The Concept Of Joint Control Under The Data Protection Law Enforcement Directive 2016/680 In Contrast To The GDPR

by **Tristan Radtke***

Abstract: While the EU General Data Protection Regulation 2016/679 (hereinafter the GDPR) is on everyone's lips, the EU Data Protection Law Enforcement Directive 2016/680 (hereinafter the LED) exhibits a rather shadowy existence. This also applies with regard to the concept of multiple controllers determining purposes and means of data processing activities (Joint Control). The LED requires the Member States to implement a Joint Control concept similar to the concept set out under the GDPR. Differences between the Joint Control concepts under the GDPR and LED lie in the details, but at the same time they are significant and representative of the specifics and particular aims of the LED compared to the GDPR. The following article discusses the objectives of the LED and the Joint Control concept and explains them on the basis of the differences between the provisions related to Joint Control (Art. 26 GDPR and Art. 21 LED). In addition, collisions of application of GDPR and LED and their impact on Joint Controllers are discussed.

Keywords: Joint Control; Data Protection; GDPR; LED

Recommended citation: Tristan Radtke, The concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in contrast to the GDPR, 11 (2020) JIPITEC 242 para 1.

A. (General) Data Protection Law and the Concept of Joint Control

1 Data protection law intends to contribute to an effective protection of natural persons – the data subjects – in relation to the processing of "their" personal data (cf. Art. 1(2) GDPR and previously Art. 1(1) Data Protection Directive 95/46/EC[1] (hereinafter the DPD)). Thus, data protection law implements the corresponding right and objective enshrined in Art. 8(1) Charter and Art. 16(1) TFEU.[2]

2 Transparency (Art. 5(1)(a) GDPR) on data processing operations, the pursued purposes and the persons having control over the data processing operations is a key element to ensure data subjects are able to exercise their (other) data subject rights laid down in Art. 12 et seqq. GDPR.[3] For example, a data subject who is not aware that personal data are stored incorrectly is practically unable to obtain rectification of such data. In addition, transparency is particularly relevant when it comes to the addressee of any data subject right and claims. Such

* Tristan Radtke is working as Academic Assistant at the Institute for Media and Information Law (Professor Dr. Paal, M.Jur. (Oxford)) at the University of Freiburg and is working on his doctoral thesis with focus on data protection law.

1 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 [1995] OJ L281/31.

2 Recital (1) GDPR.

3 EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 362.

an addressee is generally the controller under the GDPR. It is the natural or legal person determining purposes and means of the processing of personal data (Art. 4(7) GDPR). As it can be assumed such a person is able to control the circumstances of data processing activities and would be able to implement changes, the controller is responsible for compliance with the GDPR (Art. 24(1) GDPR).

3 Already under the DPD the European legislator acknowledged that a natural or legal person may determine the purposes and means "jointly with others" – and gave birth to the concept of Joint Control.[4] For example, the CJEU considered the cooperation of a social network and a fan page provider[5] or social plugin embedder[6] as constellations of Joint Control. Such a broad interpretation[7] of the joint determination attracted the attention of the internet community. However, under the DPD the judgments led "only" to the sharing of the role of controllers by two or more persons in such constellations. Although the Article 29 Working Party has – prior to the judgements – taken the view that a clear allocation of responsibilities is necessary[8] and there might be a joint and several liability in some cases,[9] the provisions of the DPD laid down no such consequences or particular obligations of Joint Controllers explicitly.

4 The GDPR implemented changes in this regard.[10] The GDPR does not only provide for answers in case of liability when multiple controllers and/or processors might be involved (Art. 82(4) GDPR), but stipulates additional consequences of controllers being considered Joint Controllers explicitly in Art. 26 GDPR. It should not be overlooked that Joint Control also offers an opportunity to realize cooperation in a transparent manner and with agreement requirements that are not as strict as in the case of the engagement of a processor under Art. 28(3) GDPR.[11] According to Art. 26(1),(2) GDPR, Joint Controllers shall determine their responsibilities in a transparent manner in an arrangement (hereinafter Joint Control Agreement, abbrev. JCA) and the essence of such a JCA shall be made available to the data subject. Such an obligation is another implementation of the transparency principle (Art. 5(1)(a) GDPR)[12] and necessary for "the protection of the rights and freedoms of the data subjects".[13] However, pursuant to Art. 26(3) GDPR data subjects may exercise their rights in respect of and against each of the data controllers. Therefore, the effectiveness of the exercise of data subjects' rights does not (completely) depend on whether the JCA determines the responsibilities in a transparent manner. The transparency of the JCA still affects data subjects indirectly, e.g., when Joint Controllers are unable to ensure the lawfulness of the data processing activities due to non-transparent and unclear determinations, or when the lack of additional information impairs the success of data subjects' requests.

