3. A divided European data protection framework: A critical reflection on the choices of the European legislator post-Lisbon

Eleni Kosta

1. INTRODUCTION

The Data Protection Directive (DPD)[1] was adopted in 1995 and regulated the issue of processing of personal data and their free movement, setting out the general principles that have to be followed. However, the DPD left outside its scope the processing of personal data with regard to activities that relate to 'police and judicial cooperation in criminal matters'.[2] Such processing was later regulated by the 2008 Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[3] The adoption of these two separate legal instruments was dictated by the three-pillar structure that was introduced with the Treaty of Maastricht in 1993.[4] The first pillar consisted of the European Community covering internal market issues, while the third pillar regulated issues on cooperation in justice and home affairs. The role of the Commission and the European Parliament was limited in the second and third pillars, while the Council was the institution with the greatest power deciding on the issues falling under these two pillars. The Amsterdam Treaty[5] modified the Treaty of Maastricht; it extended the powers of the Commission and the Parliament and strengthened the role of the European Court of Justice in third pillar issues. In accordance with the pillars system, the Data Protection Directive was adopted as first pillar legal instrument, while the Framework Decision was adopted under the third pillar.

The Lisbon Treaty[6] was signed in 2007 and abolished the three-pillar structure. It introduced Article 16 in the Treaty on the Functioning of the European Union (TFEU),[7] which establishes the right to data protection and offers the legal basis for the adoption of a framework that

[1] European Parliament and the Council of the European Union, Directive 95/46/EC 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 [1995] OJ L281/31 (23.11.1995).

[2] Article 3(2) DPD referring to Title VI TEU.

[3] 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).

[4] European Union, Treaty on European Union (Consolidated Version), Treaty of Maastricht, 7 February 1992, Official Journal of the European Communities C 325/5; 24 December 2002.

[5] European Union: Council of the European Union, *Treaty of Amsterdam Amending the Treaty on European Union, The Treaties Establishing the European Communities and Related Acts*, 10 November 1997.

[6] 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.

[7] Article 1 TEU.

ensures the uniform application of data protection rules in all areas of EU law. In 2010 the European Commission presented a Communication on the future of the Area of Freedom, Security and Justice (hereafter AFSJ) where it highlighted, among other points, the need for consistent application of the right to data protection: 'We need to strengthen the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention as well as in our international relations.'[8] A second Communication followed at the end of the same year on the reform of the data protection framework in Europe.[9] Among the core issues discussed in the latter Communication was the revision of the data protection rules in the area of police and judicial cooperation in criminal matters.[10] The Commission Communications paid special attention to the need for revision of the rules contained in the Framework Decision. As the Lisbon Treaty abolished the three-pillars structure and Article 16 TFEU could be used as the legal basis for a uniform data protection framework with a broad scope of application – covering former first- and third-pillar issues, the European Commission committed, among others, to:

> consider the extension of the application of the general data protection rules to the areas of police and judicial cooperation in criminal matters, including for processing at domestic level while providing, where necessary, for harmonised limitations to certain data protection rights of individuals, e.g., concerning the right of access or to the principle of transparency.[11]

The European Parliament repeatedly highlighted that the level of protection offered in the Framework Decision was lower than the DPD and urged the Commission to propose and the Councill to adopt a legal instrument on the adoption of organic data protection legislation under the third pillar, which would provide guarantees equivalent to those under the DPD with regard to the first pillar of the Union.[12] It is interesting to note that there has not been a similar push for the harmonisation of the rules for CFSP.

In 2012, the European Commission presented a comprehensive proposal for the review of the data protection framework in Europe. The review covered, on the one hand, the replacement of the DPD with a Regulation as regards the general processing of personal data, and, on

---

[8] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Delivering an area of freedom, security and justice for Europe's citizens – Action Plan Implementing the Stockholm Programme (20.04.2010) COM/2010/0171 final.

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union (04.11.2010) COM (2010) 609 final.

[10] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union (04.11.2010) COM (2010) 609 final, p. 5.

[11] European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, 04.11.2010, COM (2010) 609 final, p. 14.

[12] European Parliament, resolution on progress in 2002 in implementing an area of Freedom, Security and Justice (Articles 2 ad 39 EU Treaty(P5_TA(2003)0126, 27.03.2003), European Parliament, Resolution on the progress made in 2003 in creating an area of freedom, security and justice (AFSJ) (Articles 2 and 39 of the EU Treaty), (P5_TA(2004)0179, 11.03.2004), European Parliament, Motion for a Resolution, (B5-0148/2004, 29.03.2004); Mark Leiser and Bart Custers, The Law Enforcement Directive – Conceptual challenges of the EU Directive 2016/680, EDPL [2019] 3, p. 367.

the other hand, the replacement of the 2008 Framework Decision with a Directive as regards the processing of personal data for law enforcement purposes. The adoption of the new framework was turbulent and long. On 15 December 2015, after three years of negotiations, the Council and the European Parliament reached an agreement on the text of both the General Data Protection Regulation (GDPR or Regulation)[13] and the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law Enforcement Directive, or LED).[14] Both the GDPR and the LED were adopted on 27 April 2016 and established a new regime for the protection of personal data in the EU.

The abolishment of the three-pillar structure, the extensive amendments introduced by the Treaty of Lisbon, and the establishment of Article 16 TFEU offered new possibilities for the regulation of data protection in the EU. The European legislator was confronted with the dilemma to either retain the fragmented data protection regime with two separate legal instruments (a Regulation and a Directive instead of the pre-existing Directive and Framework Decision) or to follow a comprehensive approach and regulate the issues on data protection in one and single legislative instrument that would cover these two fields of EU competence.[15]

This chapter aims at exploring the legislative options offered by the EU primary legislation for the regulation of data protection and reflecting on the favouring of a divided system in European data protection regulation. The chapter will first briefly present the European data protection framework that was applicable before the Treaty of Lisbon. Secondly, it will elucidate on the amendments introduced by the Treaty of Lisbon and the maze of provisions in EU primary law that are relevant for the regulation of data protection, in order to sketch the framework in which the European legislative bodies had to make their choices, leaving outside its scope a detailed analysis of the adopted secondary legislation. It further discusses the adoption of the GDPR and the LED as separate legal instruments. The chapter focuses in particular on the LED which offers a lesser level of protection to the data subject compared to the GDPR. Next, reactions at national and European level on the decision of the European regulator to adopt two separate legal instruments are presented. Finally, the chapter provides a critical reflection on the favouring a divided system in European data protection regulation, which remains fragmented, and thoughts on an alternative model based on the Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices, and agencies and on the free movement of such data.

---

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

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

[15] Paul De Hert and Vagelis Papakonstantinou, The new Police and Criminal Justice Data Protection Directive – A first analysis, (2016) 7(1) *New Journal of European Criminal Law* p. 7.

