the act concerning the conditions of accession to the European Union of the Republic of Croatia and the adjustments to the Treaty on European Union, the Treaty on the Functioning of the European Union and the Treaty establishing the European Atomic Energy Community (OJ L 112, 24.4.2012, p.21).

[344] Council decision No. 2004/752/EC, Euratom of 2 November 2004, establishing the European Union Civil Service Tribunal, JO L 333 of the 9.11.2004.

[345] Article 91 of Regulation No. 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ 45 of the 14.6.1962, p. 1385) as lastly amended by Regulation (EU, Euratom) No. 1023/2013 of the European Parliament and of the Council of 22 October 2013 (OJ L 287 of the 29.10.2013, p. 15).

Procedures in which the CJEU can impose financial convictions

There are only three instances in which the CJEU can impose financial convictions on the defendant.

1/ According to article 260 TFEU, in the context of an action for failure to fulfil obligations against a EU Member State, the Court of Justice can impose a lump sum or penalty payment to a Member State which:

- has not complied with its judgment;
- has not fulfilled its obligation to transpose a directive.

2/ According to article 268 TFEU referring to article 340 TFEU, in the context of an action for damages against a European institution or body, the General Court can condemn the institution or body to pay damages in case of non-contractual liability.

3/ In the context of an action for damages before the Civil Service Tribunal, the Tribunal can also condemn the defendant, a European institution or body or a staff member, to pay damages.

Among those three instances, one relates to sanctions against Member States and the other two relate to damages. It appears that the TFEU and the related legislative texts do not grant the CJUE per se the power to take financial sanctions upon European institutions and bodies.

In this regard, we refer to the *Consorzio Cooperative d'Abruzzo*[346], which has initiated a well-established case law since 1987 in support of such a statement.

In this particular case, the *Consorzio Cooperative d'Abruzzo* (hereinafter the "Consorzio") brought an action before the Court of Justice of the European Communities (CJEC) under article 173 of the European Economic Community Treaty[347] (today's article 263 TFEU), for the annulment of a European Commission decision amending a first decision relating to the allocation of a contribution by the Guidance Section of the European Agricultural Guidance and Guarantee Fund (EAGGF). In addition to the annulment of the amending decision, the Consorzio also requested the Court to hold that the first Commission decision was valid and irrevocable and to order the Commission to pay the contribution. On this specific point, the judgment established that the Court of Justice was not empowered to issue an injunction against the EU administration:

"*The Consorzio's other two claims are inadmissible since the power to annul measures conferred upon the Court by Article 173 of EEC Treaty does not authorize it either to confirm Commission decisions or to issue order to the Commission.*"

It has been interpreted that the CJEU cannot grant itself powers of injunction against EU institutions and bodies since these powers are not provided for in the TFEU[348]. The same reasoning could be applied to a power of financial sanction granted to the CJEU. Since the TFEU does not expressly confer this power to the CJEU, the CJEU would not be able to take financial sanctions against EU institutions and bodies.

Regarding the power of financial sanctions granted to the CJEU, it would be necessary to amend the TFEU - as was done in 1993[349] - when the Maastricht Treaty granted theCJEC the power to impose a lump sum or penalty payment on a Member State[350].

In these circumstances, should the EDPS be granted with the power to impose financial sanctions on European institutions and bodies, this power would not interfere with the prerogatives conferred on the CJEU.

[346] CJCE, 26 February 1987, *Consorzio Cooperative d'Abruzzo,* 15/85, point 18.
[347] European Economic Community Treaty, Rome, 25 March 1957.
[348] F. Donnat, « *Le contrôle juridictionnel des institutions et de l'administration de l'Union »,* in J.-B. Auby et J. Dutheil de la Rochère (dir.), « *Traité de droit administratif européen* », 2e éd., Bruylant, 2014, p. 253.
[349] Treaty on European Union, Maastricht, 7 February 1992, OJ C 191 of 29.7.1992.
[350] F. Donnat, « *Le contrôle juridictionnel des institutions et de l'administration de l'Union »:* op. cit.