5 To sum up, Joint Control under the GDPR ensures the protection of data subject rights in several ways and particularly in complex, pluralistically controlled[14] data processing operations.

4 EDPS, 'Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (2019) 22.

5 CJEU, Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388 para 42, 44; discussed by Charlotte Ducuing and Jessica Schroers and Els Kindt, 'The Wirtschaftsakademie Fan Page Decision: A Landmark on Joint Controllership - A Challenge for Supervisory Authorities Competences' (2018) 4 Eur Data Prot L Rev 547.

6 CJEU, Case C-40/17, Fashion ID, ECLI:EU:C:2019:629 para 84; discussed by Louisa Specht-Riemenschneider and Ruben Schneider, 'Stuck Half Way: The Limitation of Joint Control after Fashion ID (C-40/17)' (2020) 69 GRUR Int. 159.

7 René Mahieu and Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World' (2019) 10 JIPITEC 39 para 39.

8 Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) WP 169, 24. A revised (final) version of this Opinion by the EDPB is expected for the next months.

9 Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) WP 169, 22, 24.

10 Emphasized too by Paul de Hert and Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 CLSR 179, 185; Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibility and Liability* (intersentia 2019) para 206.

11 Similar Valentina Colcelli, 'Joint Controller Agreement under GDPR' (2019) 3 ECLIC 1032.

12 Implied by Valentina Colcelli, 'Joint Controller Agreement under GDPR' (2019) 3 ECLIC 1032, 1032 ff.

13 Recital (79) GDPR; previously SEC (2012)72 final, 'Impact Assessment - Annex 1', 18.

14 Joachim Schrey in Daniel Rücker and Tobias Kugler (eds), *New European General Data Protection Regulation* (2018) para 495.

B. Specifics of the LED

6 The LED is the *lex specialis*,[15] the GDPR for the area of law enforcement, i.e., for "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" (Art. 1(1) LED). The EU decided that the processing of personal data under such circumstances does require a substantially different legal concept,[16] as demonstrated by the limited scope of the GDPR (Art. 2(2)(d) GDPR).

7 The LED contributes even more than the repealed Council Framework Decision 2008/977/JHA (hereinafter the Framework Decision)[17] to a harmonized and effective data protection law in the field of police and law enforcement.[18] As diverse legal acts for specific data processing cooperation such as Europol and Eurojust are still in place, the scope of the LED is limited (cf. Art. 60 LED).[19] Nevertheless, as its predecessor – the Framework Decision – with respect to the DPD,[20] the LED adopts quite a lot of provisions from the GDPR. This hardly comes as a surprise as both the GDPR and the LED aim to protect the rights and freedoms of data subjects (Art. 1(2)(a) LED), albeit under different circumstances. Some provisions such as important definitions in Art. 3 LED, (most) data protection principles in Art. 4(1) LED and most data subject rights in Art. 12 et seqq. LED, the concept of data protection by design and by default (Art. 20 LED) as well as provisions on data processors (Art. 22 LED), records of processing activities (Art. 24 LED), data protection impact assessments (Art. 27 LED), and data security measures (Art. 29 et seqq. LED) have been adopted in essence or even almost verbatim. However, as it will be shown with regard to the Joint Control concept below, the different circumstances of data processing activities under the LED required modifications.

8 Such different circumstances referred to are: (i) the legal status of the Directive addressing only the Member States instead of a general application such as with respect to the GDPR (cf. Art. 288 TFEU); (ii) the controllers being usually public authorities, each of the same Member State and its derivatives; and (iii) the different circumstances of data processing activities under the LED allowing transparency requirements which are not as strict as under the GDPR.

