Computer Law & Security Review, Volume 28, Issue 6, 2012, Pages 627-633,
http://dx.doi.org/10.1016/j.clsr.2012.09.004

[Page 627]

Data Processing by Police and Criminal Justice Authorities in Europe – The Influence of the Commission's Draft on the national Police Laws and Laws of Criminal Procedure

Matthias Bäcker (University of Mannheim, Germany), ***Gerrit Hornung*** (University of Passau, Germany)[1]

ABSTRACT

The proposal for a fundamental reform of the European data protection law, published by the EU Commission on 25 January 2012 is composed of two elements. Apart from a General Data Protection Regulation, the Commission proposes a second regulatory instrument, namely a Directive with regard to data processing by police and criminal justice authorities that shall supersede the Council Framework Decision 2008/977/JHA. This paper seeks to analyse the draft Directive in the context of the entire reform approach and scrutinizes a number of specific issues in regard to the scope, the requirements of data processing, notification duties and data transfer to third countries.

1. Background

Currently, data protection in the area of security law (i.e. data processing carried out by police and criminal justice authorities under the former "third pillar") is significantly less strictly regulated in Europe than other areas of public administration and of the economic sector. Whilst these areas have long been regulated by the uniform framework of the Data Protection Directive 95/46/EC[2] (hereafter: EDPD), a – partial – consolidation for police and criminal justice authorities was achieved just recently through the Council Framework Decision 2008/977/JHA[3], which, however, only covers cross-border data traffic. The Commission's recent reform proposal recommends major changes in both areas, which in each case concern the substantive provisions as well as the respective regulatory instrument. The scope of the current Directive is covered by the proposal of a "Regulation 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)"[4] (hereafter: GDPR), whilst a "Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the

---

[1] An earlier version of this paper was published in German in the *Zeitschrift für Datenschutz* (ZD) 2012, 147-152. This version is published with its permission. The authors are grateful to Mr Markus Lieberknecht and Mr Ray Migge for their support on the revised version.

[2] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the movement of such data, OJ L 281 23 Nov 1995, 31.

[3] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30 Dec 2008, 60.

[4] European Commission, COM(2012) 11 final, 25 Jan 2012; for a detailed analysis, see G Hornung, "A General Data Protection Regulation For Europe? Light And Shade In The Commission's Draft Of 25 January 2012", (2012) 9:1 SCRIPTed 64, http://script-ed.org/?p=406.

purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the

[Page 628]

movement of such data"[5] (hereafter: DCOCP; Articles cited without further designation refer to the Directive) is meant to supersede the Council Framework Decision. In contrast to the Decision, the DCOCP would for the first time regulate data processing on a purely domestic level.

The overall strategy – now based on Art. 16 TFEU[6] – is clarified in more detail by a comprehensive Communication titled "Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century".[7] A preliminary version of the three texts was leaked in November 2011.[8] Compared to these drafts, the DCOCP expands the criminal justice authorities' competences to process data,[9] in part, by using questionably vague legal terms.[10]

Changing to the instrument of a Directive for the first time enables the European Parliament to participate in the legislative process, whereas the Council Framework Decision was adopted by an (unanimous) vote of the Council. Similarly to the GDPR, the Directive leads to a higher degree of communitarisation. However, the DCOCP – partly expressly, partly implicitly – leaves a significantly larger margin of appreciation to the Member States. Consequently, it does not constitute a full harmonization, at least in some areas.

2. Structure and Content at a Glance

The draft is divided into ten chapters. With the exception of Chapter IX of the GDPR (which deals with data processing in specific situations, in particular relating to journalism, the employment context, scientific research, health purposes and religious associations), the chapters of both instruments correspond with each other. The same applies to a large extent to the normative content.

The general provisions of the DCOCP (Chapter I) describe the scope and the objectives (Art. 1 contains, similarly to the GDPR, two partly conflicting objectives , namely the protection of personal data and fundamental rights on the one hand and the free movement of personal data on the other), determine the scope (Art. 2), and contain definitions (Art. 3). Due to the subject

---

5 European Commission, COM(2012) 10 final, 15 Jan 2012.

6 In regards to changes of primary law due to the Treaty of Lisbon in the area of data protection, see F Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, 2011, p. 116 et seq.; I Spiecker and M Eisenbarth, "Kommt das 'Volkszählungsurteil' nun durch den EuGH? – Der Europäische Datenschutz nach Inkrafttreten des Vertrags von Lissabon" (2011) 60 *JuristenZeitung* 169-177.

