REVIEW OF EUROPEAN ADMINISTRATIVE LAW; VOL. 8, NR. 1, 125-151, PARIS LEGAL PUBLISHERS © 2015

# The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?

Antonella Galetta

*Researcher, Vrije Universiteit Brussel*

Paul De Hert*

*Professor, Vrije Universiteit Brussel*

## Abstract

*The right to remedy breaches of data protection is laid down in both Directive 95/46/EC (Art. 22) and the Council of Europe Data Protection Convention no. 108 (Art. 8 (d)). Although data protection violations are remedied mainly at the national level, it is possible to identify a set of procedural rules on how to remedy data protection violations under EU law. Currently, there is a three-layered remedial system in place (composed of access rights, the administrative system and the court system). Worthy of attention are the EU's data protection reforms which will introduce new provisions aimed at 'proceduralising' data protection remedies. This paper investigates how data protection breaches are remedied in the EU and under EU law in light of Directive 95/46/EC and the proposed reforms.*

## 1 Introduction

The right to remedy data protection violations can be exercised in several ways under EU law. The remedial system in place relies, first of all, on individual initiatives taken by citizens who need to exercise their data protection rights by contacting the data controller or processor first. Secondly, violations can be remedied by Data Protection Authorities (DPAs) that assist individuals and enforce data protection law through the exercise of administrative power. Thirdly, every type of national court has the jurisdiction to remedy data protection violations (from civil and commercial courts to criminal courts). Fourthly, remedies for data protection violations can also be awarded by European courts.

This paper investigates what redress there is for data protection violations under EU law. The analysis looks at 'proceduralisation' rules which emerge from the EU data protection legislation and case law, and in particular from

* DOI 10.7590/187479815X14313382198412
The authors thank Vagelis Papakonstantinou for his comments on an early draft of the paper.

the EU data protection reform. As will be shown, although the reform will introduce new provisions on how to remedy data protection violations, there is still room to make the remedial system more effective and more data subject-oriented. After having provided a general overview of EU data protection law and of the remedies established therein,[1] we will examine remedies which are sought before the data controller (or processor) (section 2) and before DPAs (section 3). They represent preliminary steps for remedying data protection violations before national courts (section 4). In section 5 there will be a brief illustration of the remedies for violations relating to police and criminal data and reference will be made to the Schengen remedial system. This analysis will help us elaborate on the effectiveness of data protection remedies. Sections 6-8 will be devoted to the EU data protection reform. Here light will be shed on improvements made by the reform with regard to data protection remedies. In section 9 we will assess those improvements from a critical perspective addressing the question of how the right to remedy data protection violations could be strengthened further under EU data protection law. Lastly, we will draw conclusions in section 10.

It is not possible to map data protection remedies and their procedural norms without considering the EU data protection legal framework. Taking shape from the right to privacy, the right to the protection of personal data emerged with the Council of Europe Convention no. 108[2] and then developed with Directive 95/46/EC.[3] While data protection principles and norms took root in the former first pillar, they also began to be embedded in EU treaties issued from the second and third pillars, though in a piecemeal fashion.[4] As a result, data protection norms in police and criminal matters are scattered over a series of ad-hoc legal instruments such as the Convention implementing the

1 *Infra*.

2 Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data (1981), www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm (last accessed 2 January 2015).

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [*OJ* 1995 L 281/31].

4 P. De Hert & B. De Schutter, 'International transfers of data in the field of JHA: the lessons of Europol, PNR and Swift', in: B. Martenczuk & S. Van Thiel (Eds) *Justice, Liberty, Security: New Challenges for EU External Relations* (Brussels: Brussels University Press 2008), 303-339.

Schengen Agreement[5] and in decisions concerning Europol[6] and Eurojust.[7] A more elaborated set of rules on data protection in police and criminal matters was introduced in 2008 with the Framework Decision 2008/977/JHA.[8] Promoted also by the jurisprudence of European Courts, the right to the protection of personal data is now considered to be a fundamental right of the EU[9] safeguarded by Article 8 of the European Charter of Fundamental Rights (EU Charter)[10] and Article 16 of the Treaty on the Functioning of the EU (TFEU).[11] Hence, norms and procedures on how to remedy data protection violations at the EU level stem from several data protection instruments. In this paper we will focus mainly on the remedial system established by Directive 95/46/EC and refer to some remedies in place in the former third pillar.

Chapter III of Directive 95/46/EC deals with judicial remedies, liability and sanctions against data protection violations. These norms are contained in three very short articles (22-24) meant to regulate this pathological stage in data protection law. Article 22 (remedies) sets forth the right to an effective remedy and imposes on Member States the obligation to provide for this right in national law.[12] Article 23 (liability) entitles persons who have suffered damage to receive compensation for data protection violations. Lastly, Article 24 (sanctions) holds that Member States should adopt 'suitable measures' against data protection violations.[13]

---

5 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [*OJ* L 239, 22.9.2000] 19-62.

6 Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) [*OJ* L 121/37, 15.5.2009] (Europol Decision).

7 Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime [*OJ* L 61/3, 6.3.2002] (Eurojust Decision).

8 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (FDPJ) [*OJ* L 350/60 2008].

9 G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

10 Charter of Fundamental Rights of the European Union [*OJ* C 83, 30.3.2010], 389-403.

11 Consolidated version of the Treaty on the Functioning of the European Union [*OJ* C 326/47, 26.10.2012].

12 Art. 22 of the Directive stipulates that 'without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question'.

13 Similarly, Arts. 19 and 20 of the 2008 Framework Decision safeguard the right to compensation and judicial remedies respectively.

The provisions on remedies under Directive 95/46/EC are very general in content and rather vague in tone. Although they touch upon a fundamental right of data subjects, no detail is provided as to how data protection breaches should be remedied and as to the intensity of the sanctions that should be imposed in such cases. The 'minimalist' approach of the EU legislator is partly justified by the fact that Directive 95/46/EC was established mainly to remove barriers to the development of the internal market, not to sanction data protection violations.[14] Moreover, a cautious approach of the European legislator is apparent in regulating a sector which issued partly from the third pillar within the pre-Lisbon EU legal framework.[15] Lastly, and on a more general level, procedural rules have always been considered as belonging to the competence of Member States rather than the EU, although the relevant field of substantive law fell under the former first pillar.[16]

As observed above, data protection remedies can be exercised in different ways under EU law. Three main possibilities are envisaged, as follows:

1. data protection remedies sought before the data controller (or processor): access rights (layer 1); [17]
2. data protection remedies sought before DPAs (layer 2);
3. data protection remedies sought before national courts (layer 3).[18]

---

14 R. Jay, *Data protection: law and practice* (Sweet & Maxwell 2007).

15 R. Schütze, *European constitutional law* (Cambridge University Press 2012).

16 See the contribution of O. Dubos within this publication.

17 It is important to stress that the right of access to personal data is not the only right the data subject can claim in order to challenge a (supposed) data protection violation perpetrated by the data controller. The data subject can seek also the right of rectification, cancellation (or erasure) and opposition (or blocking) (see Art. 12(b) of Directive 95/46/EC). Moreover, data subjects' rights are complemented by the right to object (Art. 14 of Directive 95/46/EC). Access holds a leading position within data subjects' rights as data subjects need to know which data about them is processed by the data controller before claiming rectification, cancellation or opposition. Nevertheless, the procedural rules which relate to the exercise of access rights also apply to rectification, cancellation and opposition.