I. Directive instead of Regulation

9 Due to its legal act specifics, a Directive takes a different approach than a Regulation.[21] The Directive is addressed to the Member States (Art. 288(3) TFEU) and leaves it up to them – at least in theory – to choose the form and methods to achieve a result. This choice with respect to the LED has been criticized[22] as it may impair the degree of harmonization.[23] This may be not only the case when Member States adopt provisions on the basis of an opening clause in the

15 Teresa Quintel, 'Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive' (2018) 4 Eur Data Prot L Rev 104, 104. However, as the GDPR implements a scope exception in Art. 2(2)(d) GDPR for purposes covered by the LED, there is no true conflict of laws.

16 Paul De Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7 New J Eur Crim L 7, 8.

17 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 [2008] OJ L350/60.

18 Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework' (2017) 33 CLSR 324, 328; cf. SEC (2012)72 final, 'Impact Assessment - Annex 1', 31 ff.

19 Cf. Diana Alonso Blas, 'Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom' (2010) 11 ERA Forum (2010) 233, 238. For the history of the different legal acts see Paul de Hert and Vagelis 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 CLSR 403, 405 and 413.

20 Due to the limited scope of the Framework Decision it has a comparably low impact, Paul De Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7 New J Eur Crim L 7, 7; Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework' (2017) 33 CLSR 324, 325.

21 Stressing this too EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 385; Paul de Hert and Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 CLSR 179, 182.

22 Cf. EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 305.

23 Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework' (2017) 33 CLSR 324, 328 ff.

LED but also when they provide for an even stronger protection in general as allowed pursuant to Art. 1(3) LED.[24]

10 The flexibility of the Member States under the Directive affects the provisions on Joint Control as well as other provisions. For example, Art. 21(2) LED allows the Member States to choose whether the data subject should be able to exercise his or her rights in respect of and against each of the Joint Controllers. In contrast, a similar provision is mandatory under the GDPR. In addition, each Member State may take into account specifics of its LED relevant data processing activities and may provide for additional safeguards for Joint Control constellations, e.g., with respect to information obligations and to align Art. 21 LED with Art. 26 GDPR.

II. Public Authorities as Controllers

11 While under the GDPR any public or non-public body can be considered a controller (Art. 4(7) GDPR), under the LED only competent authorities[25] are controllers (Art. 3(8) LED). Insofar the circumstances are similar to those under the Regulation (EU) 2018/1725[26] stipulating data processing activities carried out by the Union institutions, bodies, offices and agencies. Accordingly, a comparison of the Joint Control concept under the LED and the Regulation might be useful for the interpretation of Art. 21 LED and will therefore be made in the following (see below C.IV., E.).

12 Pursuant to Art. 3(7)(b) LED "any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes" set out in Art. 1(1) LED may be considered a competent authority too.[27] Thus private bodies may be controllers under the LED. However, taking into account the police purposes as classical governmental tasks, the majority of controllers will still be public authorities.

13 In most cases, only the authorities within a Member State will cooperate in data processing activities under the LED as each Member State would like to uphold its national sovereignty in the fields of data processing for police purposes.[28] In such a case, only the authorities of one Member State and its bodies are Joint Controllers. Thus, the data subject is faced with data controllers as liability subjects of equal solvency. Therefore, it is of less importance to the data subject whether he or she can exercise his or her rights in respect of and against each of the Joint Controllers and whether they are each held liable for the entire damage. Nevertheless, (personal) data transfers between Member States or even to third countries could be admissible, as Art. 35 et seqq. as well as Art. 50 LED demonstrate.

14 In addition, each Member State will most likely regulate the processing activities of its authorities – as Art. 8(1) LED with Union or Member State law as only legal base demonstrates[29] and as already required for example by the German constitution.[30] Even possible constellations of Joint Control might be already governed by the respective law. There is less need for an additional transparent agreement if the legislator itself has already regulated the responsibilities in detail and by means of mostly public accessible law.

III. Restriction of Transparency due to specific purposes

15 With respect to (iii), transparency is a leading principle of the GDPR and not of such great importance under the LED.[31] Even when comparing the occurrence of

24 Refer as well to recital (15) LED.

25 Preferring a narrow understanding of this term Plixavra Vogiatzoglou and Stefano Fantin, 'National and public security within and beyond the Police Directive' in Anton Vedder and others (eds), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia 2019) 31 and 48 ff; EDPS, 'Opinion 6/2015 – A further step towards comprehensive EU data protection' (2015) 9.