2. PRE-LISBON EUROPEAN DATA PROTECTION FRAMEWORK

The Data Protection Directive was adopted before the Lisbon Treaty under Article 100a of the Treaty of the European Community (then Article 95 TEC and now Article 114 TFEU) as an Internal Market measure. The Court of Justice of the European Union (CJEU) in two of its first data protection cases, *Rundfunk*[16] and *Lindqvist*,[17] ruled on Article 95 TEC as the legal basis for the DPD. In response to claims raised under both cases that the application of an internal market measure, i.e., the DPD, was not relevant for these cases, the Court took the position that there is no need to have an actual link with free movement between Member States in every situation for the DPD to apply. What is important, held the Court, was that the measure, in these cases the DPD, shall have the intention to improve the conditions for the establishment and functioning of the Internal Market.[18] The Court further argued that a contrary interpretation:

> could make the limits of the field of application of the directive particularly unsure and uncertain, which would be contrary to its essential objective of approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislations.[19]

The 2008 Framework Decision on data protection in police and judicial cooperation in criminal matters was adopted on the basis of Articles 30, 31 and 34(2)(b) of the Treaty of the European Union (TEU)[20], as an instrument regulating a common action in the field of police cooperation and judicial cooperation in criminal matters, leaving outside its scope all national data processing activities. The Framework Decision was a third pillar legal instrument with extensive powers of the Council in deciding on its content.[21]

The borderline between the Data Protection Directive and the Framework Decision is not always clear in practice, leaving a number of issues in a grey zone, such as the exchange of personal data between private parties and the police for the purposes of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, which were surrounded by legal uncertainty.[22] A prominent example was the transfer of Passenger

[16] Judgment of 20 May 2003, *Österreichischer Rundfunk and others* (C-465/00, C-138/01 and C-139/01, ECR 2003 p. I-4989) ECLI:EU:C:2003:294.

[17] Judgment of 6 November 2003, *Lindqvist* (C-101/01, ECR 2003 p. I-12971) ECLI:EU:C:2003:596.

[18] Judgment of 20 May 2003, *Österreichischer Rundfunk and others* (C-465/00, C-138/01 and C-139/01, ECR 2003 p. I-4989) ECLI:EU:C:2003:294, para. 41.

[19] Judgment of 20 May 2003, *Österreichischer Rundfunk and others* (C-465/00, C-138/01 and C-139/01, ECR 2003 p. I-4989) ECLI:EU:C:2003:294, para. 42. For an in-depth analysis see Derrick Wyatt QC, Community competence to regulate the Internal market, in Michael Dougan and Samantha Currie, *50 Years of the European Treaties: Looking Back and Thinking Forward* (Hart Publishing 2009), p. 93 ff and in particular 130 ff.

[20] Consolidated Version of the Treaty on European Union [2008] OJ C115/13.

[21] Paul de Hert, Vangelis Papakonstantinou, The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for, (2009) 25(5) *Computer Law & Security Review*, p.403 ff.

[22] Magdalena Brwczyńska, A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation, in E. Kosta and R.E. Leenes, *Research Handbook on EU Data Protection* (Edward Elgar, 2022).

Name Record (PNR) data from airline companies to the US Customs and Border Protection (CBP). The European Court of Justice in a 2006 judgment[23] ruled that such transfer falls outside the scope of the DPD, as it constitutes processing operations concerning public security and the activities of the State in areas of criminal law.[24] Although the data were initially collected for commercial purposes, the Court found that the actual purpose of their transfer falls within a framework established by the public authorities that relates to public security and thus the processing falls outside the scope of protection of the DPD. In that specific case, the Framework Decision was clearly not applicable. The data collected for commercial purposes fell within the protective ambit of the DPD, but when the same data were further transferred for public security reasons, they were not covered by data protection rules.[25] The judgment of the CJEU created a substantial *lacuna legis* in the protection of PNR data, raising the general problem of protection of personal data that are not covered by the DPD.[26] The CJEU did not follow the same reasoning in a 2009 case examining the legal basis of the Data Retention Directive.[27] Although the Data Retention Directive in fact regulated the storage of traffic and location data for the purpose of the investigation, detection and prosecution of serious crime, the Court found that it was correctly adopted under the first pillar.[28] Both these cases illustrate that the line between the first and third pillar legal instruments was not always clear and left certain data processing operations in a grey zone of protection.

3. THE QUEST FOR HARMONISATION AFTER THE LISBON TREATY

3.1 The Treaty of Lisbon

The Lisbon Treaty was adopted by the Intergovernmental Conference and was signed on 13 December 2007. The European Union is, after the Lisbon Treaty, founded on two treaties with the same legal value, the TEU and the TFEU: the former containing provisions on democratic principles, the institutions, enhanced cooperation, and common foreign and security policy (CFSP), while the latter specifies the legal bases on which the EU and its institutions act and legislate. The Lisbon Treaty abolished the three-pillar structure and established the 'ordinary

---

[23] Court of Justice of the European Union, Judgment of 30 May 2006, Parliament/Council (C-317/04 and C-318/04, ECR 2006 p. I-4721) ECLI:EU:C:2006:346.

[24] Paragraph 56 Court of Justice of the European Union, Judgment of 30 May 2006, Parliament/Council (C-317/04 and C-318/04, ECR 2006 p. I-4721) ECLI:EU:C:2006:346.

[25] Kosta, Eleni, Coudert Fanny and Dumortier Jos Data protection in the third pillar: in the aftermath of the ECJ decision on PNR data and the data retention directive, (2007) 21(3) *International Review of Law, Computers and Technology*, p. 343–358.

[26] See also the analysis made by Hielke Hijmans, in Hielke Hijmans 'De derde pijler in de praktijk: leven met gebreken Over de uitwisseling van informatie tussen lidstaten'. SEW 2006.91, under chapter 4.1.

[27] 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, OJ L 105, 13.4.2006, p. 54–63.

[28] C-301/06 - Ireland v Parliament and Council, judgment of the Court (Grand Chamber) of 10 February 2009.

legislative procedure',[29] which was known as co-decision procedure before the Lisbon Treaty, putting an end to separate policy-making procedures and regimes among the EU actions and activities. The Lisbon Treaty also redefined the fundamental rights architecture in the EU and included specific provisions for the protection of personal data.[30]

The TFEU in Title V covers the area of Justice and Home Affairs, which is renamed the Area of Freedom, Security and Justice (AFSJ). Chapter 2 of Title V TEU contains specific provisions on CFSP. In reality, the Lisbon Treaty, although it abolishes the second pillar, it retains its main characteristics.[31] Article 24(1) TEU clearly specifies the special regime of CFSP: 'The common foreign and security policy is subject to specific rules and procedures. It shall be defined and implemented by the European Council and the Council acting unanimously, except where the Treaties provide otherwise. The adoption of legislative acts shall be excluded.'[32]

3.2 Data Protection Provisions in the Lisbon Treaty

Article 16 TFEU is the cornerstone provision on the regulation of the protection of personal data across the EU stipulating that 'Everyone has the right to the protection of personal data concerning them.'[33] It establishes a clear rule that 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 relating to the free movement of such data, are regulated under the ordinary legislative procedure exercised by the European Parliament and the Council[34] and aims at ensuring the uniform application of rules in all areas of EU law in relation to the processing of personal data. The TFEU pays special attention to the issue of oversight in the area of data protection assigning oversight of compliance with data protection rules to independent authorities.[35]

Article 39 TEU makes use of a derogation foreseen in Article 16(2) TFEU in relation to CFSP and establishes a different regime for the processing of personal data by the Member States when they carry out activities falling within the scope of CFSP.[36] With regard to these issues, the Council is empowered to adopt a decision on the regulation of the processing of personal data in the area of CFSP.[37] As Article 39 TEU covers only Member States when regulating the processing of personal data, such processing in the area of CFSP by Union institutions, bodies, offices, and agencies will remain under the protective ambit of Article 16 TFEU.[38]

---

[29] Chalmers D, Davies G and Monti G, *European Union Law*, (Cambridge University Press, 4th edn, 2019), pp. 121 ff.