18 In addition, data protection violations can also be remedied before administrative authorities (i.e. ombudsman and Working Party 29). In many EU Member States ombudsman institutions were replaced by DPAs. See EU Agency for Fundamental Rights (FRA), *Data protection in the European Union: The role of national Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II* (European Union Agency for Fundamental Rights 2010). Moreover, specific arrangements on how to settle data protection disputes can be laid down in codes of conduct agreed upon by professional organisations or other organisations at national level (i.e. bodies representing categories of controllers and trade unions). Those norms (as well as codes of conduct in their entirety) need to be submitted to the scrutiny of the national DPA (see Art. 27(2) of Directive 95/46/EC). The Dutch Data Protection Act for instance establishes that where a code of conduct provides for the arrangement of disputes about its observance, the national DPA should make sure that guarantees of independence are provided and may issue a declaration to this end (Art. 25(1)).

Given this articulated framework, it is very likely that data subjects may somehow become lost in the process of claiming data protection violations. Complaints and cases can be handled from different organisations and persons, ranging from administrative bodies to courts, while shifting from the domain of administrative and civil law to criminal law. Moreover, further complication is given by the fact that one or more of these channels can be activated by the data subject as they are not mutually exclusive.

The EU data protection framework is currently undergoing a reform process which will lead to the General Data Protection Regulation (GDPR)[19] and General Data Protection Directive (GDPD).[20] Following the European Parliament's vote on the reform in March 2014, the new framework awaits the final vote under the co-decision procedure.[21] Apart from establishing new rights for the data subject[22] and new obligations for the data controller,[23] the reform will introduce new procedural rules on how to remedy data protection breaches under EU law. This represents the first attempt of the EU legislator to 'proceduralise' norms of this kind and to set common rules for court proceedings. Moreover, the GDPR sets the bar even higher by harmonising administrative sanctions for data protection breaches (Article 79 GDPR). The new data protection remedial system is analysed in sections 6-8.

---

19 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft, Brussels, 25 January 2012.

20 European Commission, 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, investigations, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (General Data Protection Directive), COM(2012) 10 final, Brussels, 25 January 2012.

21 Discussions on the EU data protection reform are currently being held within the Council of the European Union with a few to reach an agreement with the European Parliament on every single aspect which composes the reform. As the Latvian Minister for Justice and President of the Council (Mr Dzintars Rasnačs) has recently stated, 'Data protection is like a rough diamond being polished and finally starting to shine and hopefully in June it will reach its full potential'. See the Council's press release 'Data protection: Council agrees on general principles and the 'one stop shop' mechanism', available at: www.consilium.europa.eu/en/press/press-releases/2015/03/13-data-protection-council-agrees-general-principles-and-one-stop-shop-mechanism/ (last accessed 17 March 2015).

22 Such as the right to be forgotten (Art. 17 GDPR).

23 Such as the obligation to appoint Data Protection Officers (DPOs) (Arts. 35-37 GDPR and Arts. 30-32 GDPD).

## 2 Data Protection Remedies Sought Before the Data Controller: Access Rights (Layer 1)

The first mechanism foreseen in EU data protection law to remedy data protection violations consists in the exercise of access rights and other related subjective rights.[24] By exercising access rights the data subject can assess whether or not a violation occurred (or is occurring): that is, whether or not an unlawful and/or illegitimate data processing took place. The right of access to personal data is one of the main data subjects' rights. It is safeguarded by Article 8.2 of the EU Charter, as well as by Article 12 of Directive 95/46/EC which elaborates on the content of this right as follows:

1. right to obtain confirmation as to whether or not data subjects' rights are being processed and information as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed;
2. right to obtain communication of the data undergoing processing;
3. right to know the logic involved in any automatic processing of personal data.

In order to introduce a complaint or to submit an access request the data subject needs to locate the data controller (or processor) first. Second, he needs to determine the procedure that should be followed for this purpose, in accordance with national law. In particular, the data subject needs to be able to do the following:

– identify the data controller who is legally responsible for processing the data;
– identify where a request should be submitted (if there is a specific department/officer to whom to address access requests);
– determine how to submit a subject access request (orally, in writing, online, via post, etc.);
– determine if the data controller in question processes requests in a particular way (via access rights forms or templates);
– determine the cost of making such a request (if applicable);

---

24 For a comparison of the subjective rights provided by data protection law and by non-discrimination law, their different nature and the essentially empowering role of data protection rights, see R. Gellert, K. De Vries, P. De Hert & S. Gutwirth, 'A Comparative Analysis of Anti-Discrimination and Data Protection Legislations', in: B. Custers, T. Calders, B. Schermer B. & T. Zarsky (Eds), *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases* (Berlin-Heidelberg, Springer-Verlag 2013) (61-90), 70-71.

– find out if there are time limit obligations on either the requester or the data controller.[25]

If data subjects go through this checklist to determine how to access data across Europe, significant variations will emerge. In general, access rights requests are introduced in writing to data controllers (such as in Belgium, Hungary and the United Kingdom), but this is not always the case. In some Member States an access request can also be made orally, subject to the agreement of the data controller (such as in Austria),[26] or upon agreement of the data controller and data subject (such as in Norway).[27] Generally speaking, the exercise of access is free of charge for the data subject (such as in Belgium, Germany and Spain). However, in some Member States access is not free (such as in the UK)[28] or is free so long as no more than one request is submitted to the same data controller within a year (such as in Austria).[29] Once an access request is made, it should normally be handled within a certain time frame. Significant variations in this respect arise at national level. Time lapses range from 15 days (such as in Italy),[30] to 30 days (such as in Norway and Spain),[31] 40 days (in the UK)[32] 45 days (in Belgium),[33] and 56 days (in Austria).[34] Last but not least, it is important to note that in some Member States data subjects cannot have access to certain categories of personal data directly, but only indirectly, addressing the national DPA in lieu of the data controller (or processor) (see section 5).