26 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 [2018] OJ L 295/39.

27 Refer as well to recital (11) LED.

28 Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15' (1987) para 29.

29 In detail Juraj Sajfert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for police and criminal justice authorities' in Mark D Cole and Franziska Boehm (eds), *GDPR Commentary* (Edward Elgar Publishing, forthcoming) 6.

30 Cf. EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 399, 401.

31 Critical EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012)

the words "transparency" and "transparent" in both legal acts, the GDPR prevails with 14 against 2 occurrences. This might be justified because of the specific character of the data processing purposes within the scope of the LED.[32] Consequentially the LED does not explicitly require controllers to process personal data "in a transparent manner in relation to the data subject" (cf. Art. 5(1)(a) GDPR). The principle of "lawfulness, fairness and *transparency*" (Art. 5(1)(a) GDPR) has been narrowed down to a principle of lawfulness and fairness (Art. 4(1)(a) LED).[33] The information to the data subject has to be provided not in a "concise, *transparent*, intelligible and easily accessible form" (Art. 12(1) GDPR) but in a "concise, intelligible and easily accessible form" (Art. 12(1) LED). Therefore, the LED gives the impression that public data processing activities related to criminal offences require less transparency in general. As covert investigations, video surveillance or other forms of covert data processing activities are more likely under the circumstances covered by the LED, this might be an explanation for such an adaption[34] – whether this can be criticized or not.

16 In addition, there are several specific exemptions from the right of access in Art. 15 LED, e.g., to "avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties" (Art. 15(1)(b) LED). However, transparency still has to be taken into account by controllers under the LED.[35]

C. Joint Controllers – Consequences according to Art. 21 LED

17 As under Art. 26 GDPR, important aspects – in particular responsibilities regarding the exercise of data subject rights – related to Joint Control constellations falling within the scope of the LED shall be determined in a Joint Control Agreement (Art. 21 LED). This important legal consequence of Joint Control has been modified in several respects under the LED. Such modifications are representative for the necessary deviations from the GDPR provisions due to the described specifics of the LED such as its material scope.

18 After all, the GDPR concept of Joint Control in essence has been implemented under the LED as well. The Joint Control concept implemented in the LED aims to protect the data subjects too, particularly when it comes to transparency and effective data subject rights. And even under the LED, despite the minor importance of transparency thereafter, a clear "allocation"[36] – respectively "attribution"[37] – of the responsibilities of Joint Controllers is necessary.

I. Legislator first

19 When it comes to responsibilities of Joint Controllers determined by the legislator there are virtually no differences between the GDPR and the LED. To the extent "the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject" there is no need for determining such in an arrangement between the Joint Controllers (Art. 21(1)(2) LED). As described above (see B.II.), the constellations of Joint Control within the scope of the LED will mostly be governed by Union or Member State law when assigning tasks to their authorities and bodies. Therefore, a provision such as Art. 21(1)(2) GDPR is of much higher importance under the LED and there will be fewer Joint Control Agreements compared to constellations to which the GDPR applies.

20 In Germany, for instance, there is a central anti-terrorism file, which is fed by the data transferred by several public authorities and might be considered a Joint Control constellation. However, the legislator probably takes a different view as the respective Act ("Antiterrordateigesetz")does not provide for an explicit allocation of responsibilities within the meaning of Art. 21(1)(2) LED.

para 327.

32 Spring Conference of European Data Protection Authorities, 'Position paper on Law Enforcement & Information Exchange in the EU' (2005) 10.

33 Taking a different view Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework' (2017) 33 CLSR 324, 330.

34 Recital (26)(2) LED. See also EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 364; Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15' (1987) para 44 ff; Paul De Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7 New J Eur Crim L 7, 9; Diana Alonso Blas, 'Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom' (2010) 11 ERA Forum (2010) 233, 243.