[30] Gloria González Fuster, *The Emergence of Data Protection as a Fundamental Right of the EU* (Springer Switzerland, 2014), p. 230.

[31] Jean Claude Piris, *The Lisbon Treaty – A Legal And Political Analysis*, Cambridge Studies in European Law and Policy, (Cambridge University Press, 4th edn, 2011), p. 67.

[32] Article 24(1) TEU.

[33] Article 16(1) TFEU.

[34] Article 16(2) TFEU

[35] Article 16(2) TFEU.

[36] Chapter 2 TFEU: 'Specific provisions on the common foreign and security policy.'

[37] Article 39 TEU.

[38] Hijmans H and Scirocco A, Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?, (2009) 46 *Common Market Law Review*, pp.1485–1525 (1515).

The Intergovernmental Conference that adopted the Treaty of Lisbon also adopted a number of declarations concerning provisions of the Treaties. In relation to the processing of personal data, the Intergovernmental Conference declared that:

> whenever rules on protection of personal data to be adopted on the basis of Article 16 [TFEU] could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter. It recalls that the legislation presently applicable (see in particular Directive 95/46/EC) includes specific derogations in this regard.[39]

The Intergovernmental Conference continued by adopting Declaration No 21 acknowledging that 'specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields'.[40] This Declaration allows a set of different rules to be applicable in the fields of judicial cooperation in criminal matters and police cooperation.

The Lisbon Treaty introduced an important change to the vesting with jurisdiction on former second and third pillar issues to the CJEU. It further introduced two limitations to judicial control in criminal matters, both relating to security: the CJEU does not have jurisdiction to provisions relating to CFSP nor to acts adopted on the basis of those provisions.[41] However, Article 275 TFEU recognises that the CJEU remains competent for reviewing the legality of CFSP decisions 'providing for restrictive measures against natural or legal persons'. Hijmans and Scirocco mention as examples of such decisions blacklisting measures adopted withing the CFSP framework.[42] The TFEU further limits the powers of the CJEU in relation to judicial co-operation in criminal matters and police co-operation (Chapters 4 and 5 of Title V of Part Three TFEU). More concretely the CJEU does not have:

> jurisdiction to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.[43]

This limitation is relevant for cases relating to data protection in the context of judicial co-operation in criminal matters and police co-operation.

3.3 Protocols Relating to the Area of Freedom, Security and Justice with an Impact on the Regulation of Data Protection

A number of Protocols were annexed to the Lisbon Treaty in relation to the AFSJ, which impact the regulation of the processing of personal data in the former third pillar, i.e., in the context

---

[39] Declaration No 20 on Article 16 of the Treaty on the Functioning of the European Union.

[40] Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation.

[41] Art. 275 TFEU.

[42] Hijmans H and Scirocco A, Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?, (2009) 46 *Common Market Law Review*, pp.1485–1525 (1523).

[43] Article 276 TFEU.

of judicial cooperation in criminal matters and police cooperation. Although the Amsterdam Treaty integrated the Schengen *acquis* in 2009 in the Treaties, the United Kingdom, Ireland, and Denmark chose to remain outside the Schengen area. These three countries continued to participate in issues relating to judicial and police cooperation in criminal matters, with the exceptions of issues falling under the Schengen *acquis*.

Among the Protocols annexed to the Treaty of Lisbon, two related to the AFSJ: one was adopted on the position of the United Kingdom and Ireland and a second one on the position of Denmark, which however have different scope. Protocol 21 stipulated that the United Kingdom and Ireland shall not take part in the adoption by the Council of proposed measures pursuant to the AFSJ. Therefore:

> no measure adopted pursuant to that Title (i.e., Title V of Part Three of the TFEU on AFSJ), no provision of any international agreement concluded by the Union pursuant to that Title, and no decision of the Court of Justice interpreting any such provision or measure shall be binding upon or applicable in the United Kingdom or Ireland; and no such provision, measure or decision shall in any way affect the competences, rights and obligations of those States; and no such provision, measure or decision shall in any way affect the Community or Union acquis nor form part of Union law as they apply to the United Kingdom or Ireland.[44]

However, the UK and Ireland retained the right to take part in the adoption and application of any proposed measure relating to the AFSJ, following a specific procedure.[45]

Article 6a of Protocol 21 was dedicated to the processing of personal data and reads as follows:

> The United Kingdom and Ireland shall not be bound by the rules laid down on the basis of Article 16 [TFEU] which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of that Treaty (i.e. on Judicial cooperation in criminal matters and on Police cooperation) where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16.[46]

This protocol clearly offers the possibility to the UK and Ireland not to participate in specific aspects of judicial cooperation in criminal matters and police cooperation and in such cases they do not have an obligation to protect personal data.

Protocol 22 annexed to the Lisbon Treaty regulates the position of Denmark and is a very broad and complicated opt-out protocol from the whole AFSJ.[47] Contrary to Protocol 21 on the position of the UK and Ireland, Protocol 22 on the position of Denmark does not provide for a voluntary participation of Denmark in the adoption and application of proposals on AFSJ measures, establishing in this way a very strict opt-out regime for Denmark. Actually, Denmark chose to add an Annex to Protocol 21, where it categorically exempts itself from

---

[44] Article 2 of Protocol 21 annexed to Lisbon Treaty.

[45] Article 3 of Protocol 21 annexed to Lisbon Treaty. More on this issue, Jean Claude Piris, *The Lisbon Treaty – A Legal and Political Analysis*, Cambridge Studies in European Law and Policy, (Cambridge University Press, 4th edn, 2011), p. 195 ff.

[46] Protocol 21 annexed to Lisbon Treaty on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice.

[47] Protocol 22 annexed to Lisbon Treaty on the position of Denmark.

any participation in the adoption by the Council of measures proposed in relation to the AFSJ, with the exception of Schengen-building measures. Denmark established thus a much stricter opt-out regime compared to the UK and Ireland.[48]

Protocol 36 annexed to the Lisbon Treaty contains transitional provisions. According to Protocol 36:

> The legal effects of the acts of the institutions, bodies, offices and agencies of the Union adopted on the basis of the Treaty on European Union prior to the entry into force of the Treaty of Lisbon shall be preserved until those acts are repealed, annulled or amended in implementation of the Treaties. The same shall apply to agreements concluded between Member States on the basis of the Treaty on European Union.[49]

However, a deadline to adapt the old instruments to the new Treaty provisions, for instance in case they do not comply with Article 16 TFEU, is not explicitly provided in the Protocol. Article 10(1) of Protocol 36 contains a specific transitional measure in relation to acts of the European Union in the field of police cooperation and judicial cooperation in criminal matters that were adopted before the entry into force of the Treaty of Lisbon. In this context:

> the powers of the institutions shall be the following at the date of entry into force of that Treaty: the powers of the Commission under Article 258 [TFEU][50] shall not be applicable and the powers of the Court of Justice of the European Union under Title VI of the Treaty on European Union (i.e., Provisions on Police and Judicial Cooperation in Criminal Matters), in the version in force before the entry into force of the Treaty of Lisbon, shall remain the same, including where they have been accepted under Article 35(2) of the said Treaty on European Union.[51]

Such transitional measures shall cease to have effect five years after the date of entry into force of the Treaty of Lisbon[52] (Article 10(3) of Protocol 36). The UK could make use of Article 10(1) of Protocol 36 in order to opt-out from legislation in the field of police cooperation and judicial cooperation in criminal matters, while under Article 10(5) of Protocol 36 the UK can choose to opt-in in relation to some legislation in the aforementioned field.