The link between the right to a remedy for data protection violations and the right of access to personal data is not only made for practical convenience. Instead, as European courts confirm, it is necessary to keep these two rights together. In the Case *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* the CJEU stressed that the right of access of data subjects to information about them held by data controllers is necessary to enable them to exercise the right to remedy data protection violations.[35] This idea can also be found in the case law of the ECrtHR on Article 13 of the European Convention

25 C. Norris, P. De Hert, X. L'Hoiry & A. Galetta (Eds), *The unaccountable state of surveillance. Exercising access rights in Europe* (Springer 2015) (forthcoming).
26 This possibility is contemplated in Art. 26 of the Austrian Data Protection Act.
27 Sections 17 and 24 of the Norwegian Personal Data Act.
28 Section 7 of the UK Data Protection Act.
29 Article 26 (6) of the Austrian Data Protection Act.
30 Article 146.2, Data Protection Code, 2003. Paragraph 3 of this Article sets a longer timeframe in case the data subject's request is 'especially complex', namely 30 days from its receipt.
31 Article 16, Personal Data Act and Article 15, Personal Data Protection Act, 1999, respectively.
32 Section 7 (10), Data Protection Act, 1998.
33 Article 10, Privacy Act, 1992.
34 Article 26 (4), Data Protection Act, 2000.
35 Case C-553/07 *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* [2009] ECR I-3889, para. 52.

on Human Rights (ECHR). In *Klass and Others v. Germany* the Court pointed out that a person cannot allege that a violation has occurred unless he is first able to lodge a complaint to that effect with the concerned authority.[36] In this circumstance the right to remedy a violation is given in order to both have his claim decided and, if appropriate, to obtain redress.[37] Thus, although at first sight the right to remedy data protection violations and the right of access to personal data seem not to have much in common, the latter represents the first step towards the enforcement of data protection.

## 3 Data Protection Remedies Sought Before DPAs (Layer 2)

Like the EU anti-discrimination framework, the EU data protection framework relies heavily upon the existence of supervisory bodies: Equality bodies for the former, Data Protection Authorities (DPAs) for the latter.[38] In all Member States it is possible to submit a claim before DPAs (as it is also possible to initiate a criminal or other proceeding before national courts, see below).[39] The data subject can introduce a complaint to a national DPA if the data controller (or processor) does not provide any feedback to an access request, if the reply provided does not satisfy the data subject, or if the alleged violation persists. Alternatively, he/she can initiate judicial proceedings (see section 4). Article 28 of Directive 95/46/EC establishes norms on the role and powers of DPAs. DPAs have the duty to 'hear claims lodged by any person, or by an association representing that person' concerning the protection of personal data. Moreover, they can initiate judicial proceedings and bring violations to the attention of judicial authorities *ex officio* (see Art. 28 (3)).[40] In order to remedy a data protection violation before a DPA the data subject should locate the DPA first and then look for specific information as to how to submit a complaint. Hence, he needs to undertake the six actions described earlier in section 2 in the case of requests to data controllers (or processors). Once the DPA receives the complaint, the data subject is notified about this. From that moment on the DPA mediates between the data controller and the data subject making sure that the data controller provides the data subject with the required

36 *Klass and Others v. Germany* (App. 5029/71), ECrtHR, judgment of 6 September 1978, para. 64.
37 *Ibid.*
38 R. Gellert, K. De Vries, P. De Hert & S. Gutwirth, 68-70, op. cit.
39 EU Agency for Fundamental Rights (FRA), *Data protection in the European Union: The role of national Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*, op. cit., 31-33.
40 However, this case is not dealt with in this paper.

information and/or puts an end to a certain data protection violation (if any). In general, Member States' legislation does not set any time limit within which the national DPA has to process the data subject's complaint. Similarly, there is no legal obligation in this regard descending from Directive 95/46/EC. However, as will be illustrated in section 7, the data protection reform will set a time limit to achieve this end.

Although it may sound quite unusual that authorities other than judicial institutions are entitled to remedy violations on legal grounds, this remedial system is very practical because citizens need swift support to counter data protection violations. DPAs come to the aid of data subjects and this allows them to remedy data protection violations in a timely manner and for free. Similarly, the precious support offered by DPAs allows data subjects to have access to an effective remedy, in compliance with Article 13 ECHR, and so to keep the yardstick represented by this article high. This is confirmed by the European jurisprudence which has given quite a broad interpretation of the right to an effective remedy (Article 13 ECHR) in privacy and data protection matters. In *Silver and Others v. the UK*[41] and *Leander v. Sweden*[42] the ECrtHR elaborated on the right to an effective remedy as follows:

*a*. the right to an effective remedy entitles individuals to have both a claim decided and, if appropriate, to obtain redress (see also the *Klass* case);
*b*. the authority referred to in Article 13 'need not be a judicial authority but, if it is not, the powers and the guarantees which it affords are relevant in determining whether the remedy before it is effective';
*c*. the right to an effective remedy can be satisfied not only through a single remedy but also the 'aggregate of remedies provided for under domestic law may do so'.[43]

Under the case law of the ECrtHR principle (b) represents the normative tool through which data protection violations are enforced by authorities which are not necessarily judicial, such as DPAs. According to the Court, regardless of their identity, these authorities should have powers and guarantees relevant enough to make the remedy effective. The need to ensure effective remedies emerges also from the EU primary and secondary data protection law. As stated in Article 8(3) of the EU Charter and Article 16(2) TFEU, data protection viola-

41 *Silver and Others v. the United Kingdom* (App. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75) ECrtHR, judgment of 25 March 1983, para. 113.
42 *Leander v. Sweden* (App. 9248/81), ECrtHR, judgment of 26 March 1987, para. 77.
43 At point (d) the Court also noted that Art. 13 does not guarantee 'a remedy allowing a Contracting State's laws as such to be challenged before a national authority on the ground of being contrary to the Convention or equivalent domestic norms'.

tions are subject to control by an independent authority. Article 28(1) of Directive 95/46/EC states that DPAs 'act with complete independence in exercising the functions entrusted to them'.

European courts have often pronounced themselves on the independence of DPAs. In 2010 the CJEU was asked to interpret the words 'complete independence' in Article 28(1) of Directive 95/46/EC in the Case *Commission v. Germany*.[44] Embracing a broad interpretation of Article 28(1) of the Directive, the CJEU pointed out that

'when carrying out their duties, the supervisory authorities must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence of the State or the *Länder*'.[45]

Moreover, the Court stated that the requirement of independence precludes any external influence which could call into question the performance by DPAs of their tasks and competences descending from the Directive.[46] Similarly, in the Case *European Commission v. Austria* the CJEU argued that the Austrian legislation precluded the Austrian DPA from exercising its functions with complete independence.[47] In particular, the Court found that the Austrian legislation failed to transpose the requirement of 'complete independence' of Article 28(1) because the Austrian DPA was integrated with and subject to supervision of the Federal Chancellery. Moreover, the Federal Chancellery had the right to be informed at all times of all aspects of the work of the DPA, it supervised its work and supplied its workforce, which was not compatible with the duty of complete independence.[48] More recently, the CJEU argued that in order for the complete independence of DPAs to be safeguarded Member States have the obligation to allow DPAs to serve their full term of office (*European Commission v. Hungary*).[49] In this latter case the Court concluded that Hungary failed to fulfil its obligations under Directive 95/46/EC 'by prematurely bringing to an end the term served by the supervisory authority for the protection of personal data'.[50]