7 European Commission, COM(2012) 9 final, 25 Jan 2012.

8 See Statewatch, "Observatory on data protection in the EU" (2011) available at http://www.statewatch.org/eu-dp.htm; on this topic, see G Hornung, "A General Data Protection Regulation for Europe? Light and shade in the Commission's draft of 25 January 2012" (2012) 9:1 SCRIPTed 64 (http://script-ed.org/?p=406), p. 66.

9 E.g. concerning the general principles of Art. 4, the limitation of duties to inform (Art. 23), the expanded grounds for permission of data transfers to third countries (Art. 33 et seq, especially Art. 35, 36), the limitations of powers of supervisory authorities (Art. 46), the limited judicial remedies as well as the deletion of joint operations of supervisory authorities (originally contained in Art. 52 of the draft) and the specific rules on genetic data (Art. 10 of the draft, now in a weakened form contained in Art. 8).

10 E.g. "not excessive" (Art. 4 (c)), "as far as possible" (Art. 5 (1), Art. 6 (1)), "all reasonable steps" (Art. 10 (1)).

matter of the DCOCP (i.e. data processing by criminal justice authorities), some definitions have been adjusted or deleted (in particular Art. 4 (8), 13-17 GDPR). The definition of children is identical to the GDPR but in contrast to the Regulation, the DCOCP does not establish specific restrictions or requirements for the processing of children's data.[11]

Chapter II contains principles for the processing of data, namely general principles (Art. 4), conditions for the lawfulness of processing personal data (Art. 7),[12] restrictions with regard to special categories of sensitive personal data (Art. 8), and measures based on profiling and automated processing (Art. 9, which allows for derogation rules in domestic law if measures to safeguard the data subject's legitimate interests are also adopted; Art. 20 GDPR is far more detailed in that respect). While the aforementioned provisions correspond with those of the GDPR, the PDCOCP introduces two new distinctions, namely one based on different categories of data subjects (Art. 5: suspects, convicts, victims, witnesses, contacts or associated persons, and other persons), and another based on different degrees of "accuracy and reliability" of personal data (Art. 6: "personal data based on facts are distinguished from personal data based on personal assessments", cf. Art. 8 (1) of the current Council Framework Decision). Notably, the DCOCP does not tie any direct legal consequences to the controller's duty to distinguish these categories of data and data subjects; Recital 23 does not address this question either. Since Art. 16 does not refer to the said provisions, a violation does not result in a right to erasure. However, a right to rectification (Art. 15) may result from a data subject being allocated to the wrong category. Besides, the duty to distinguish between both categories may amount to obligations as regards the structures and matters of data processing processes that may be monitored by the supervisory authorities within their powers (Art. 46).

Like the GDPR, Chapter III contains modalities for exercising the rights of the data subject and general duties of the controller (Art. 10, including the obligation that any action taken by the controller following the exercise of such rights shall be free of charge). In particular, Art. 11 establishes a duty to inform the data subject whenever personal data is collected.[13] Art. 12 contains a general right of the data subject to obtain information from the controller (this includes the confirmation whether or not personal data has been processed, the information what specific kind of data is involved and the right to obtain a copy of the data). However, Member States may limit this right to a considerable extent (Art. 13). In this case, the data subject may request the supervisory authority to review the lawfulness of the processing. The Member States then have to establish an in-camera review and, as a minimum requirement, inform the data subject about the results pursuant to Art. 14 (3). Moreover, the draft

[Page 629]

allows for a right to erasure, while in certain cases the data shall be marked instead of erased (Art. 16). Finally, Art. 17 opens up the possibility for the Member States to regulate the rights of the data subject within the framework of their domestic law of criminal procedure if the personal data is contained in a judicial decision or record processed in the course of criminal investigations and proceedings.

Chapter IV deals with the obligations of the controller and the processor. The general obligations (Art. 18) and the regulation regarding data protection by design and by default

---

[11] The only legal consequence is contained in Art. 45 (2) 2nd sentence obliging the supervisory authority to dedicate specific attention to activities addressed specifically to children.

[12] See *Ibid*, p 6 et seq.

[13] See *Ibid*, p 8 et seq.