The UK made use of the powers under Article 10(1) of Protocol 36 and decided in July 2013 to opt-out from the pre-Lisbon measures in the field of police and judicial cooperation in criminal matters. The decision was effective as of 1 December 2014. The UK, at the same time, made use of the option offered under Article 10(5) of Protocol 36 and chose to opt back into 35 'ex-third pillar' measures, including the 2008 Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal

---

[48] More on this issue, Jean Claude Piris, *The Lisbon Treaty – A Legal and Political Analysis*, Cambridge Studies in European Law and Policy, (Cambridge University Press, 4th edn, 2011), p. 194

[49] Article 9 of Protocol 36.

[50] Article 258 TFEU (ex Article 226 TEC): 'If the Commission considers that a Member State has failed to fulfil an obligation under the Treaties, it shall deliver a reasoned opinion on the matter after giving the State concerned the opportunity to submit its observations. If the State concerned does not comply with the opinion within the period laid down by the Commission, the latter may bring the matter before the Court of Justice of the European Union.'

[51] Article 10(1) of Protocol 36.

[52] The Lisbon Treaty entered into force on 1 December 2009.

matters.[53] The aforementioned Framework Decision was transposed into the UK legislation through the Criminal Justice and Data Protection (Protocol No. 36) Regulation 2014 (hereafter the 2014 Regulations).[54]

3.4 Interim Thoughts

The AFSJ was divided under the first and the third pillar and measures relating to AFSJ fell under 'asymmetrical regimes',[55] which was enhanced by the restricted scope of application of the DPD and the Framework Decision, as well as the lack of clear principles for security related data processing in the case law of the CJEU.[56] The analysis of the provisions in the TEU and the TFEU that relate to the regulation of data protection in the AFSJ illustrate that these provisions form a complex matrix and there is a patchwork of legal instruments that regulate data protection related issues at EU primary law level.

4. ADOPTION OF TWO MAIN LEGAL INSTRUMENTS ON DATA PROTECTION

4.1 Towards a New European Data Protection Framework

The introduction of Article 16 TFEU aimed at facilitating the adoption of unified data protection principles in the EU. However, the patchwork of the primary rules relating to ASFJ and CFSP creates a complex landscape for the regulation of data protection issues that fall in these areas. The study of the relevant provisions of the Lisbon Treaty showed that the European legislator did not have an obligation to retain the divided system on the processing of personal data that existed pre-Lisbon. Declaration 21 annexed to the Lisbon Treaty provides the European legislator with the option ('may prove necessary') to adopt two different legal instruments: one on the general processing of personal data and one with specific rules on the

---

[53] See relevant documents on the 'UK notification according to Article 10(4) of Protocol No 36 to TEU and TFEU' on the website of the European Council: http://data.consilium.europa.eu/doc/document/ST-12750-2013-INIT/en/pdf (accessed 15 July 2021). Also see 2014/857/EU, Council Decision of 1 December 2014 concerning the notification of the United Kingdom of Great Britain and Northern Ireland of its wish to take part in some of the provisions of the Schengen acquis which are contained in acts of the Union in the field of police cooperation and judicial cooperation in criminal matters and amending Decisions 2000/365/EC and 2004/926/EC and 2014/858/EU, Commission Decision of 1 December 2014 on the notification by the United Kingdom of Great Britain and Northern Ireland of its wish to participate in acts of the Union in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon and which are not part of the Schengen acquis, O.J. L 345, 1 December 2014.

[54] The Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014, Series: UK Statutory Instruments, 2014 No. 3141.

[55] Gloria González Fuster, *The Emergence of Data Protection as a Fundamental Right of the EU*, (Springer Switzerland, 2014), p. 220; Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice – Towards harmonized data protection principles for information exchange at EU-level*, (Springer Berlin-Heidelberg, 2012), p. 171.

[56] Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice – Towards harmonized data protection principles for information exchange at EU-level*, (Springer Berlin-Heidelberg, 2012), p. 171.

protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation.

In light of early discussions for the modernisation and review of the European data protection framework, already in 2009, the European Data Protection Supervisor (EDPS) expressed his opinion on the actual policy options of the European legislator after the adoption of the Treaty of Lisbon:

> the Lisbon Treaty does not necessarily have to lead to *one* instrument applicable to *all* kinds of processing. A separate instrument for police and/or justice is not excluded and is even supported by Declaration added to the Treaty stating that specific rules on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation may prove necessary because of the specific nature of these fields. […] However, the new instruments should have a general scope and be fully consistent with each other. Both are certainly not the case now.[57]

De Hert and Papakonstantinou summarised the European legislator's choices as follows:

> (1) to release a single, comprehensive, standard-setting text that would set the general rules for all personal data processing within the EU, or (2) to continue distinguishing between commercial and security-related processing through the continued existence of the 1995 Directive and the 2008 Framework Decision, appropriately amended, respectively.[58]

Did the European legislative bodies make full use of the opportunities offered by the introduction of Article 16 TFEU or did they make choices that would contribute to further fragmentation of the EU data protection rules? The European Commission, followed by the European Parliament and the Council, chose to take up the option offered by Declaration 21 and adopted next to the GDPR, the LED, with an extended scope compared to the Framework Decision of 2008. The GDPR sets high standards and strict obligations for legitimate data processing, while it leaves data processing by competent authorities for law enforcement purposes outside its scope. The GDPR also clearly excludes from its scope of application processing of personal data by Member States, when they carry out activities that relate to the CFSP, protected in Chapter 2 of Title V of the TEU.[59] The main argument for the establishment of data protection rules in these two separate instruments is that in this way the LED offers the national legislator sufficient flexibility, which the Member States were arguing for, while the GDPR would ensure the full harmonisation of the fragmented data protection rules in the commercial context that was heavily demanded from the industry.

The European Commission defended its choice to propose two different legal instruments, claiming that such a choice would not create inconsistencies in the protection of personal data in Europe. Françoise Le Bail, Director-General (Justice) of the European Commission supported the choices of the Commission to apply Declaration 21 and highlighted the similarities between the two proposals prepared by the Commission: 'The same principles of data protection apply at the core of the Regulation, but I think the new element is that they are at

---

[57] European Data Protection Supervisor, Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulations, 11th Conference on Data Protection and Data Security - DuD 2009, Berlin, 8 June 2009.