According to well-established case law of the ECrtHR the existence of a neutral, independent and impartial authority is an important parameter against

44 Case C-518/07 *European Commission v. Federal Republic of Germany* [2010] ECR I-1885.
45 *Ibid.*, para. 25.
46 *Ibid.*, para. 30.
47 Case C-614/10 *European Commission v. Republic of Austria* [2012] ECR nyr para. 66.
48 *Ibid.*, para. 55 et ss.
49 Case C-288/12 *European Commission v. Hungary* [2014] ECR nyr para. 60.
50 *Ibid.*, para. 62.

which the proportionality of data protection violations should be assessed. In *Leander* for instance the Court found that the refusal to grant access to personal data to the applicant did not constitute an illegitimate interference because the decision about disclosure was taken by a specific Parliamentary Board. Its composition and functions provided adequate guarantees of neutrality, independence and impartiality.[51] Similar conclusions were drawn in the Case *Odièvre v. France*.[52] On the contrary, in *Gaskin* v. *the UK* the ECrtHR stated that as there was no independent authority established at national level, the concerned interference was not proportionate.[53] Similar findings were reached in the Case *M.G. v. UK*[54] where the Court pointed out that the decision about denial of access had not been taken by an independent authority and did not give the applicant the possibility to challenge that decision.[55]

Although the principles of neutrality, independency and impartiality of DPAs belong to data protection law, they mostly characterise the judiciary. In fact, the right to have access to a neutral, independent and impartial authority is guaranteed by Article 6(1) ECHR in the framework of civil and criminal proceedings, as corollary to the right to a fair trial. It is important to stress that these principles have a broader application in data protection law than in other bodies of law, as they apply in all steps which characterise data protection enforcement. Moreover, according to data protection law, a system of neutral, independent and impartial DPAs should be the necessary and sufficient condition to ensure effective remedies to data protection violations, regardless of whether or not the case will end up before a judicial authority.

## 4 Data Protection Remedies Sought Before National Courts (Layer 3)

As explained at section 3, instead of addressing a complaint to a national DPA, the data subject can also initiate judicial proceedings before national courts. Moreover, access to judicial review is guaranteed also after having sought a remedy from the national DPA as these two remedies are not mutually exclusive. Currently, Member States have a wide discretion in establishing and shaping the court system for data protection conflicts. The data

51 Each of the members of the board had a right of veto. Furthermore, a Parliamentary Committee on Justice scrutinized the decisions of the Board and the Parliamentary Ombudsman supervised its activity. ECrtHR, *Leander v. Sweden*, paras 65-66.

52 *Odièvre v. France* (App. 42326/98), ECrtHR, judgment of 13 February 2003.

53 *Gaskin v. the United Kingdom* (App. 10454/83), ECrtHR, judgment of 7 July 1989, para. 49.

54 *M.G. v. the United Kingdom* (App. 39393/98), ECrtHR, judgment of 24/12/2002.

55 *Ibid*., para. 30.

subject may end up starting civil, administrative or criminal proceedings according to national data protection law and procedures established therein. Similarly, the liability and sanctions regime will depend on the specific norms in place at national level. Substantial differences emerge by a comparison of data protection remedies sought before national courts across the EU.[56] Article 24 of Directive 95/46/EC (on 'Sanctions') provides that

'[t]he member states shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive'.

These provisions thus leave the choice of the enforcement regime to the Member States, including the establishment of appropriate sanctions and remedies via criminal law provisions. 'Suitability' seems to be the only requirement.[57]

In the following we compare the remedial system established in Belgium and Italy.[58] Although in Italy remedies before the national DPA (Garante) and judicial remedies are both actionable (see Article 145 of the Italian Data Protection Code (DPC)),[59] the remedial system is mainly based on administrative proceedings. Article 149 DPC sets out a detailed procedure for data protection remedies before the Garante.[60] Civil law proceedings are equally foreseen. They

---

56 A comparative description of enforcement mechanisms and procedures established at national level can be found in the DLA Piper Handbook *Data Protection Laws of the World*, available online at: dlapiperdataprotection.com/#handbook/ (last accessed 30 January 2015).

57 Similarly, as the ECrtHR stressed in *James and Others v. the UK*, Art. 13 ECHR 'guarantees the availability within the national legal order of an effective remedy to enforce the Convention rights and freedoms in whatever form they may happen to be secured'. *James and Others v. the United Kingdom* (App. 8793/79), judgment of 21 February 1986, para. 84.

58 In this section we focus on data protection remedies in Belgium and Italy in order to provide an overview of what these differences could be. Of course, a broader and more detailed analysis of such differences at European level should be extended to all 28 Member States.

59 Data Protection Code, Legislative Decree No 196/2003, available at: www.garanteprivacy.it/home_en/italian-legislation (last accessed 30 January 2015).

60 Once the complaint is submitted to the Garante, communication is provided to the data controller within three days. The data controller, data subject and possibly the data processor have the right of being heard before the Garante and of submitting pleadings or documents. In the course of the proceeding the Garante may request one or more expert assessments (Art. 149 DPC). The Garante may provisionally order either the partial or total blocking of some of the data, or the immediate termination of one or more processing operations. Hence, if the complaint is found to be grounded, the Garante issues a reasoned decision ordering the data controller to abstain from the unlawful conduct. The decision specifies how the data controller should enforce the data subject's rights and sets a deadline in this respect. If the Garante does not issue any decision within 60 days from the moment in which the complaint was lodged, the complaint should be considered as dismissed (Art. 150 DPC). If the concerned complaint is particularly complex or upon agreement of the parties this term may be extended of 40 additional days, at a maximum (Art. 149.7 DPC).

follow the rules of employment law proceedings and procedures are simplified.[61] In particular, proceeding against the decision of the Garante should be initiated within 30 days,[62] otherwise they are rejected; the proceedings are dismissed if the claimant fails to appear at the first hearing; and the court's ruling is not appealable.[63] Because of the lengthy and costly proceedings before national courts, proceedings before the Garante are preferred in Italy.[64] Administrative sanctions can be ordered by the Garante and they consist of the payment of administrative fines (Articles 161 and 162 DPC). Criminal sanctions can be imposed but only in specific cases which mainly concern the processing of judicial and sensitive data and cases in which the data controller does not comply with legal provisions of the DPC or with orders given by the Garante (Articles 167-168 DPC).