(Art. 19 which, like Art. 23 GDPD, only reluctantly addresses this important area), joint data processing by several controllers (Art. 20) or by processors on behalf of a controller (Art. 21, 22), documentation (Art. 23) as well as cooperation with the supervisory authority (Art. 25, 26, including prior consultation where certain categories of data or specific risks are involved) essentially correspond with the GDPR concerning objectives and basic content. The keeping of records is regulated separately (Art. 24). Accordingly, the controller shall ensure that "records are kept" of the collection, alteration, consultation, disclosure, combination and erasure of data. The records shall show the purpose, date and time of such operations and, "as far as possible", the identification of the person carrying out the processing; Art. 24 (2) requires that the records shall only be used for certain purposes. Contrarily, the provisions dealing with data security (Art. 27-29; fortunately, the duty to report "data breaches"[14] to the supervisory authority extends to criminal justice authorities) and data protection officers (Art. 30-32) are again based on the GDPR. Some elements are phrased rather openly (taking account of the general character of a Directive), whereas other parts are phrased more straightforward than in the GDPR (e.g. the list of measures contained in Art. 27 (2) which corresponds with Art. 22 of the Council Framework Decision, as well as e.g. the German legal situation).[15] Apparently, at this point the Commission has included provisions in the DCOCP that within the GDPR will be adopted afterwards using its power to adopt delegated acts.[16] The DCOCP neither contains a regulation concerning data protection impact assessments (Art. 33 GDPR; still contained in Art. 31 of the November 2011 draft), nor does it address the use of certification technology (Art. 39 GDPR).

Chapter V contains exhaustive (Art. 33) regulations with regard to the transfer of personal data to third countries and international organisations,[17] which is to be distinguished from data transfers between Member States as well as from or to bodies of the EU. The approach of the DCOCP does not distinguish the latter from transfers between authorities of a single Member State, consequently their permissibility is governed by the general principles of the DCOCP and the provisions of separate legislative acts that remain unaffected by the Directive pursuant to Art. 59.

The detailed regulation of supervisory authorities (Chapter VI) corresponds largely with the GDPR, particularly regarding the complete independence[18] and the right to adequate resources (Art. 40), conditions for the members (Art. 41) and the establishment of the supervisory authority (Art. 42). The duties set forth by Art. 45 are in fact identical to those in Art. 52 GDPR.[19] However, the powers are considerably limited compared to the GDPR (the draft had adopted more content from the GDPR) but still grant the supervisory authorities "effective powers of intervention", including the restriction, erasure or destruction of data and

---

[14] See M Burdon, B Lane and P von Nessen, "Data breach notification law in the EU and Australia – Where to now?" (2012) 28 *Computer Law & Security Review* 296-307; Art. 29 Data Protection Working Party, WP 184: Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments; G Hornung, "Informationen über 'Datenpannen'– Neue Pflichten für datenverarbeitende Unternehmen" (2010) 63 *Neue Juristische Wochenschrift* 1841-1845.

[15] See annex to § 9 of the German Federal Data Protection Act.

[16] Regarding the role of the Commission in the GDPR, see G Hornung, "A General Data Protection Regulation For Europe? Light And Shade In The Commission's Draft Of 25 January 2012", (2012) 9:1 SCRIPTed 64, http://script-ed.org/?p=406, p. 77 et seq.

[17] For more details, see *Ibid*, p. 9 et seq.

[18] See currently Art. 25 (1) of the Council Framework Decision.

[19] Additionally, Art. 45 (1) (c) provides for the review procedure laid down in Art. 14, which does not have an equivalent in the GDPR.

the temporary or definitive ban on processing. This is in accordance with Art. 25 of the Council Framework Decision.

Chapter VII contains rules regarding the mutual assistance of supervisory authorities (Art. 48) and the tasks of the European Data Protection Board (Art. 49, cf. Art. 64 et seq. GDPR). A consistency mechanism as set forth by Art. 57 et seq. GDPR is not included; accordingly, the role of the commission is a much weaker one than under the GDPR. Chapter VIII governs the right to lodge a complaint with a supervisory authority (Art. 50; including a right to bring representative action that is independent from individual complaints), as well as judicial remedies available against the authority (Art. 51, including the obligation to act on a complaint but, contrary to Art. 74 GDPR, without the opportunity to request the supervisory authority of the applicant's own Member State to bring proceedings against the authority of another Member State). Besides, Art. 52 provides for remedies against the competent criminal justice authorities and processors. However, in contrast to Art. 75 (2) 2nd sentence, proceedings cannot be brought against controllers in the data subject's Member State if these controllers reside in a different Member State; this differs from the original draft. Liability and the right to compensation (Art. 54) are essentially equivalent to the GDPR, whereas the penalties applicable to infringements set forth by Art. 55 are largely left to the implementing power of the Member States. For instance, the Member States may determine whether administrative sanctions shall, as laid down in Art. 79 GDPR, be available against public authorities as well.[20]

Chapter IX regulates delegated acts and implementing acts. Those acts are now only possible pursuant Art. 28 (5), whilst the draft had contained far more provisions. The final provisions (Chapter X) repeal the Council Framework Decision, define the relation with previously adopted acts, and set forth a duty of the Commission to evaluate the application of the Directive.