[58] Paul De Hert, Vagelis Papakostantinou, The police and criminal justice data protection directive: comment and analysis. 22(6) *Computers & Law Magazine of SCL*, 1 at 3.

[59] Article 2(2)(b) GDPR.

the core also of the Directive, which was not necessarily the case to start with.'[60] She further argued that in the area of judicial cooperation in criminal matters and police cooperation the European legislator would have to be taking into account the different cultures of the European Member States and that a Directive would both fight against fragmentation that existed in the implementation of the framework decision across the Member States, while at the same time would offer the flexibility that was considered necessary in the field.[61]

4.2 The LED as Data Protection Legal Instrument

As already mentioned in the introduction, the European Parliament had repeatedly highlighted that the level of protection offered in the Framework Decision was lower than the DPD and asked for the adoption of organic data protection legislation under the third pillar which would provide guarantees equivalent to those under the DPD with regard to the first pillar of the Union.[62] Thus, the text of the LED was long awaited since the 2008 Framework Decision failed to regulate internal data processing activities of law enforcement, as mandated by Article 16 TFEU.

The LED applies to both domestic and cross-border processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security ('law enforcement').[63] The LED makes clear reference to 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 which adopted the Treaty of Lisbon, in which:

> the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.[64]

Despite being a milestone in the regulation of law enforcement data processing activities, the Directive was developed in the shadow of the heavily debated GDPR. Several key aspects have received too little attention and crucial questions remain unsolved, including the role

---

[60] UK House of Commons, Justice Committee, The Committee's opinion on the European Union Data Protection framework, Third Report of Session 2012-13, HC 572, published on 1 November 2012, p. 8.

[61] UK House of Commons, Justice Committee, The Committee's opinion on the European Union Data Protection framework, Third Report of Session 2012-13, HC 572, published on 1 November 2012, p. 8.

[62] European Parliament, resolution on progress in 2002 in implementing an area of Freedom, Security and Justice (Articles 2 and 39 EU Treaty (P5_TA(2003)0126, 27.03.2003), European Parliament, Resolution on the progress made in 2003 in creating an area of freedom, security and justice (AFSJ) (Articles 2 and 39 of the EU Treaty), (P5_TA(2004)0179, 11.03.2004), European Parliament, Motion for a Resolution, (B5-0148/2004, 29.03.2004); Mark Leiser and Bart Custers, The Law Enforcement Directive – Conceptual challenges of the EU Directive 2016/680, EDPL [2019] 3, p. 367.

[63] Article 1(1) LED, European Commission, Communication to the European Parliament and the Council on the 'Way forward on aligning the former third pillar acquis with data protection rules', 24.06.2020, COM(2020) 262 final, p.2.

[64] Recital 10 LED.

of consent, the categorisation of data subjects, the separation between facts and opinions, the application of the LED on national security agencies, the rights of the data subjects etc.[65] Nevertheless, for the first time, the LED provides a harmonised framework for data processing activities performed for the prevention, investigation, detection or prosecution of criminal offences. It forms a major building block in the data protection architecture of the EU criminal justice and law enforcement area and should be read together with other specific instruments that regulate data processing activities of EU agencies and cross-border data flows.

The initial proposal of the European Commission dedicated the scope of application of the LED to 'the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'.[66] The Council in its 2015 general approach wished to extend the scope of the Directive to the safeguarding against and the prevention of threats to public security. The Council wished to clarify via a recital what are the activities that could be covered under the Directive, as follows:

> Recital 11a
> The activities carried out by the police or other law enforcement authorities are mainly focused on the prevention, investigation, detection or prosecution of criminal offences including police activities without prior knowledge if an incident is a criminal offence or not. These can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. Those activities performed by the above-mentioned authorities also include maintaining law and order as a task conferred on the police or other law enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law, which may lead to a criminal offence.[67]

The EDPS criticised in particular the fact that

> Recital (11a) gives examples of what would be covered: police activities at demonstrations, major sporting events and riots, or, more in general, police activities maintaining law and order. We therefore recommend restricting the scope of the Directive to the activities of criminal law enforcement by police and judicial authorities, as was done in the original proposal of the Commission.[68]

---

[65] Mark Leiser and Bart Custers, The Law Enforcement Directive – Conceptual challenges of the EU Directive 2016/680, EDPL [2019] 3, p. 367 ff.; Juraj Saifert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for police and criminal justice authorities', available at SSRN: https://ssrn.com/abstract=3285873 (accessed 15 July 2021); Plixavra Vogiatzoglou, Katherine Quezada Tavárez, Stefano Fantin, Pierre Dewitte, 'From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives', Jipitec (2020) 11(3), p. 274ff.

[66] 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/2012/010 final - 2012/0010 (COD), Article 1(1).

[67] Council of the European Union, 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 on the free movement of such data (General Data Protection Regulation) - Chapter I - Article 2(e) - scope of the General Data Protection Regulation and the Data Protection Directive, 8745/3/15, Interinstitutional File: REV 3, 2012/0011 (COD) LIMITE, DATAPROTECT 73 JAI 280 MI 295 DIGIT 33 DAPIX 73 FREMP 100 COMIX 216 CODEC 689 (5 June 2015).

[68] European Data Protection Supervisor, Opinion 6/2015, A further step towards comprehensive EU data protection - EDPS recommendations on the Directive for data protection in the police and justice sectors, 28.10.2015.

Although this recommendation of the EDPS was not taken up by the EU legislative bodies, the final text of the Directive adopted a modified version of the aforementioned recital. Recital 12 stipulates that:

> The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence. Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of Regulation (EU) 2016/679.[69]

The LED is neither applicable to the data processing of most of the AFSJ law enforcement agencies, such as Europol and Eurojust, nor to other AFSJ exchange systems, such as the Schengen Information System (SIS, Schengen) or the Customs Information System (CIS, Customs) or to exchange of information falling under the Prüm decision.[70] It remains unclear however, whether the LED is applicable in cases where for instance personal data are processed for the detection or prosecution of criminal offences, let us say in the context of border controls. Sajfert and Quintel refer to the example where:

> police officers process personal data for identification or verification purposes in the field of migration and border control. A person crossing the Schengen borders irregularly might be checked by a police officer and, in those Member States where the irregular crossing of borders qualifies as a criminal offence, the police officer may change the purpose of the processing, depending on whether it is carried out for migration purposes or for prosecuting the criminal offence. However, once the irregular migrant applies for asylum, the processing of his application will fall within the scope of the GDPR, notwithstanding the initiated criminal proceedings.[71]

Moreover, the LED has not been transposed in a timely and harmonised way in the various European Member States, raising a number of conceptual and practical issues.[72]

---

[69] Recital 12 LED.

[70] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1–11.

[71] Juraj Saifert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for police and criminal justice authorities', available at SSRN: https://ssrn.com/abstract=3285873 (accessed 15 July 2021).

[72] Hudobnik, Matthias M. 'Data protection and the law enforcement directive: a procrustean bed across Europe?' in 21(3) *ERA Forum*, pp. 485–500 (Springer Berlin Heidelberg, 2020). For a detailed analysis of the conceptual and practical issues see: Mark Leiser and Bart Custers, 'The Law Enforcement Directive – Conceptual challenges of the EU Directive 2016/680', EDPL [2019] 3, p. 367 ff.