A different remedial regime is in place in Belgium, where proceedings under the Belgian Data Protection Act (BDPA)[65] have mainly a civil and criminal nature. Although Article 13 BDPA states that data protection remedies can be sought before the Belgian DPA (Privacy Commission), this DPA has no formal administrative powers and cannot impose sanctions but can only mediate between the data controller and data subject in case a complaint arises (see Article 31 BDPA). Article 14 BDPA establishes specific norms for remedying data protection violations before national courts, which consist in summary proceedings. The President of the Court of First instance, having heard the parties, handles the complaint and then issues an order which is immediately enforceable notwithstanding appeal or opposition (Article 14(2) BDPA).[66] The judicial proceedings established by the BDPA puts significant emphasis on the evidence that is or may be produced by the parties. The President of the Court may take measures to prevent the concealment or disappearance of evidence (Article 14(7) BDPA). Moreover, it is noteworthy that the burden of proof is reversed for damages deriving from violations of the provisions of the BDPA. In this case the data controller needs to provide evidence that the damage cannot be ascribed to him in order to be exempted from liability (Article 15 bis BDPA). A detailed set of criminal sanctions is laid down at Articles 37-43 BDPA which

61 These norms are established by Art. 10 of Legislative Decree No 150/2011.
62 Within 60 days if the claimant lives abroad (see Art. 10.3 Legislative Decree No 150/2011).
63 However, a remedy before the Court of Cassation can be sought anyway (Art. 10.6 Legislative Decree No 150/2011).
64 EU Agency for Fundamental Rights (FRA), *Access to data protection remedies in EU Member States* (2013: European Union Agency for Fundamental Rights), 38-40.
65 Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, *Belgian Official Journal* 18 March 1993.
66 In the course of the proceedings the President of the Court can order the data controller to inform third parties of the rectification or erasure of personal data in case it is incorrect, incomplete or irrelevant data were transferred to them (Art. 14.6 BDPA).

include fines as well as imprisonment of up to two years. Both swift procedures and the reversal of the burden of proof represent legal guarantees to remedy data protection violations in a timely and concrete way.[67] The importance of guarantees of this kind should not be underestimated. Benefiting from the reversed burden of proof, the data subject does not need to prove the liability of the data controller for the detrimental effects resulting from the concerned violation.[68]

These two country discussions allow us to make some observations about data protection remedies under national legislation across Europe. *Firstly*, very much like EU equality and non-discrimination law,[69] we find in most EU states a mixture of remedies provided by civil, administrative or criminal law. In 2013, the European Union Agency for Fundamental Rights (FRA) found with regard to data protection that 'in almost all member states criminal sanctions can be imposed, in the form of a fine or imprisonment'.[70] Considering that Directive 95/46/EC left the choice of the enforcement regime to the discretion of the Member States, the use of criminal sanctions varies from one country to another. Whereas some states (like the UK and the Netherlands) only criminalised some data protection wrongs and mainly used civil law or administrative sanctions, others opted for an extensive set of data protection crimes. Some countries (like Belgium) have exclusively opted for criminal law enforcement.[71] This explains why in Italy the remedial system relies mainly on administrative sanctions,

---

67 Guarantees of this kind are also in place in other Member States such as Greece where access to courts is made easier for data protection violations according to a special procedure provided for in Articles 664-676 of the Greek Civil Procedure Code.

68 In the context of data protection in police and criminal matters this implies that the data controller (or processor) needs to prove that the negative consequences of certain profiling practices for instance should not be ascribed to him, whereas the data subject can address the police directly without producing any evidence.

69 R. Iordache & I. Ionescu, 'Discrimination and its sanctions – Symbolic vs. effective remedies in European anti-discrimination law' [2014/19] *European Anti-discrimination Law Review* 11-24.

70 EU Agency for Fundamental Rights (FRA), *Access to data protection remedies in EU member states*, op. cit., 1-64, 7. The FRA added that '[s]anctions that data protection authorities are empowered to impose differ between member states. [...] The duration of a sentence and the amount of a fine also vary across member states' (*Ibid.*, 7).

71 If a country opts for criminal law sanctions, these are almost always to be found in the respective data protection acts, with the exception of France. A 1992 French law moved the sanctions of the 1978 general data protection law to the criminal code, more particularly to a section on 'Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques'. For instance, Article 226-18 of the criminal code provides that 'Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende'. See Code pénal, via www.legifrance.gouv.fr/initRechCodeArticle.do. The change seemed logical at the time, since the French data protection act was mainly based on a criminal law approach with only some provisions dealing with administrative sanctions. Comp. C. Bernier, 'Overview and definition of personal data offences: impact of criminal aspects', Association Française de Droit de l'Informatique et de la Télécommunication, 25 February 2013.

while the criminal path seems to be favoured in Belgium with its abundance of criminal sanctions. This also explains why most, but not all Member States, have chosen to mandate their DPAs to sanction data protection violations with administrative fines. Again, there is a striking analogy with the current non-discrimination law landscape in the EU.[72]

Both administrative and criminal sanctions have the punitive character of denoting the likelihood that data protection violations not only affect the data subject but also the general public, and hence the 'social fabric'.[73] However, most Member States laws, again like most non-discrimination laws, emphasise in one way or another the use of civil remedies. Reading the Belgian data protection law suggests that this is the kind of court procedure the legislator has in mind. We recall that civil remedies are victim-focused. Civil court procedures are not as much about the erosion of the social fabric, but deal with the dignity of the victim, and are aimed at bringing data protection violations to an end, restoring the *status quo ante* and ensuring compensation and damages for harm incurred as well as for future loss of earnings.[74] Similarly to other fields often grasping with 'mass harm',[75] one might question this focus on civil court procedures and one cannot but applaud reform plans to install collective actions under European data protection law (see section 7).

*Secondly*, regardless of differences between legal systems, we notice in many countries efforts to go beyond the provisions on remedies in the 1995 Directive and to incorporate provisions designed to ensure prompt and effective remedies against data protection violations. As we will point out in section 9, these 'best practices' were not considered when reforming the EU legislation. Almost none of these procedural mechanisms set at Member State level are found in the EU data protection reform under discussion.

## 5 Data Protection Remedies for Police and Criminal Data and the Schengen Remedial System

The data protection remedial regime established at national level also depends on the categories of data we consider. In some Member States violations concerning personal data processed for police and criminal

72 R. Iordache & I. Ionescu, 18; P. De Hert & D. Ashiagbor (Eds), *Comparative study on access to justice in gender equality and anti-discrimination law*. Synthesis report. (European Commission, Directorate-General for Employment, Social Affairs and Equal Opportunities, 2011).