[Page 630]

3. Scope

According to Art. 2 (1), the DCOCP applies to the processing by "competent authorities for the purposes referred to in Art. 1 (1)". While the term "authority" may be ambiguous, processing activities by courts in the fields of crime prevention or prosecution do fall within the scope of the DCOCP. This is clarified expressly by Recital 55, and some provisions refer directly to judicial data processing (e.g. Art. 11 (4) (a), Art. 13 (1) (a) and Art. 17). Hence, national courts are subject to the substantive data protection law and are only exempted from the supervisory authorities' competence by virtue of Art. 44 (2) when acting in their specific judicial capacity.[21]

According to Art. 2 (2), the DCOCP applies only to data processed (at least in part) by automated means or using a filing system. This includes the collection of data using automated investigative methods (e.g. interception of telecommunications, mandatory retention of certain types of data, video surveillance, automatic recognition of number plates, etc.). Moreover, the scope also extends to non-automated measures if the data obtained is intended to be processed by automated means or to be collected in a filing system later on. The term "filing system" is defined by Art. 5 (3). A filing system in that sense does not

---

[20] In the original draft this measure was explicitly available.

[21] European Commission, COM(2012) 10 final, 25 Jan 2012, p 12; see also J Klink, *Datenschutz in der elektronischen Justiz* (Kassel: Kassel University Press, 2010).

require electronic processing. According to Recital 15, it includes files and sets of files if they can be structured according to "specific criteria". Depending on the definition of these "criteria", it might already be sufficient that a file is given a document number and can be classified somehow, for instance, by the type of offence or the name of the individual. In any event, the widespread distribution of electronic processing systems will most likely lead to nearly all data processing carried out by criminal justice authorities falling into the scope of the Directive in the near future. By then at the latest, only purely manual measures such as *stop-and-frisk* searches would be outside the scope, and even these would be covered as soon as the data obtained is stored or matched with available files (for example the list of wanted persons).

The Commission mentions the limited scope of the Council Framework Decision – in particular the exclusion of domestic data processing by criminal justice authorities – as an essential reason for the reform plans.[22] Consequently, Art. 2 (3) (a) excludes only those areas that generally do not fall under the scope of European Union Law, e.g. national security. Neither the relevant Recital 15, nor the DCOCP itself define what exactly is meant by national security. Presumably, it should include not only national defence but also the activities of domestic and foreign intelligence services.

According to Art. 2 (3) (b), the DCOCP does not apply to data processing by Union institutions, bodies, offices and agencies. This seems reasonable in so far as there are good reasons to regulate such processing in a separate set of rules. However, it is difficult to comprehend why the Commission – while making the pretence of creating a "Data Protection Framework for the 21st Century"[23] – has not simultaneously issued a proposal with regard to Union institutions. In particular, the data protection rules concerning Europol have been widely and rightly criticized as inadequate in the past.[24] At least in the medium term it will be necessary to establish uniform rules for national criminal justice authorities on the one hand and Europol and Eurojust on the other hand.

4. Specific Regulatory Areas

4.1. Requirements for Data Processing

The DCOCP itself does not regulate comprehensively which types of data processing shall be permitted on which legal conditions. Rather, it presupposes that such permissions exist in Union Law and in the domestic law of Member States. For domestic rules that allow data processing activities, the DCOCP postulates minimum standards. These standards appear deficient at first glance. In particular this part of the Directive has been considerably weakened in comparison to the draft that was leaked in November 2011. Strict requirements can be attained, however, by interpreting the DCOCP in the light of the fundamental rights granted by the CFR.

Art. 4 and 7 of the November 2011 draft had entailed strict requirements for domestic legislation: The provisions had drawn up detailed standards for domestic rules governing data processing by criminal justice authorities. This was complemented by procedural safeguards for the case of criminal justice authorities accessing data that have not been generated or collected for criminal justice purposes. Finally, the draft had imposed a complete ban on the

---

22 European Commission, COM(2012) 10 final, 25 Jan 2012, p 2.

23 European Commission, COM(2012) 9 final, 25 Jan 2012.

24 See F Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, 2011.

use of data once they have been processed unlawfully. This would have introduced a radical *fruit of the poisonous tree* doctrine into the law on criminal procedure of the Member States.