35 Recital (26)(1) LED and Article 29 Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (2017) WP 258, 17.

36 Recital (79) GDPR.

37 Recital (54) LED.

II. Lower requirements for content of the arrangement

21 Both the GDPR and the LED stipulate that the Joint Controllers have to determine the responsibilities for compliance with central data protection obligations by means of a Joint Control Agreement. The determination of the responsibilities regarding the exercise of data subject rights, including the information obligation(s), is emphasized as essential for the protection of data subjects. In addition, according to Art. 26(2)(1) GDPR, Joint Controllers shall ensure that the roles and relationships between them are duly reflected. This requires inter alia the description of the parties involved and information on different stages of the processing activity.[38] By requiring Joint Controllers to get an overview of their cooperation, transparency *vis-à-vis* data subjects is not only facilitated by preparing the provision of information to data subjects, but it also encourages Joint Controllers to assess whether the envisaged data processing activities meet essential requirements of data protection law (cf. Art. 24(1) GDPR).

22 Such a requirement regarding the reflection of the roles is completely missing in Art. 21 LED. This can again be explained by the fact that most controllers under the LED are public authorities and the legislator at least reflected the roles in the respective legal act. There is no need to reflect the roles and relationships in a JCA if this is already done by law. In addition, public authorities are particularly sensitive to the assessment of the lawfulness and admissibility of their (data processing) activities, as they are already constitutionally obliged to do so. For example, the German constitution and the principle of the rule of law enshrined therein require the authorities to always act in accordance with the law ("Gesetzmäßigkeit der Verwaltung") and provides for even stricter requirements in the (LED) area of the prosecution of criminal offences. Nevertheless, such an obligation of Joint Controllers would also have been suitable under the LED. There are similar controller obligations in general under the LED, even though controllers might be mostly public controllers (cf. Art. 19(1) LED). Particularly with respect to fundamental rights, which are of crucial relevance for data processing activities within the scope of the LED,[39] such a provision can sensitize public authorities, encourage them to self-control, and may therefore reduce the risk of unclear and non-transparent data processing activities which violate principles of data protection law. Accordingly, the German legislator, for example, requires that the roles and responsibilities shall be reflected in the Joint Control Agreement (Section 63 of the German Federal Data Protection Act ("BDSG")).

III. Mandatory contact point

23 According to Art. 26(1)(3) GDPR, Joint Controllers are free to designate a contact point. Such a designation may avoid the administrative effort necessary to forward data subjects' requests to the other Joint Controllers. At the same time, it may also allow for a request from a data subject being processed more quickly, which is of direct benefit to the data subject.[40] Ultimately, the provision is thus a manifestation of Art. 12(2)(1) GDPR (cf. Art. 12(2) LED), which requires controllers to facilitate the exercise of data subject rights. However, its material impact under the GDPR is limited, since the data subject may exercise his or her rights in respect of and against each of the Joint Controllers (Art. 26(3) GDPR).

24 In contrast, the designation of a contact point under the LED is mandatory pursuant to Art. 21(1)(3) LED – similar to Art. 24(1)(3) of the GDPR Draft of the Council.[41] This allows the data subject to contact a single person with regard to all data subject rights, so that the effective enforcement of data subject rights can be ensured. Due to the specific issue that the data subject is usually confronted with solvent public authorities as Joint Controllers and as a contact point (see above B.II.), this can therefore contribute almost as effectively to the protection of the data subject as the joint and several liability, the implementation of which is at the discretion of the Member States according to Art. 21(2) LED. This background completely changes the role of the contact point: While under the GDPR it is the icing on the cake for the data subjects, under the LED, in the absence of mandatory joint and several liability of the Joint Controllers, it is crucial for the effective protection of the data subjects and their

38 Jürgen Hartung in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung/BDSG* (2nd edn, C.H. Beck 2018) Art. 26 DS-GVO para 22.

39 EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 305 and 366; CJEU, Case C-362/14, Schrems, ECLI:EU:C:2015:650 para 86, 87, 94 et passim; CJEU, joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), ECLI:EU:C:2014:238. In detail on the required balance of interests and rights Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice* (Springer 2012) 19 ff.

40 Similar Valentina Colcelli, 'Joint Controller Agreement under GDPR' (2019) 3 ECLIC 1032, 1039.

41 Council of the European Union, Doc. 9565/15.

rights.[42] Even though, the concept of Joint Control and the requirement for the determination of responsibilities are not redundant. The mandatory contact point cannot contribute to the same extent to the effectiveness of data protection compliance, in particular with respect to data subject rights. Whether there is a contact point or not, the internal allocation of responsibilities by the (Joint) Controllers or the legislator ensures that each (Joint) Controller is aware of its specific obligations. Additionally, the allocation of responsibilities encourages each Joint Controller to implement appropriate measures and procedures necessary for data protection compliance when processing the personal data "of" the data subject within the scope of his responsibility.