73 R. Iordache & I. Ionescu, op. cit. 15.

74 Comp. R. Iordache & I. Ionescu, op. cit. 13 & 15.

75 Comp. L. Farkas, 'Collective actions under European anti-discrimination law' [2014/19] *European Anti-discrimination Law Review* 25-40, 25.

purposes can be remedied directly by the data subject contacting the data controller.[76] While a mixed direct-indirect system can also be found,[77] in other Member States access to this data is indirect only.[78] Although different layers in the enforcement of data protection can be identified in this area, they do not necessarily follow the pattern described in our introductory section.[79] Whenever indirect access is in place, layer 1 disappears and DPAs come into play questioning the data controller about the relevant data (ex layer 2), prompted by the initiative of the data subject. As a result, the data subject may obtain access to personal data via the national DPA but most of the time the DPA informs the data subject 'only that all the necessary verifications have taken place'[80] de facto restricting access to police and criminal data. Anyway, the data subject has to rely on the outcome of the DPA's enquiry. In case access is refused, the data subject could appeal to a judicial authority about the DPA's decision but this is an unlikely scenario since remedies for data protection violations are seldom sought before courts.[81] Hence, in this case layer 3 tends to disappear too. Indirect access procedures are very problematic and highly unacceptable from the perspective of the data subject. They obstruct data subjects' access to personal data and the exercise of the right to remedy data protection violations, so impinging on two of the most important rights of the data subject at once. It is remarkable that in those Member States in which indirect access *tout court* is in force such a remedial system concerns any kind of police and criminal data, from anagraphic data to crime notices and alerts. This makes indirect access even more unfriendly to the data subject. In our opinion, the resort to indirect access should be avoided or limited significantly to cover police and criminal data of 'high interest' only. Moreover, procedures for getting access to these categories of data should be streamlined and offer the data subject an element of choice.[82]

---

76 This is the case in Austria, Czech Republic, Denmark, Finland, Germany, Greece, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Malta, the Netherlands, Norway, Poland, Romania, Slovak Republic, Slovenia, Spain and Sweden. See European Data Protection Supervisor (EDPS), SIS II Supervision Coordination Group, *The Schengen Information System. A Guide for exercising the right of access*, 2014.

77 Such as in France and Hungary. *Ibid*.

78 This is the case of Belgium, Luxembourg and Portugal. *Ibid*.

79 In the case of personal data processed by Europol and Eurojust for instance, the data subject can exercise access rights by contacting these institutions (layer 1). However, if the data subject is not satisfied with the decision made by Europol or Eurojust he may seek redress by appealing to an ad-hoc body, namely the Europol Joint Supervisory Body or Eurojust Joint Supervisory Body (layer 2). Anyway, the data subject may remedy data protection violations also before national courts (layer 3). See Art. 32 of the Europol Decision and Art. 19 of the Eurojust Decision.

80 See preamble 29 of the Council Framework Decision 2008/977/JHA.

81 EU Agency for Fundamental Rights (FRA), *Access to data protection remedies in EU Member States*, op. cit.

82 P. De Hert & R. Bellanova, 'Mobility should be fun. A consumer (law) perspective on border check technology' [2011/11] *The Scientific World Journal* 490-502.

Special remedial norms and procedures in the police and criminal justice area are set forth within the Schengen legal framework. Elaborated in the Convention implementing the Schengen Agreement (CISA) which established the Schengen Information System (SIS),[83] these rules have been transposed in the so-called second-generation SIS, or SIS II.[84, 85] Article 58 of the Council Decision 2007/533/JHA (SIS II Decision) grants data subjects the right of access to data entered in SIS II (layer 1). Access requests can be introduced to any of the contracting parties following provisions on access to police and judicial data established at national level. If national law so provides, the national DPA decides whether information is to be communicated and by what procedures (layer 2). However, access may only be refused if 'this is indispensable for the performance of a lawful task in connection with an alert or for the protection of the rights and freedoms of third parties' (Article 58(4) SIS II Decision). It is stipulated that the required information should be provided 'as soon as possible and in any event not later than 60 days from the date on which he applies for access or sooner if national law so provides' (Article 58(6) SIS II Decision). The data subject can bring an action against national courts to obtain access or compensation in connection with an alert relating to him (Article 59(1) SIS II Decision) (layer 3). Enhanced forms of cooperation are part of the Schengen architecture. Where a national court or authority finds a SIS report unlawful and orders the withdrawal of an alert, all contracting parties are obliged to mutually enforce this decision (Article 59(2) SIS II Decision).

Although the Schengen information system concerns data in the police and criminal justice area, we observe that it provides a satisfactory protection of data subjects' rights. The remedial system in place therein is solid and functions well mainly because the data processing system is well structured and organised (1); the remedial system is effective (as it entails binding decisions for all contracting parties) (2) and; it establishes good cooperation mechanisms between

---

83 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [*OJ* L 239, 22.9.2000], 19-62.

84 SIS II was established in 2006 and became operational in 2006. Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [*OJ* L 205, 7.8.2007], 63-81. Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates [*OJ* L 381, 28.12.2006], 1-3.

85 SIS II contains three main categories of data, namely: persons who do not have the right to enter or stay in the Schengen area and in relation to whom an alert has been issued; (1) information on missing persons; (2) data about stolen vehicles, boats, aircrafts, firearms, containers and (3) identity documents which have been lost or stolen or used to carry out a crime.

the police, judicial and administrative authorities (3). As it has been argued, the Schengen information system could be improved.[86] Yet, in our view the system is well designed and procedural rules are detailed enough to provide data subjects with effective forms of redress.

## 6 The EU Data Protection Reform and Individual Remedies (Layer 1)

In the following sections (6-8) we will look at the EU data protection reform package and analyse relevant improvements it will introduce with regard to remedies foreseen in layers 1, 2 and 3. While more procedural rules will characterise layer 2 (and layer 1 but to a lesser extent), layer 3 remedies will not be improved by the reform.

**Procedural Rules**

Variations in the way access rights are exercised across the EU (see section 2) provide evidence of a lack of harmonisation in the enforcement of data protection. The reform is going to tackle mismatches in the exercise of access rights. Article 12(2) of the General Data Protection Regulation (GDPR) states that the data controller shall reply to an access request 'without delay and, at the latest within one month of receipt of the request', so providing a target time frame for all Member States. Moreover, Article 12(4) GDPR holds that access rights requests shall be free of charge and that the data controller may charge a fee only where requests are 'manifestly excessive'.[87] A similar provision can be found at Article 10(5) of the General Data Protection Directive (GDPD).

## 7 The EU Data Protection Reform and Administrative Remedies (Layer 2)

The most remarkable improvements introduced by the data protection reform concern layer 2. In fact, apart from strengthening the role of

---

86 E. Brouwer, 'The EU Passenger Name Record System and Human Rights. Transferring Passenger Data or Passenger Freedom?', in: *CEPS Working Document* (Brussels: CEPS 2009). E. Brouwer, *Digital Borders and Real Rights. Effective remedies for third-country nationals in the Schengen Information System, series Immigration and Asylum Law and Policy in Europe* (Leiden/Boston 2008) Martinus Nijhoff Publishers (dissertation Radboud Universiteit Nijmegen 2007).