By contrast, the DCOCP contains only few express requirements for domestic data processing, these additionally being phrased very vaguely. An important requirement however follows from an omission: The consent of the data subject is not listed in Art. 7 as a lawful ground for processing and therefore cannot constitute a legal justification for data processing by criminal justice authorities. The underlying notion that the data subject will never decide autonomously over his or her consent towards a criminal justice authority corresponds with Art. 7 (4) GDPR. This provision rules out the possibility of consent where there is a significant imbalance between the position of the data subject and the controller. The preclusion of consent would be quite relevant in practice. In particular, a criminal justice authority would be barred from asking the data subject whether it is willing to undergo an investigative measure "voluntarily" despite the fact that the legal requirements for that measure are not met ("You do not mind, do you?" situation).

Apart from that, the DCOCP seems to leave the legal grounds for data processing almost entirely to the discretion

[Page 631]

of the Member States. Art. 4 is now limited to postulating general principles relating to data processing,[25] whereas Art. 7 lists the lawful types of processing. Art. 7 (a), which will probably be most relevant in practice, allows the Member States to permit data processing if said processing is necessary to prevent or prosecute criminal offences. There are no further requirements for the exact content of such provisions. One cannot help but suspect that since the first draft became public in November 2011, there must have been intense interventions that sought to prevent effective limits to the informational powers of criminal justice authorities.

The impression that the DCOCP does not define appropriate limits to these powers might be a false one. A more specified evaluation of the limitations imposed by Union law can be made when assessing the content and execution of these limitations in the light of the fundamental right to the protection of personal data enshrined in Art. 8 CFR. According to Art. 51 (1) CFR, Member States are bound by the fundamental rights of the CFR when implementing Union Law.[26] One might argue that Art. 7 (a) only allows Member States to enable their criminal justice authorities to carry out certain processing activities but does not impose a duty to do so. Moreover, the DCOCP expressly contains only very basic standards for the lawful types of processing. The Directive therefore seems to grant to the Member States almost full discretion to determine the powers of their authorities. Nevertheless, however vaguely Art. 7 (a) may be phrased, it does erect binding standards for the provisions of Member State law that deal with the processing of personal data by criminal justice authorities. Member States, therefore, are acting within the scope of Union Law when they enact such provisions. Another argument in favour of applying Art. 8 CFR can be derived from Art. 16 TFEU. This provision, which establishes the competence of the Union to lay down data protection rules, constitutes the legal basis for the DCOCP. Furthermore, it expressly repeats the right to the protection of personal data. This reference supports the assumption that acts that are adopted on that legal basis must be interpreted in the light of this

---

[25] The provision is mostly identical to Art. 6 EDPD, which in turn essentially corresponds to Art. 5 GDPR.

[26] For a broad interpretation of the term "implementation" in Art. 51 (1) CFR see e.g. P Craig ,*The Lisbon Treaty*' (2010) 210-213.

fundamental right. Finally, the available CJEU case law on the scope of the fundamental rights of the Union clearly shows expansive tendencies although it does leave some questions unanswered.[27] In particular, the Court has already implied that the Member States are bound by the fundamental rights of the Union even when making use of a margin of regulatory discretion a Directive grants them.[28]

If Art. 7 (a) is interpreted in the light of Art. 8 CFR, this provision could serve as the starting point for an extensive fundamental rights case law of the CJEU in the field of criminal procedure. In order to specify the scope of Art. 8 CFR, the Court has so far drawn on Art. 8 ECHR and the case law of the ECtHR on that human right.[29] There are few doubts that the CJEU will continue to do so.[30] This approach might prove especially fruitful with regards to the legal questions covered by the DCOCP, notably since the ECtHR has already delivered numerous judgments addressing investigative measures taken by criminal justice authorities.[31]

4.2. Information to the Data Subject in Case of Secret Data Collection

The right of the data subject to be informed about which of his or her data is processed by whom is fundamental to the protection of personal data. Without this knowledge, the data subject is virtually unable to exercise any of his or her other rights. This right is especially important when the data subject is confronted with the actions of criminal justice authorities. Such authorities are typically authorized to collect large amounts of personal data without the participation or knowledge of the data subject. The data subject is therefore essentially depending on the competent authority to inform it actively on secret investigative measures. Otherwise, the data subject usually will have no reason to gather information concerning such measures on his or her own initiative.