25 The importance of the contact point under the LED indicates the necessity of further requirements in connection with the obligation of the Joint Controllers to designate a contact point. It already follows from the concept and aim of a contact point that it must actually be (easily) accessible for the data subject. Therefore, in particular, the data subject must be able to obtain information on whether a contact point exists and how to reach out for such a contact point, otherwise the objective pursued by this contact point will be counteracted. The obligation to designate a contact point thus implies an obligation to provide information on the contact point in accordance with Art. 12, 13 LED. In addition, the contact point must be a body which is also able to enforce the rights of the data subjects as effectively as possible. The designation of a person other than the public authorities involved as (Joint) Controllers is therefore not admissible, cf. Art. 21(1)(4) LED.

26 At this point, the Member States can fill in their regulatory leeway and thus not only ensure clarity, but also provide more details on the function of the contact person. Since a Directive requires the transposition by the Member States anyway, the prohibition of repetition[43] under European law such as for Regulations does not apply. Furthermore, pursuant to Art. 1(3) LED even stricter provisions of the Member States are permissible. Therefore, clarifications in the transposed provisions are all the more permissible. The national legislator should make use of such leeway and should explicitly stipulate the information obligations regarding the contact point. In addition, for example, national law could provide for the admissibility of the designation of an external (public) body as a contact point, provided that it (i) can process requests for data subjects at least as effectively as one of the Joint Controllers, and (ii) is an independent subject of liability, so that the Member State provides higher safeguards in accordance with Art. 1(3) LED with the implementation of an additional liability subject. However, as an example for reducing clarity as national legislator, the German transposition in Section 63 BDSG does not provide explicitly *even* for the requirement of the designation of a contact point in general.

IV. Absence of information obligation

27 In contrast to the GDPR (Art. 26(2)(2) GDPR), there is no obligation to provide data subjects with the essence of the Joint Control Agreement. One explanation might be that the obligation to reflect the respective roles and relationships (Art. 26(2)(1) GDPR) has not been adapted as well (see above C.II.). Therefore, the legislator might have been of the opinion there has been no necessity to implement Art. 26(2) GDPR as a whole. However, even under the GDPR, such essence of the Joint Control Agreement may also include information on the determination regarding the rights of the data subjects under Art. 26(1)(2) GDPR, in turn, adopted under the LED.[44] Therefore, the absence of a provision such as Art. 26(2)(1) GDPR alone cannot explain this.

28 Instead, a possible reason might be the greater relevance of the determination by the legislator as already elaborated (see above C.I.). In such a case, the legal regulation contains the information relevant to the data subject. Incidentally, this is also a manifestation of the lower transparency requirements (see above B.III.). Here, however, what is said about the mandatory designation of a contact point (see above C.III.) becomes particularly relevant. Since under the LED a contact point for data subjects must be designated in any case (Art. 21(1)(3) LED), additional information is of less importance for the exercise of the other data subject rights. Finally, the data subject is faced with a solvent contact point mostly (see above B.II.) against whom he or she can exercise all his or her data subject rights.

29 Insofar as the Member States implement the joint and several liability regarding data subject rights according to Art. 21(2) LED, such as the German legislator, such a national provision becomes more similar to Art. 26 GDPR. Nevertheless, there is no obligation under Art. 21 LED to provide data subjects

42 One might also discuss with respect to Art. 12(2) LED whether there is an obligation of Joint Controllers to forward a data subject request to the competent Joint Controller.