87 It is also established that in this kind of case the data controller shall bear the burden of proving the manifestly excessive character of the request.

DPAs, the reform will establish new procedures for remedying data protection violations, such as the one-stop-shop mechanism.

**Procedural rules**

The EU data protection framework currently in place does not set time frames within which complaints should be handled by DPAs. The proposed reform will introduce a new provision in this regard. Article 74(2) of the GDPR establishes a time frame of three months within which DPAs should answer to data subjects' requests. In fact,

'in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint',

data subjects have the right to a judicial remedy.[88] This provision can also be found at Article 51(2) GDPD.

**Collective Actions**

It will be possible to enforce collective actions under the new European data protection framework. The GDPR entitles any organisation or association which aims to protect data subjects' rights to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if data subjects' rights have been infringed (Article 73(2)), or independently of the data subject's complaint if a personal data breach has occurred (Article 73(3)). Moreover, Article 76(1) GDPR points out that organisations and associations are entitled to the right to a judicial remedy against a supervisory authority (Article 74 GDPR) and the right to a judicial remedy against a controller or processor (Article 75 GDPR). The same provisions are enshrined in Article 50(2) and 50(3) GDPD.

While expectations from NGOs to bring claims for data protection violations against DPAs and judicial authorities are growing, doubts on the nature and effectiveness of this form of remedy are emerging. Firstly, the reform does not set clear rules on legal standing. Although the EU legislator uses a wide definition of bodies, associations and organisations which can exercise this remedy, it is not clear whether DPAs themselves will be entitled to do so. Secondly, as the European Commission stressed, although collective forms of redress are

88 This provision substantiates the 'right to a judicial remedy against a supervisory authority' (Art. 74 of the GDPR).

good instruments to enforce EU law, there are different types of collective actions in Europe.[89] It is not clear for instance whether collective actions in data protection law will take the form of class actions, test case proceedings or *actio popularis* claims, which are also used in EU anti-discrimination law.[90] Given the silence of the European legislation, there are good reasons to suppose that they will take the form of collective remedies[91] and follow the same procedural rules established for 'individual' access requests. In addition, theoretical doubts are coupled with more important practical concerns. As recent studies confirmed,

'there is a scarcity of civil society organisations that are able to offer comprehensive and well-publicised services, developing a public profile in the area of data protection. This limits people's access to remedies in practice'.[92]

**One-stop-shop**

One of the cornerstones of the data protection reform consists in the introduction of the one-stop-shop mechanism. It applies in cases in which the data controller (or processor) is established in more than one Member State and allows data subjects and companies to deal with one single DPA. The competent DPA will be the one in which the company's main establishment or representative is located (Article 51(2) GDPR).[93] The implementation of this mechanism will entail two main positive consequences. First, it will relieve data subjects from the duty to introduce multiple complaints about the same issue against a certain company in different Member States. Second, one DPA will take the lead in handling complaints in these circumstances, relieving other DPAs from the same task. Hence, the one-stop-shop mechanism represents a system for streamlining procedures and allocating competences among DPAs. Some have argued that the one-stop-shop mechanism risks creating a data protection

89 European Commission, Commission Staff Working Document, Public Consultation: Towards a coherent European approach to collective redress SEC(2011)173 final [04.02.2011].

90 L. Farkas, 'Collective actions under European anti-discrimination law', *European Anti-discrimination Law Review*, op. cit.

91 On 11 June 2013 the European Commission issued recommendations on collective redress mechanisms in European Member States. See European Commission, Recommendations of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law (2013/396/EU), *OJ* L 201/60, 26.07.2013.

92 EU Agency for Fundamental Rights (FRA), *Access to data protection remedies in EU Member States*, op. cit.

93 According to Art. 51.2 GDPR 'Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation'.

shopping regime for private companies which will be tempted to locate their main establishment in Member States where the enforcement of data subjects' rights is rather weak.[94] Although this certainly represents a risk, much will depend on the way the one-stop-shop will be implemented and on the level of cooperation among DPAs. Recent debates going on about the one-stop-shop mechanism demonstrate that DPAs are aware of the negative consequences this mechanism may entail. Yet, DPAs consider it as a way to strengthen data subjects' rights. Mr Jacob Kohnstamm (chair of the Dutch DPA) for instance has recently pointed out that the one-stop-shop mechanism should only be used in cross-border cases and that consensus should be reached among all involved DPAs before applying the mechanism.[95] This position has recently been endorsed by the European Council according to which cases with minor cross-border relevance should be exempted from the application of the one-stop-shop mechanism.[96] Apart from these considerations, it is important to note that the proposed mechanism does not prevent the data subject from addressing his complaint to a judicial authority in case he is not satisfied with the decision of the lead DPA. Thus, from the perspective of the data subject the one-stop-shop mechanism will simplify procedures and will not exhaust data protection remedies.

## 8 The EU Data Protection Reform and Court Remedies (Layer 3)

Apparently the full focus of the EU reform has been on administrative remedies. Apart from minor improvements which are described below, the EU data protection reform does not introduce new provisions with regard to remedies before national courts. There is, for instance, no harmonisation of the use of criminal sanctions, and, consequently, the possibility of seeking redress and compensation before national criminal courts.[97] There will be further discussion of other omissions in the reform in a later section.

94 C. Fritsch, 'Data processing in employment relations; impacts of the European General Data Protection Regulation focussing on the Data Protection Officer at the Worksite', in: S. Gutwirth, R. Leenes & P. De Hert (Eds), *Reforming European Data Protection Law* (Springer 2015) 147-170.

95 Speech given by Mr Jacob Kohnstamm at the Academy of European Law (ERA) annual conference on European data protection law, 7-8 April 2014.

96 European Council's press release 'Data protection: Council agrees on general principles and the 'one stop shop' mechanism', available at: www.consilium.europa.eu/en/press/press-releases/2015/03/13-data-protection-council-agrees-general-principles-and-one-stop-shop-mechanism/ (last accessed 17 March 2015).

97 P. De Hert, 'The EU data protection reform and the (forgotten) use of criminal sanctions' [2014/4] *International Data Privacy Law* 262-268.

**'Ne Bis in Idem' and Cooperation Among Judicial Authorities**

The principle of *ne bis in idem* (or prohibition of double jeopardy) belongs mainly to criminal law and criminal procedural law.[98] In the proposed data protection reform the EU legislator applies this principle to judicial proceedings for data protection matters initiated before more than one Member State. Article 76(3) of the GDPR states that

'where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State'.

Moreover, 'where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings' (Article 76(4) GDPR).