Art. 11 obliges the Member States to create a duty to inform about both open and secret collections of data, thus taking into account the legitimate interests of the data subject. The general duty to inform is, however, weakened considerably by Art. 11 (4). According to this provision, the Member States may delay, restrict or omit the notification of the data subject for a vast number of reasons. Moreover, all of the exemption clauses are phrased very broadly. For example, Art. 11 (4) (b) allows to omit the notification in order to "avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties". Notably, the wording does not require that the

---

[27] For more recent examples of "activist" case law see M Cartabia, "Europe and Rights: Taking Dialogue Seriously", *5 European Constitutional Law Review (2009)* 5, 8-15.

[28] Case C-540/03 *Parliament v Council* [2006] ECR I-5769, para 104; see also in the context of a regulation which leaves some discretion to the Member States joined cases C-411/10 and C-493/10 *N.S. and others*, para 64-69. For a detailed discussion see F de Cecco, "Room to Move? Minimum Harmonization and Fundamental Rights" *43 Common Market Law Review (2006)* 9.

[29] Joined cases C-405/00, C-138/01 and C-139/01 *ORF* [2003] ECR I-4989, para 71; case C-275/06 *Promusicae*, para 64; case C-518/07 *Commission v Germany*, para 21; joined cases C-92/09 and C-93/09 *Schecke and Eifert*, para 72.

[30] It seems questionable whether the CJEU is obliged to draw on Art. 8 ECHR in order to interpret Art. 8 CFR by virtue of Art. 52 (3) CFR. For practical purposes, however, this question is largely irrelevant. For a detailed discussion on the scope and the significance of Art. 52 (3) CFR see W Weiß "Human Rights in the EU: Rethinking the Role of the European Convention on Human Rights after Lisbon" *7 European Constitutional Law Review (2011)* 64, 69-75.

[31] See eg cases No 5029/71 *Klass and others v Germany*; No 27798/95 *Amann v Switzerland*; No 44787/98 *P.G. and J.H. v United Kingdom*; No 30562/04 and 30566/04 *Marper v United Kingdom*; No 35623/05 *Uzun v Germany*. For a detailed account of the case law of the ECtHR see S Schiedermair, *Der Schutz des Privaten als internationales Grundrecht* (2011) Habilitation Thesis, University of Mainz, to be published in 2012, Part 3, A VI 5 c and 6 d.

criminal offence in question constitute the reason for the processing. Moreover, it need not even be a criminal offence that the concerned data subject has committed itself or is connected to in any way. On this basis, the duty to notify could

[Page 632]

be virtually meaningless in practice. This is especially true for investigative measures which form part of an ongoing proactive strategy. Investigations in criminal fields such as terrorism or organised crime are often designed to observe and analyse complex criminal structures for a long time. The ultimate goal of such investigations is to break up those structures as thoroughly as possible. In such cases, it will almost always be arguable that a notification might impair the investigation in some way.

The exception reservations to "avoid obstructing official or legal inquiries, investigations or procedures" and to "protect public security" are phrased in an equally open manner. Furthermore, by virtue of Art. 11 (5), the Member States are authorized to determine categories of data processing that may wholly or partly fall under the exemptions of paragraph 4. Therefore, for certain types of data processing or for certain kinds of investigations, a notification of the data subject may be precluded in a general manner, without regard to the circumstances of the particular case.

However, according to Art. 11 (4), any restriction on the duty to notify must be necessary and proportionate. To determine the requirements for such proportionality, the fundamental rights guaranteed by the CFR should be referred to, as shown above. Therefore, Art. 8 CFR limits the power of the Member States to exclude notification. The right to the protection of personal data might be complemented by the right to an effective judicial remedy enshrined in Art. 47 CFR. The latter right applies if it is interpreted so as to entail requirements for the administrative procedure of criminal justice authorities in order to ensure that the data subject has in fact access to an effective remedy.[32]

The fundamental importance of informing the data subject in cases where personal data is collected secretly implies that the exemption clauses of Art. 11 (4) need to be interpreted very narrowly. For instance, it would be disproportionate to exclude the information for a long period of time or permanently only because the data subject may be able to draw any conclusions as to the *modus operandi* or the objectives of the authority. Instead, the data subject's interest to be informed should generally be balanced with the authority's secrecy concerns based on all relevant circumstances of the individual case. Consequently, Art. 11 (5), which authorizes the Member States to exclude the information without any regard to the circumstances of the case at hand, will most likely be given a rather narrow scope.