43 CJEU, Case 34/73, Variola, ECLI:EU:C:1973:101 para 9 ff. Cf. recital (8) GDPR.

44 Probably Valentina Colcelli, 'Joint Controller Agreement under GDPR' (2019) 3 ECLIC 1032, 1037; Mario Martini in: Boris P Paal and Daniel A Pauly (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz* (3rd edn, C.H. Beck 2021) Art. 26 DS-GVO para 32.

with the essence of the agreement. Such information is still necessary to enable the data subject to choose the best addressee instead of the contact point in order to exercise the data subject rights as effectively as possible. Thus, it might be possible for the addressed Joint Controller to act on the request more quickly, due to the distribution of tasks. The sense of such a duty to provide information on the responsibilities is therefore not completely eliminated under the LED. This is also confirmed by the Regulation (EU) 2018/1725: Although controllers in the meaning of this Regulation are (Union) public authorities (Art. 3(8) Regulation (EU) 2018/1725), Art. 28(2)(2) Regulation (EU) 2018/1725 obliges Joint Controllers to make the essence of the JCA available to the data subject and Art. 28(3) Regulation (EU) 2018/1725 stipulates a joint and several liability. Therefore, the fact that controllers under the LED are mostly public authorities may not justify such an omission of Art. 26(2)(2) GDPR.

30 Member States can fill in their regulatory leeway in this respect. Insofar as the Directive (EU) 2018/1725 provides as well as the GDPR for a Joint Control information obligation, this does not mean that the reverse conclusion can be drawn that a corresponding provision in the context of the LED would be inadmissible due to Art. 21 LED being conclusive in this regard. Such an information obligation would be an example par excellence for a higher safeguard in the meaning of Art. 1(3) LED. It is therefore once again up to the Member States to provide for an information obligation when transposing the LED and thus ensure more transparency vis-à-vis data subjects. Such a provision could at the same time include the obligation to inform the contact point (see C.III. above) implementing a coherent overall Joint Control concept.

D. Right to compensation

31 Infringements of the GDPR resulting in a person suffering damage give the data subject[45] the right to compensation according to Art. 82 GDPR. While this right to damages is regulated in detail in Art. 82 GDPR, Art. 56 LED leaves the details to the Member States. Thus, the provision on joint and several liability of multiple controllers, such as Joint Controllers, in Art. 82(4) GDPR is not mandatory under the LED. In view of the lower solvency risks with regard to public authorities as potential debtors (see above B.II.), the negative impact on the data subjects under the LED is limited. However, a particular disadvantage could be that, due to non-transparent or even uncommunicated cooperation between the Joint Controllers, the data subject does not know for certain in respect of and against which Joint Controller he or she can exercise his or her right to compensation. Even though, it should be noted that the right to compensation constitutes a right within the meaning of Art. 21(1)(4) LED. Thus, the data subject can also exercise his or her right to compensation in respect of and against the contact point. The wording ("right") does not contradict this, but even supports such an interpretation. Systematically, especially the position of Art. 21 LED outside Chapter III shows that reference is not only made to rights mentioned there but also includes rights such as the right to compensation from Chapter VIII (Art. 56 LED).

E. Collision of the GDPR and LED

32 Considering the differences between the implementation of the Joint Control concept under the GDPR and the LED, it could become particularly challenging if both the GDPR and the – Member State transpositions of the – LED would be applicable to such cooperation.

33 The material scope of the GDPR and the LED are mutually exclusive based on the processing purposes (Art. 2(2)(d) GDPR, Art. 2(1),1(1) LED). As the GDPR covers all data processing purposes except for the purposes covered by the LED, the LED is considered the *lex specialis*.[46] Nevertheless, in some constellations it may not be entirely clear whether the purpose falls within the scope of the LED, as for example in the case of migration and border control and potential criminal offences.[47] However, there is no combined applicability of the Joint Control concepts of the GDPR and LED – i.e. controllers under the GDPR and LED being considered together as Joint Controllers – for two reasons.

34 First, in practical terms, whenever personal data are processed by the competent authorities for the purposes covered by the LED with particular relevance to fundamental rights, the legislator will not want to provide for the right of other (GDPR) bodies to determine purposes and means of such processing activities, especially when personal data

45 Art. 82(1) GDPR just states "any person".

46 Cf. Teresa Quintel, 'Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive' (2018) 4 Eur Data Prot L Rev 104, 104.

47 In detail Juraj Sajfert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for police and criminal justice authorities' in Mark D Cole and Franziska Boehm (eds), *GDPR Commentary* (Edward Elgar Publishing, forthcoming) 3; EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 317.

are or should be transferred to private bodies.[48] This would be in line with the Council of Europe's recommendation that data transfers from the police sector to recipients for non-police purposes should be limited to the absolute minimum necessary.[49] If one thinks for example of a private body providing retained personal data to a competent public authority for the purpose of investigation detection or prosecution of criminal offences,[50] the private body and the public authority do not determine such purpose jointly and are therefore not Joint Controllers.[51]