5.3.3. Rules and principles applicable to an attribution of sanctioning power to the EDPS

The EDPS currently has a large array of powers enshrined in Article 47 of Regulation (EC) No 45/2001, in order to carry out its supervisory tasks. When compared to the European Ombudsman, these powers are more extensive, given the possibility of the EDPS to compel institutions to act in a certain way (see Article 47(1)(e)).[351] These powers, however, do not entail the imposition of administrative fines on other EU institutions.

While the possibility of conferring sanctioning powers to EU institutions is not expressly addressed in the Treaties, it is, in principle, possible to provide such sanctioning power through legislative measures. Article 261 TFEU addresses the possibility of ensuring judicial review of sanctions included in regulations:

'*Regulations adopted jointly by the European Parliament and the Council, and by the Council, pursuant to the provisions of the Treaties, may give the Court of Justice of the European Union unlimited jurisdiction with regard to the penalties provided for in such regulations*.'

This provision, however, does not address the establishment of sanctioning power as such and does not give indications on the addressee of these sanctions.

However, according to current interpretation, the possibility to confer the power to impose sanctions in secondary law is limited to sanctions against natural and legal persons other than the Member States and the EU organs.[352] Indeed, although sanctioning powers are granted through regulations to the European Central Bank[353] or the European Commission in the context of competition law[354], such sanctions are directed against private entities and not European institutions or Member States. This interpretation seems to be reinforced through the fact that the Courts' ability to impose sanctions on Member States according to Art. 260 required a Treaty amendment. Thus, it seems that possibility to impose sanctions against EU institutions would always have to be enshrined in the Treaties, rather than be created through secondary law.

Regardless of whether or not the sanctioning powers against institutions could be established via secondary legislation, the delegation of such powers to the EDPS would - under the current framework - also face a further constraint: the so called *Meroni* doctrine. This was originally established in the early case law of the EU Courts in order to clarify the limits of the delegation of powers from Union institutions to other bodies having their own legal personality.[355] The original judgment established that a delegation of power can never extend beyond the power that the delegating body has been accorded under the Treaties.[356] Since the current Treaty framework does not contain the power for any EU institution to impose fines on another institution, it does not seem within the remit of the current Treaty framework to confer such powers on the EDPS. Thus a Treaty amendment would, first of all, have to introduce the power to fine Union institutions and bodies, which could then eventually be delegated by the legislating institutions to the EDPS. Attention must

[351] H. Hofman, G. Rowe and A. Türk, *Administrative Law and Policy of the European Union,* (Oxford: Oxford University Press, 2011), at p. 743.
[352] D. Booβ, 'AEUV Art. 261 Rn. 1-18', in E. Grabitz, M. Hilf and M. Nettesheim, *Das Recht der Europäischen Union* (54. Ergänzungslieferung), (München: Beck, 2014); J. Schwarze, 'Artikel 229 EGV', in J. Schwarze (Ed.), EU Kommentar (Baden-Baden: Nomos, 2000).
[353] Council Regulation (EC) No 2532/98 of 23 November 1998 concerning the powers of the European Central Bank to impose sanctions, OJ L 318, 27.11.1998, p. 4–7.
[354] See e.g. Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation), OJ L 24, 29.1.2004, p. 1–22.
[355] Case 9/56 *Meroni and Co., Industrie Metallurgiche S.p.A. v. Highly Authority* [1957-58] ECR 133; Case 10/56 *Meroni and Co., Industrie Metallurgiche S.p.A. v. Highly Authority* [1957-58] ECR 157.
[356] Ibid., p. 149-150.

be drawn to the fact that the delegation of power to fine would imply the ability of the EDPS to take legally binding decisions.