4.3. Data transfer to third countries

As by now, Art. 13 of the Council Framework Decision only regulates the transfer to third countries if the competent authority of one Member State has received personal data from the authorities of another Member State.[33] In contrast, Art. 33 et seq. apply to every transfer to a third country. This issue is of special importance since, when transferred to a third country, the data is subject to a different – and typically more lenient – regulatory framework and may

---

[32] See in this respect the case law of the *Bundesverfassungsgericht* on the right to an effective remedy as guaranteed by Art. 19 (4) of the German Basic Law: decisions volume 100, p. 313 at 361 and 364; volume 109, p. 279 at 363; volume 118, p. 207; volume 125, p. 260 at 334.

[33] On data transfers between Member States, see F Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, 2011.

eventually prove to be detrimental to the data subject, for example when visiting other countries. Pursuant to Art. 33 (a), the basic requirement for any transfer is that it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Additionally, Art. 33 (b) requires that the conditions for a permission are met, namely an adequacy decision (Art. 34), appropriate safeguards (Art. 35) or other conditions (Art. 36).

Adequacy decisions may be adopted either based on Art. 41 GDPR or – in this case specifically for the area of security law – pursuant to Art. 34 (2)-(4); Art. 34 (5) also allows for the decision that a third country does not provide an adequate level of protection. An adequacy decision may be replaced by the assumption of "appropriate safeguards" within terms of Art. 35 (1) (a) if these have been provided for by a legally binding instrument. In contrast to Art. 42 (2) GDPR,[34] neither these instruments, nor their legal requirements are defined more precisely, therefore their impact remains unclear. It is even sufficient under Art. 35 (2) (b) that the controller or processor has "assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data". This assessment must be documented pursuant to Art. 35 (2) and the documentation must be made available to the supervisory authority. Nevertheless, this does hardly constitute an effective legal safeguard: not only does the provision not require a legally binding instrument, under the current wording it is also sufficient if the safeguards only exist from the ex ante perspective of the involved persons.

Finally, Art. 36 is titled "derogations" but in fact contains provisions concerning all activities of the criminal justice authorities. Art. 36 (d) in fact renders all other provisions of Chapter V that deal with data transfer superfluous. Accordingly, it shall be possible in "individual cases" to transfer personal data to third countries for the purposes of "prevention, investigation, detection or prosecution of criminal offences or the execution of a specific criminal penalty". However, Art. 33 (a) already establishes the exact same requirement, which leads to the situation of Art. 33 (a) and (b) (via Art. 36 (d)) being essentially identical. Consequently, the remaining provisions of the chapter are not only technically superfluous but legally harmful because they pretend to be a safeguard that does not exist in reality. The overall standard of protection even falls short of the current legal situation since Art. 13 (3) (a) (ii) of the Council Framework Decision only grants permission to a data transfer without adequate safeguards provided by the third country due to "legitimate prevailing interests, especially important public interests".

As a result, the DCOCP abstains from establishing real substantive requirements for the assessment of data protection legislation in third countries that receive data transfers from criminal justice authorities. This should be changed by restricting the exemption clauses contained in Art. 36. Art. 35

[Page 633]

should also be phrased more restrictively in order to avoid leaving the protection of the data subject largely to the transferring authority.

---

[34] The provision explicitly refers to binding corporate rules, standard protection clauses and authorized contractual clauses.

5. Prospects: The Future of Fundamental Rights Protection in the Area of Criminal Justice

Viewed as a whole, the Directive brings about several improvements and specifications while leaving a number of questions unanswered, especially concerning the transfer of data. Eventually, the legal requirements which the Directive introduces expressly might prove less important than the effect of the Directive to bring major parts of the domestic criminal procedure law of the Member States within the scope of the fundamental rights of the CFR. Considering previous case law as well as the general tendency of the CJEU to expand the scope of the fundamental rights of the Union, it seems rather likely that the Court will assume a binding effect of those rights within the scope of the Directive. This development could bring about far-reaching substantive and institutional consequences.