4.3 Criticism on Favouring a Divided System in European Data Protection Regulation

This choice of the European legislative bodies to retain the divided system in European data protection was not accepted without criticism. The EDPS criticised the adoption of the LED as a self-standing document[73] and favoured the adoption of a Regulation that would set out the rules on data protection, which would be further complemented by additional sectoral rules.[74] In the UK, the Justice Committee of the UK House of Commons was critical of the choice of the European legislator to introduce two instruments as 'this could cause confusion, both for data subjects, and for organisations within the criminal justice system in particular, as they will have to consider which law applies in their given circumstance'.[75] The UK Information Commissioner, Christopher Graham, expressed the position that 'the Information Commissioner's Office is deeply sceptical of this proposal to split the current Directive between a Regulation and a Directive. All sorts of mischief follows from that decision'.[76] The Deputy Commissioner and Director of Data Protection at the UK Information Commissioner's Office, David Smith, concurred with the position of the Information Commissioner and added that:

> Once we start to diverge and we have a Regulation for the commercial sector and a different legal instrument for police and justice, you start to move away from that and you cause particular problems in areas like local authorities, perhaps, which have functions that will come under the Regulation and others that will come under the Directive.[77]

Already in 2012, the EDPS had highlighted that in specific areas, where private entities and LEAs interact with each other, 'borderlines are becoming increasingly blurred'.[78] The EDPS presented a number of situations where there is lack of clarity on the applicable legal framework:

---

[73] European Data Protection Supervisor, Opinion on the data protection reform package, 07 March 2012, paras 36–40.

[74] European Data Protection Supervisor, Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – 'A comprehensive approach on personal data protection in the European Union', 14 January 2011, para. 48; European Data Protection Supervisor, Opinion 6/2015, A further step towards comprehensive EU data protection - EDPS recommendations on the Directive for data protection in the police and justice sectors, 28.10.2015, para. 34.

[75] UK House of Commons, Justice Committee, The Committee's opinion on the European Union Data Protection framework, Third Report of Session 2012-13, HC 572, published on 1 November 2012, pp. 8–9.

[76] UK House of Commons, Justice Committee, The Committee's opinion on the European Union Data Protection framework, Third Report of Session 2012-13, HC 572, published on 1 November 2012, p. 7.

[77] UK House of Commons, Justice Committee, The Committee's opinion on the European Union Data Protection framework, Third Report of Session 2012-13, HC 572, published on 1 November 2012, p. 8.

[78] European Data Protection Supervisor, Opinion on the data protection reform package, 07 March 2012, para. 38.

> for instance when information is transferred between a law enforcement authority and a private entity or when a law enforcement authority would transfer data to another public authority not responsible for law enforcement. It becomes even more complex if public information systems are partly established in the area of police and judicial cooperation in criminal matters, and partly in other areas. The clearest example on EU level is the Schengen Information System, which in addition also has national and European parts.[79]

5. LACK OF EFFECTIVE HARMONISATION

5.1 The Scope of Application of the LED

Crucial for the application of the LED is to identify whether the processing is carried out (a) by a competent authority, and (b) for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Competent authorities are defined in the LED as:

> (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[80]

Thus the LED does not apply only to traditional law enforcement authorities, such as police or the public prosecutor, but can for instance cover also private entities that are conducting data processing for law enforcement purposes, if this is foreseen in Member State's law. At the same time, the LED does not apply to every data processing operation carried out by 'competent authorities'. Such processing needs to be carried out 'for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.[81] The LED thus applies to policy and judicial authorities, leaving out other authorities, such as tax authorities, customs, authorities dealing with combating of fraud, immigration authorities etc.[82] that remain subject to the GDPR.

5.2 Involvement of Private Actors to Law Enforcement Activities

The seemingly straightforward divided system established by the GDPR and the LED is actually challenged by increasingly common practices where private entities become engaged in

---

[79] European Data Protection Supervisor, Opinion on the data protection reform package, 07 March 2012, para. 39.

[80] Art. 3(7) LED.

[81] Art. 1(1) LED.

[82] European Data Protection Supervisor, Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – 'A comprehensive approach on personal data protection in the European Union', 14 January 2011, para. 35.

providing information to LEAs. Such examples can be found in the field of cybercrime and in the field of Anti-Money Laundering/Counter Financing of Terrorism, where banks enter into collaborative agreements with law enforcement authorities and establish Public-Private Partnerships (PPPs). The European Commission expert group on the GDPR and the LED (hereafter Expert Group) focused on the delineation between the GDPR and the LED, asking for clarification of the legal framework applicable on 'data controllers from the financial sector, normally covered by the Regulation, with quite strong reporting obligations related to suspicious financial activities derived from anti-money laundering legal instruments'.[83] The activities in the context of collaboration between private companies and LEAs lay in a 'grey-zone'[84] between GDPR and LED, as in many cases it is unclear which of these instruments is directly applicable. This reality creates a risk of uncertainty as to the regime governing the processing, the applicable principles and the rights and obligations of the actors involved.[85] In practice, this means, for instance, limitation of data subject's right to access, rectify or request erasure of collected data or of data controller's processing notification obligations.

The complexity is increased by the fact that Member States have given a different interpretation in the notion of competent authority in their transposition of the LED and that some Member States apply the LED only to traditional law enforcement authorities while others extend its application to administrative authorities, such as customs and border guards. When private entities entrusted with the exercise of public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences, carry out processing of personal data, then the LED clearly applies; for instance, in the case of banks that report suspicious transactions in line with the European legal framework on anti-money laundering. Vogiatzoglou and Fantin discuss however the case of Critical Infrastructure (CI) entities as rather problematic in terms of the legal regime applicable to them when processing personal data.[86] Legislative provisions foresee that CI entities secure their facilities and bear the obligation to

> prevent physical threats and attacks against their infrastructures or individuals on field, attacks which comprise of criminal offences in the realm of criminal laws, as well as a wide range of attacks attempted or committed against their information systems, which also constitute a criminal act and as such will have to be investigated and prosecuted.[87]

---

[83] Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Minutes of the first meeting (23 September 2016), available online at https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=27804&no=2 (accessed 15 July 2021).

[84] Nadezhda Purtova, 'Between the GDPR and the Police Directive: navigating through the maze of information sharing in public-private partnerships' (2018) *IDPL* 3.

[85] E.g., Catherine Jasserand, 'Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in Directive 2016/680?' (2017) *CLSR* 3.

[86] Vlogiatzoglou Plixavra and Fantin Stefano, 'National and public security within and beyond the Police Directive' in: Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (eds*), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Cambridge, Antwerp, Chicago: Intersentia, 2019), pp. 27–62 (49).

[87] Vlogiatzoglou Plixavra and Fantin Stefano, 'National and public security within and beyond the Police Directive' in: Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (eds), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Cambridge, Antwerp, Chicago: Intersentia, 2019).