35 Second, Art. 26(1)(1) GDPR as well as Art. 21(1)(1) LED require "two or more *controllers*" in the meaning of the GDPR and the LED, respectively, as a condition for Joint Control. In contrast, Art. 28(1)(1) Regulation (EU) 2018/1725 stipulates explicitly "controllers other than Union institutions and bodies" and includes therefore controllers, which are not controllers in the sense of the Regulation (EU) 2018/1725. Thus, as long as there is only one GDPR and one LED controller only the relevant act will apply in each case. Provided that there are at the same time two or more (Joint) Controllers under the GDPR or LED for connected data processing activities, the respective Joint Control provisions will apply for the data processing activities covered by the scope of either the GDPR or the LED. It might be theoretically conceivable that the identical processing activity serves a purpose in terms of both the GDPR and the LED. In practice, however, it will be possible to split up such processing activity and separate the processing activities clearly, for example if the personal data already collected under the LED are processed further for statistical purposes in accordance with the GDPR *at a later time*. The (Joint) Control under the LED/GDPR thus ends with the corresponding processing activity such as a transmission – and the (Joint) Control under the GDPR/LED begins with the corresponding subsequent processing activity such as a collection. As such a constellation may happen only when the LED *and GDPR* purposes are pursued for connected data processing activities, the function of the LED as a *lex specialis* with regard to the *LED purposes* does not prevent such a consecutive Joint Control according to two legal acts. Such a constellation may take place when a LED controller works together with a GDPR controller for GDPR purposes and is therefore a GDPR controller when processing the same data. For example, personal data might be processed for purposes within the meaning of Art. 1(1) LED and later as part of different processing activities for internal administrative purposes, such as in cases of theft and lost property,[52] or scientific research purposes and statistical purposes (cf. Art. 9(2) LED).[53] However, this will also take place regularly within one authority and the processing activities will be strictly separated.

36 Therefore, a real collision of both provisions is unlikely. When the same public authority is considered a controller under both the GDPR and LED for related data processing activities and there are two controllers under the GDPR and/or LED, then each provision will apply separately and only to the data processing activities covered by the respective legal act. As there are different processing activities, separated inter alia by the different purposes, such a consecutive application and e.g., two Joint Control Agreements can be handled in practice.

F. Summary

37 The concept of Joint Control has been implemented in both the GDPR and the LED. Due to its legal nature as a Directive, public authorities being data controllers in most cases, and different transparency requirements, the implementation of the Joint Control concept required deviations from the GDPR, e.g., in case of Joint Control and Art. 21 LED. Under the LED, not only will the legislator stipulate Joint Control situations more frequently, but there are also less strict requirements for the JCA and – even

48 For instance, information concerning stolen credit cards, Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15' (1987) para 63. Regarding the necessity of transfers for the LED purposes Diana Alonso Blas, 'Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom' (2010) 11 ERA Forum (2010) 233, 242; Spring Conference of European Data Protection Authorities, 'Position paper on Law Enforcement & Information Exchange in the EU' (2005) 4 and 7. For any data processing activities falling in the scope of the GDPR, in addition compliance with Art. 10 GDPR has to be ensured.

49 Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15' (1987) para 56 ff.

50 Recital (11) LED.

51 Cf. Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) WP 169, 20.

52 Cf. Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15' (1987) para 53.

53 Denis Kelleher and Karen Murray, *EU Data Protection Law* (Bloomsbury 2019) para 21.13. For another example EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 317; and in general recital (19)(4) GDPR. In Germany, for example, one might think of the police crime statistics ("Polizeiliche Kriminalstatistik (PKS)").

though not always comprehensible[54] – information obligations. However, the contact point is gaining in importance under the LED and in this respect an obligation to inform who the contact point is. The Member States should fill in their regulatory leeway to align the Joint Control concept under the LED with the GDPR with respect to transparency. A Joint Control constellation with applicability of both the GDPR and LED to connected data processing activities is conceivable, but the respective provisions need to be assessed separately and the different purposes and separable data processing activities allow for the handling of such a constellation.

54 Cf. EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 441.