The substantive consequences of the Directive would be most significant for the United Kingdom[35] and the Netherlands,[36] whose judiciary generally cannot nullify acts of parliament for breaching fundamental rights. Should the Directive enter into force, the courts of those states would have to set aside any domestic statute that violates the Directive, which would erect strict standards for domestic law precisely because it would have to be interpreted in the light of fundamental rights. In effect, the Directive would oblige the courts to exceed the previous limits of their jurisdiction with respect to one of the most sensitive fields of law from a fundamental rights point of view.[37]

As for the Member States in which acts of parliament may already be nullified by a domestic court if they breach fundamental rights, the consequences of the Directive would be subtler but still significant. This is especially true for those states in which the jurisdiction to declare statutes void is confined to the (constitutional or other) court at the top of the domestic judicial hierarchy.[38] As a result of the Directive, any domestic court would have jurisdiction to set aside criminal procedure law if it does not comply with the fundamental rights provided for by the CFR. Union Law would not even necessarily require that court to refer the matter to the CJEU before it refrains from applying domestic law. Lower courts would never be obliged to do so. Even highest courts would only have to refer the matter by virtue of Art. 267 (3) TFEU if the relevant question has not yet been decided and cannot be answered with certainty.[39]

Taken as a whole, the DCOCP enhances the institutional relevance of the CJEU considerably. Unlike national constitutional courts, the Court would determine the level of fundamental rights protection with respect to data processing by criminal justice authorities for the entire Union. As a result, the importance of national constitutional courts in this highly important

---

35 See s. 4 of the Human Rights Act 1998.

36 See Art. 120 of the Constitution of the Netherlands.

37 Art. 1 (1) of the Protocol on the application of the charter of fundamental rights of the European Union to Poland and to the United Kingdom (C 306 Official Journal of the EU, 31 Dec 2007, 154) does not protect the United Kingdom against the application of the CFR within the scope of the DCOCP. The Protocol does not function as a general opt-out from the Charter and does not principally limit the scope of the fundamental rights guaranteed in it; see joined cases C-411/10 and C-493/10 *N.S. and others,* para 116-122. For a detailed discussion on the significance of the Protocol see C Barnard , "The ‚Opt-Out' for the UK and Poland from the Charter of Fundamental Rights: Triumph of Rhetoric over Reality?" in S Griller/J Ziller (eds), *The Lisbon Treaty* (2008) 257; D Anderson/CC Murphy, "The Charter of Fundamental Rights: History and Prospects in Post-Lisbon Europe", *EUI Working Paper Law 2011/08,* 9-12.

38 See e.g. Art. 100 (1) of the German Basic Law. For a comprehensive comparative analysis of different approaches to constitutional review see http://www.concourts.net/comparison.php.

39 Case 283/81 *CILFIT* [1982] ECR 3415.

field of fundamental rights protection would be significantly reduced. Admittedly, national fundamental rights might remain applicable in so far as the DCOCP leaves a margin of regulatory discretion to the Member States.[40] Nevertheless, should the CJEU protect fundamental rights against measures of criminal justice authorities effectively, the question would eventually come up whether it is reasonable to review domestic criminal procedure law by two different sets of fundamental rights. Moreover, although it seems more than likely that the CJEU will draw on the ECHR and the case law of the ECtHR to flesh out the fundamental rights of the CFR when they are applied to criminal justice authorities, the DCOCP would probably enhance the status of the CJEU in its relationship with the Strasbourg Court, too. Firstly, fundamental rights questions usually would have to be referred to the CJEU by virtue of Art. 267 (3) TFEU before the ECtHR could be addressed. Secondly, unlike the ECtHR, the CJEU possesses *de facto* the power to set aside domestic statutes of the Member States due to the supremacy of Union Law. The Directive could therefore increase the impact of the ECHR and the ECtHR indirectly while at the same time reducing their direct significance.[41]

The DCOCP consequently places the CJEU in the key position for the protection of fundamental rights against data processing by criminal justice authorities. However, whether the EJC does in fact live up to this role will also depend on its confidence to take on the workload that comes with it.

Matthias Bäcker (mbaecker@mail.uni-mannheim.de) is Junior Professor for Public Law at the Department of Law, University of Mannheim, Germany.

Gerrit Hornung (gerrit.hornung@uni-passau.de) is Professor for Public Law, IT Law and Legal Informatics at the Institute of IT-Security and Security Law, University of Passau, Germany.

---

[40] E.g. the *Bundesverfassungsgericht* draws on this criterion to determine the scope of the fundamental rights of the Basic Law when it is asked to rule on the constitutionality of measures by German authorities which are based on EU law, see decisions volume 118, p. 79 at 95 et seq., volume 125, p. 260 at 306 et seq.

[41] For a similar assessment of the potential effects of the CFR in general see S Douglas-Scott "The European Union and Human Rights after the Treaty of Lisbon", *11 Human Rights Law Review (2011)* 645, p. 657 et seq.