Whether these entities fall under the definition of competent authorities under the LED is left in the hands of the national legislator. Kranenborg argues that:

> to a certain extent, the precise delimitation between the GDPR and LED depends on the law of the Member States. As follows from recital 18 GDPR (and recital 18 LED) a single public authority can be subject to both the GDPR and the LED depending on the purposes of its activities.[88]

5.3 National Security and Data Protection

Lynskey argues that maybe the most difficult issue that arises from this divided regime is the fact that for certain data processing operations neither the LED nor the GDPR are applicable, as in the case of data processing for national security purposes.[89] The complexity is increased due to the blurry borderlines between the notions of 'law enforcement activity, public security and national security'.[90] According to Article 4(2)TEU 'national security remains the sole responsibility of each Member State'. Mitsilegas discussed the terminological confusion between *internal* security and *national* security arguing that it is unclear 'whether "national security" coincides or overlaps with "internal security", or whether "internal security" should be seen as covering primarily police co-operation, while 'national security' should be seen as covering military and/or intelligence action'.[91] If the latter interpretation is to be adopted, then he argues that 'the implications of including references to "national security" in the chapter on the "Area of Freedom, Security and Justice' leave room for clarification now that the Lisbon Treaty has entered into force'.[92]

Article 23 GDPR grants the possibility to restrict the rights attributed to data subjects and the application of all (except for the accountability) basic principles of the processing of personal data, i.e., the rights established in 'Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22'. Given that the fundamental right to data protection cannot be ensured without respecting data subject's rights and adhering to the principles of processing by data controllers, it is crucial to emphasise that restrictions under Article 23 must be considered exceptions. These exceptions from the general rules can therefore be applied narrowly and only under specifically prescribed circumstances.[93]

Accordingly, Article 23 GDPR requires that the restrictions may be introduced 'by way of a legislative measure', they must respect 'the essence of the fundamental rights and freedoms', and constitute 'a necessary and proportionate measure in a democratic society' to safeguard

---

[88] Kranenborg Herke, 'Article 2 – Material scope' in Kuner Ch, Bygrave L and Docksey Ch (eds) *The EU General Data Protection Regulation – A Commentary*, (Oxford University Press, 2020), p. 70.

[89] Lynskey Orla, Criminal justice profiling and EU data protection law: precarious protection from predictive policing (2019), 15 *International Journal of Law in Context* 162–176 (165).

[90] Lynskey Orla, Criminal justice profiling and EU data protection law: precarious protection from predictive policing (2019), 15 *International Journal of Law in Context* 162–176 (165).

[91] Mitsilegas Valsamis, European criminal law and resistance to communautarisation after Lisbon, (2010) 1(4), *New Journal of European Criminal Law*, pp. 458–480 (461).

[92] Mitsilegas Valsamis, European criminal law and resistance to communautarisation after Lisbon, (2010) 1(4), *New Journal of European Criminal Law*, pp. 458–480 (461).

[93] EDPB, 'Guidelines 10/2020 on Restrictions under Article 23 GDPR' (December 15, 2020) para. 3 https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202010_article23_en.pdf (accessed 25 May 2021).

[among others] national security, the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security or other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security.

Recently, the CJEU in its judgement *Privacy International* opined that 'the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law'[94] and concluded that in the context of the ePrivacy Directive[95] 'national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that directive'.[96] The position of the CJEU in *Privacy International* allows one to assume that in case the notion of national security in the LED is investigated by the CJEU, the Court may actually allow for the application of the LED in specific circumstances when the processing of personal data takes place for the purpose of safeguarding national security. In this way, it may actually limit the regulatory gap in the protection of personal data, to the extent that the rest of the application requirements of the LED are fulfilled. It is interesting to note that when discussing the specific issue relating to national security, the CJEU avoided any reference to the Charter and relied only on the relationship between Article 4(2) TEU and secondary legislation, in the given case of the ePrivacy Directive. This confirms the reading that in cases of national security the Charter does not apply in accordance with Article 4(2) TEU.[97]

6. AN ALTERNATIVE APPROACH: THE EUDPR MODEL

In 2011, the EDPS argued the processing of personal data carried out by EU institutions, bodies, offices and agencies would be also covered by one legal instrument.[98] He opined that processing on the EU level should be included in the GDPR, with a reminder that:

---

[94] Court of Justice of the European Union, Judgment of 6 October 2020, *Privacy International* (C-623/17) ECLI:EU:C:2020:790, para 44.

[95] European Parliament and the Council of the European Union, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 (31.07.2002).

[96] Court of Justice of the European Union, Judgment of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, para 49.

[97] See also Garstka K, Between security and data protection: searching for a model big data surveillance scheme within the European Union data protection framework, The Human Rights, Big Data and Technology Project, Available at https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2018/11/Garstka-Between-Security-and-Data-Projection-November-2018.pdf (accessed 22 October 2020).

[98] European Data Protection Supervisor, Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – 'A comprehensive approach on personal data protection in the European Union', 14 January 2011, para 45.

> this was the original intention of the former Art 286 EC which mentioned data protection for the first time on the level of the Treaty. Article 286 EC simply stated that legal instruments on the processing of personal data would apply to the institutions as well. More importantly, one legal text avoids the risk of discrepancies between provisions and would be most suitable for data exchange between the EU level and the public and private entities in the Member States.[99]

This proposal was not adopted and Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (EUDPR)[100] was published in 2018. Recital 15 EUDPR is applicable to the processing of personal data by Union institutions, bodies, offices or agencies carrying out activities which fall within the scope of Title V (General provisions on the Union's external action and specific provisions on the common foreign and security policy), Chapter 2 (Specific provisions on the common foreign and security policy) of the TEU. However, the EUDPR excludes from its scope of application processing of personal data by missions referred to in Articles 42(1), 43 and 44 TEU, which implement the common security and defence policy.[101]

The EUDPR is an interesting piece of European legislation as it regulates the protection of natural persons with regard to the processing of personal data by the Union institutions and bodies and rules relating to the free movement of personal data between them or to other recipients established in the Union, and included the processing of personal data in the context of police and judicial cooperation for criminal matters. Chapter IX of the EUDPR is dedicated to the processing of operational data[102] by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 Judicial cooperation in criminal matters) or Chapter 5 (Police cooperation) of Title V (Area of Freedom, Security and Justice) TFEU. There is thus one legal instrument, i.e., the EUDPR, that covers both general data processing and data processing in the context of police and judicial cooperation, which shows that a comprehensive approach that would cover data protection issues regulated both under the GDPR and the LED could be possible. It should nevertheless be reminded that the fully harmonised and uniform protection to aspired by the European legislator via the EUDPR

---

[99] European Data Protection Supervisor, Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – 'A comprehensive approach on personal data protection in the European Union', 14 January 2011, para 45.

[100] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance) [PE/31/2018/REV/1], OJ L 295, 21.11.2018, p. 39–98, Article 2(2).

[101] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance) [PE/31/2018/REV/1], OJ L 295, 21.11.2018, p. 39–98, Article 2(4) and Recital 15 EUDPR.