Furthermore, the Court in *Meroni* also held that it would not be possible to confer powers that involve a wide margin of discretion.[357] The prohibition of delegating measures with a wide margin of discretion has recently been further defined in a case concerning the powers of the European Securities and Markets Authority (ESMA), in which the Court established the possibility of delegating powers in cases where they '*are circumscribed by various conditions and criteria which limit (...) discretion*'.[358] Whether a delegated power is sufficiently delimited needs to be determined on a case-by-case analysis. The rationale of the prohibition of discretionary powers is the protection of the legislating institutions' prerogative to determine the policy of the Union. When applied to the situation of the EDPS, a delegation of the power to fine would thus only be possible where the data protection rules are sufficiently clear and precise to delimit the scope of the EDPS in imposing fines on other institutions. As epitomised by the *Bavarian Lager* ruling debate, this, at least for the time being, does not necessarily seem to be the case. It could, however, be possible to imagine the establishment of a detailed framework for fining in the future.

It would appear that entrusting the EDPS with the power to impose financial sanctions upon other EU institutions would, in any event, require an amendment of the Treaties. Indeed, providing the EDPS with such an authority would introduce a new supervisory mechanism to the administrative law of the Union. As it emerges from the previous analysis, currently no institution or body in the Union has been granted the power to impose financial sanctions on other EU institutions and bodies. It is therefore imperative to assess how this supervisory power would fit into the current Treaty-based institutional framework of the Union. This especially calls for an assessment in the light of the principles of institutional balance and sincere cooperation as laid down in Article 13(2) TEU.

Overall, the conferral of sanctioning power is dependent on the will to introduce the authority of administrative fining from one institution to another. It is questionable whether such sanctioning power can then be delegated to the EDPS. If a delegation of a similar authority is deemed politically appropriate, it remains subject to the constraints stemming from the criteria established in *Meroni* and further defined in the *ESMA* judgment.

Our analysis demonstrates that the introduction of a fining authority to the EDPS in order to sanction institutions for non-compliance with the data protection regulation would require a considerable change in the Treaty framework of Union.

Under current law, Article 49 of Regulation (EC) No 45/2001 provides for a powerful enforcement mechanism of the data protection regulation. This entails the possibility of starting disciplinary procedures against EU officials acting in breach of the data protection regulation:

'*Any failure to comply with the obligations pursuant to this Regulation, whether intentionally or through negligence on his or her part, shall make an official or other servant of the European Communities liable to disciplinary action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Communities or in the conditions of employment applicable to other servants*.'

This appears as a powerful mechanism aimed at deterring negligent behaviour in the handling of data by the EU institutions.

[357] Ibid., p. 152.
[358] Case C-270/12 *United Kingdom v. European Parliament and Council of the European Union*, (not yet published), para. 45.

5.3.4. Policy arguments to consider when analysing the possibility of entrusting fining authority to the EDPS

Our previous analysis demonstrates that, at least theoretically, it might be legally sound, subject to an amendment of the existing Treaty framework, to provide for a power of financial sanctions against European institutions and bodies to the benefit of the EDPS.

Nevertheless the budget of the EDPS is part of the general budget of the European Union. According to article 314 TFEU, every year, the European Commission establishes a draft of the general budget for the European Union, which must be approved by the European Parliament and the Council. The general budget draft for 2015 is divided into sections relating to the Parliament, the Commission, the Council, the Court of Justice, the Court of Auditors, the Economic and Social Committee, the Committee of the Regions, the European Ombudsman, the European data-protection Supervisor and the European External Action Service[359].

As the EDPS' budget is part of the same budget as the other EU institutions and bodies', a power of financial sanction may have limited impact. The lump sums or the financial penalty paid by the European institutions and bodies to the EDPS would only leave the European Union's budget to flow back into it immediately.

Furthermore, the EDPS considers its existing powers of enforcement and sanction sufficient to perform its tasks efficiently. The EDPS emphasized that sanctions are very rarely enforced by the EDPS. There have only been four bans of data processing operations since the EDPS' creation and they were never imposed after an inspection. Usually, and in practice, EU institutions or bodies comply with the EDPS' recommendations within a very reasonable timeframe.

[359] Draft General Budget of the European Union for the financial year 2015, COM (2014) 300, June 2014 (http://eur-lex.europa.eu/budget/www/index-en.htm).