[102] 'operational personal data' means all personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies (Article 3(2) EUDPR).

is not fully achieved, as Europol[103] and the European Public Prosecutor's Office (EPPO)[104] are left outside the scope of the EUDPR, as well as data processing covered by the Prüm convention.[105] Processing of personal data by Europol is governed by the Europol Regulation,[106] while Eurojust is processing personal data in line with the EUDPR and the Eurojust Regulation.[107] Recital 29 of the Eurojust Regulation clarifies that specific data protection rules in the Eurojust Regulation should be regarded as *lex specialis* to the provisions of the EUDPR. Nevertheless, the EUDPR allows the European Commission to propose the extension of the EUDPR provisions to Europol and the EPPO and ensure a more uniform and consistent legal framework.

The model of the EUDPR could be used as a model for the regulation of data protection in the European Union in one single document, a Regulation replacing the GDPR and the LED. This Regulation could contain a general part with the data protection principles, rights of the data subjects, transfers of personal data, following the model of the EUDPR, specifying concrete provisions on specific issues that relate to the LED, Europol etc. However, it seems that it will be very difficult, if not impossible, to get political consensus at Council level for such an approach. Alternatively, however, the European legislator could consider having next to the GDPR a set of data protection rules that apply to the ASFJ in one legal instrument and are equivalent to the ones established in the GDPR.

7. CONCLUSIONS

The analysis of key provisions of the European treaties carried out in this chapter illustrates the European legislator's limits when regulating issues of processing of personal data. Within the complex legal framework on data protection rules in the TEU and the TFEU, the European legislator chose to adopt both the GDPR and the LED on the basis of Article 16 TFEU. Although Article 16 TFEU aimed at ensuring the uniform application of data protection rules in all areas of EU law, due to the fragmentation of data protection rules, it has not achieved this objective.[108] Article 16(2) TFEU introduced a major novelty in relation to the regulation of data protection: Both the European Parliament and the Council are involved in the law-making procedures relating to the processing of personal data. The European Parliament was thus

---

[103] European Parliament and the Council, Regulation (EU) 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, pp. 53–114.

[104] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (OJ L 283, 31.10.2017, p. 1).

[105] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, pp. 1–11.

[106] European Parliament and the Council, Regulation (EU) 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, pp. 53–114.

[107] European Parliament and the Council, Regulation (EU) 2018/1727 of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, L 295/138 (21.11.2018).

[108] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015), p. 93.

offered the power to put additional pressure on the level of protection on the processing of personal data in activities that used to fall under the third pillar. However, the European Parliament faced fierce resistance by the Council. During the trialogue negotiations, a political compromise was found, as the European Parliament pushed for a 'package approach' ensuring that the GDPR and the LED would be adopted at the same time.[109] Kuner, Bygrave, and Docksey argue that it would have been an easy solution to extend the scope of application of the GDPR to cover law enforcement issues as well, but 'this proved politically impossible'.[110]

A divided system was chosen when it comes to the processing of personal data: the GDPR, as the main legal instrument laying out the rules for data protection, and the LED, for the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. However, this divided system leaves 'grey zones' on the applicable data protection framework, for example when it comes to public-private partnerships. There is great need for clarification of the applicable framework in cases where private and public bodies are collaborating.

The LED not only failed to harmonise the rules for data protection for law enforcement purposes in the various member States, but there have been also delays in the future promises of further harmonisation of data protection provisions in other legal acts that regulate processing by the competent authorities for law enforcement purposes. The upcoming review of the LED is an opportunity for the European legislator to enhance the level of protection offered in the LED in order to bring it closer to the GDPR standards. The LED provides for a grandfathering clause, according to which:

> The specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall remain unaffected.[111]

Article 62(6) LED requires the Commission to review other legal acts adopted by the Union which regulate processing by the competent authorities for law enforcement purposes, including those referred to in Article 60 LED, in order to assess the need to align them with the LED and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data within the scope of the LED.[112] Boehm

---

[109] Mark Leiser and Bart Custers, The Law Enforcement Directive – Conceptual challenges of the EU Directive 2016/680, EDPL [2019] 3, p. 367-368; Gloria Gonzalez Fuster, *The Emergence of Data Protection as a Fundamental Right of the EU*, (Springer Switzerland, 2014), p. 220.

[110] Kuner CH, Bygrave L and Docksey Ch, Background and Evolution of the GDPR in Kuner CH, Bygrave L and Docksey Ch (eds) *The EU General Data Protection Regulation – A Commentary*, (Oxford University Press, 2020), p. 11.

[111] Article 60 LED.

[112] Article 62 (6) LED. The European Commission identified 26 Union legal acts that are relevant for this review, ten of which would require alignment of data protection issues: European Commission, Communication to the European Parliament and the Council on the 'Way forward on aligning the former third pillar acquis with data protection rules', 24.06.2020, COM(2020) 262 final, p.3 and Annex with a list of these instruments; Fondazione Brodolini, Fundamental rights review of EU data collec-

was hopeful that the CJEU, following *Huber v Germany*,[113] would play a prominent role in the establishment of 'a data protection regime which goes beyond the former third pillar structure'.[114] However, the position of the CJEU has been rather conservative in this respect.

The demands of the European Parliament to extend the same level of protection for the processing of personal data to both processing operations falling under the GDPR and under the former third pillar were only partially satisfied with the adoption of the LED. The need for a further harmonisation of the data protection provisions on processing carried out by competent authorities for law enforcement purposes remains important and should be addressed. The model of the EUDPR, which comprises of a set of general provisions and a number of provisions with a more concrete focus, can be seen as a uniform attempt at European level to cover data protection for administrative data and on operational data that mirror the LED. Such an approach could be worthy of exploring in relation to the GDPR and the LED in order to get a more comprehensive and yet not identical set of rules, encompassing data protection provisions that regulate the Europol, the SIS and a number of other legal documents in order to overcome the current fragmentation of the data protection regime.

In reality, although this chapter discusses a divided system, a literal term would talk about multi-partite system and a myriad of fragmented data protection rules. The LED covers only the area of processing of personal data for law enforcement purposes, leaving outside its protective ambit a large spectrum of law enforcement agencies, such as Europol, Eurojust or data protection rules under the Prüm decision, and specific ASFJ exchange systems, such as the SIS (Schengen Information System) or the CIS (Customs Information System). Next to the GDPR, would it be more meaningful to have a set of data protection rules that apply to the whole ASFJ? From the view of consistency and coherence it would undoubtedly make sense to have one legal instrument.[115] Admittedly political consensus among the Member States will be difficult to achieve, given the sensitivity of regulating issues relating to ASFJ. Established exemptions and in particular Declaration 21 to the Treaty of Lisbon shall in any case be respected. The harmonisation of the provisions on the processing of personal data in the ASFJ should get the attention of the European legislator and become a central issue in future reforms of the European data protection legal framework.

---

tion instruments and programmes, 2019, http://www.fondazionebrodolini.it/en/projects/pilot-project-fundamental-rights-review-eu-data-collection-instruments-and-programmes (accessed 15 July 2021).

[113] Judgment of 16 December 2008, *Huber* (C-524/06, ECR 2008 p. I-9705) EU:C:2008:724.

[114] Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice – Towards harmonized data protection principles for information exchange at EU-level*, (Springer Berlin-Heidelberg, 2012), p. 171.

[115] European Data Protection Supervisor, Opinion 6/2015, A further step towards comprehensive EU data protection - EDPS recommendations on the Directive for data protection in the police and justice sectors, 28.10.2015, para. 135.