## 9 What's Missing in the Remedial System of the EU Reform?

The mere existence of procedural rules on the enforcement of data protection violations is not in itself a sufficient condition for remedying data breaches. Rather, data subjects expect data protection remedies to be effective and efficient instruments. Effectiveness is one of the recurrent words of the proposed data protection reform. In particular, the reform requires powers of DPAs to be effective, and effective administrative and judicial redress for data subjects.[99] The need to ensure effective data protection remedies has been stressed also by the ECrtHR. As mentioned in section 3, the ECrtHR highlighted this aspect in *Silver and Others v. the UK*[100] and *Leander v. Sweden*.[101] Moreover, effectiveness was at the core of the judgments *Haralambie v. Romania*[102] and *Segerstedt-Wiberg and al. v. Sweden*.[103] In *Haralambie* the Court found that the

98 It stipulates that the defendant should not be prosecuted twice (or repeatedly) for the same offence, acts or facts. B. Van Bockel, *The ne bis in idem principle in EU law* (Kluwer Law International 2010).

99 Art. 47.5 GDPR states that 'Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers'. Moreover, DPAs shall 'put in place measures for effective cooperation with one another' (Art. 55.1 GDPR). Similar provisions are laid down at Art. 40.5, 46 and 48.1 GDPD.

100 *Silver and Others v. the United Kingdom* (App. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75), ECrtHR, judgment of 25 March 1983, para. 113.

101 *Leander v. Sweden* (App. 9248/81), ECrtHR, judgment of 26 March 1987, para. 77.

102 *Haralambie v. Romania* (App. 21737/03), ECrtHR, judgment of 27 October 2009.

103 *Segerstedt-Wiberg and al. v. Sweden* (App. 62332/00), ECrtHR, judgment of 6 June 2006.

Romanian authorities failed to provide the applicant with an 'effective and accessible procedure' which would have ultimately allowed the applicant to access information he was asking for.[104] In *Segerstedt-Wiberg* the Court established that a violation of Article 13 ECHR occurred as the applicants had been given no effective remedy to challenge the supposed violations of Articles 8, 10, 11 ECHR.[105] In particular, the Court observed that although data subjects could remedy data protection violations before the Parliamentary Ombudspersons and the Chancellor of Justice, these institutions lacked the 'power to render a legally binding decision'.[106]

There are two main unanswered questions about the effectiveness of DPAs and of their powers in data protection law. First, although it is undisputed that effectiveness should drive DPAs' action, it is unclear how this goal could be reached. As confirmed by recent studies, DPAs lack adequate financial resources and are understaffed.[107] This undermines the right to an effective remedy and may compromise the enforcement of data protection as such. The data protection reform reiterates that Member States should make sure that data protection remedies established at national level are effective. However, the 'how' question remains unanswered. Second, although effectiveness in data protection law represents a priority for the EU legislator, we observe that so far the CJEU has never pronounced itself on the effectiveness of DPAs and of their powers, rather turning its attention to independence (see section 3). Effectiveness is crucial for enforcing data protection. Apart from making the right to an effective remedy void, ineffective procedures risk causing detrimental effects for the data subject. Similarly, procedures should be accessible and the data subject should be provided with clear and detailed information on how to remedy data protection breaches. Thus, we look forward to more cases like *Haralambie* and *Segerstedt-Wiberg* in the future.[108]

As illustrated in section 5, a well-functioning remedial system (like the Schengen one) is based on a structured and organised data processing, on effective redress procedures and on good cooperation mechanisms among administrative and judicial authorities. Notwithstanding improvements of the data protection reform, the EU remedial system of data protection violations seems

104 *Ibid.*, paras 86 and 96.
105 *Ibid.*, para. 121.
106 *Ibid.*, para. 118.
107 EU Agency for Fundamental Rights (FRA), *Data protection in the European Union: The role of national Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*, op. cit.
108 P. De Hert, *Citizens' data and technology: An optimistic perspective* (The Hague, Dutch Data Protection Authority 2009), 1-54, 26.

to be a bit too far from that target. In particular, decisions made by DPAs are not binding in all Member States and most of the time there is no coordinated data sharing of cases and complaints at EU level.

Apart from effectiveness, we find that other issues are not properly addressed by the data protection reform. Differences that emerge by comparing data protection remedies sought before national courts and in the former third pillar (see sections 4 and 5) are not going to be affected by harmonisation processes. The EU legislator could have fixed summary proceedings before national courts for data protection violations. Similarly, he could have established the reversal of the burden of proof for damages deriving from data protection breaches. Likewise, he could have harmonised proceedings for data protection violations in police and criminal matters addressing differences at the national level between direct and indirect remedies.[109] Generally speaking, the GDPD could have done more to assist individuals while claiming their data protection rights in the case of police and criminal data.[110]

Equally, the EU data protection reform will not improve provisions on liability and compensation and violations will continue to be assessed at national level on a case-by-case basis. Although this outcome is (once again) unsurprising, it does not consider the difficulty of national authorities in assessing data protection violations and the harm they entail.[111] This problem is more than real and has to do with the often immaterial nature of data protection harm and the difficulty to identify the individual victims.[112] As a consequence, the current data protection liability regime does not give the claimant (namely, the data subject) a clear idea of the relief he will get for the violation itself, as well as for its negative consequences. Yet, with the reform some things will change. The proposed GDPR introduces, for the first time in EU data protection law, an articulated system of administrative sanctions to challenge data protection violations and makes them mandatory (Article 79 GDPR).[113] Moreover, it lays down a catalogue of crimes which can lead to those sanctions. However, there is no provision of

---

109 Indeed, by limiting the scope of indirect remedies, redress could have been made more accessible to the data subject.

110 P. De Hert & V. Papakonstantinou, 'The police and criminal justice data protection Directive: Comment and Analysis' [2012/22/6] *Society for Computers and Law*.

111 A. Ward, 'Damages under the EU Charter of Fundamental Rights' [2012/12/4] ERA Forum, Springer, 589-611.

112 About the notion of mass harm and the reasons in non-discrimination law that account for lack of access to justice, see L. Farkas, 26-27.

113 In fact, one of the main reasons that led the European legislation to undertake the ambitious and herculean task to reform data protection consisted in the need to better enforce data protection. P. De Hert, 'The EU data protection reform and the (forgotten) use of criminal sanctions', op. cit.

this kind in the GDPD and criminal sanctions are not harmonised at all in the reform package.[114]

In spite of Member States' unwillingness to harmonise procedural and criminal law norms, we would have welcomed provisions in the GDPR and GDPD granting data subjects the right to obtain a certain monetary reparation for the damage suffered, including both pure harm and the contingent loss of profit. The EU legislator could have possibly fixed minimum (and maximum) limits for amounts awarded as compensation and care should have been devoted to find specifically tailored ways of compensation. If a plane is kept at the airport or passengers are refused boarding on unjustified grounds, a lump-sum as the baseline seems to be the most appropriate solution. Hence, the reform could have introduced a compensation scheme similar to the one established for passengers' rights under EU law.[115]

Similarly, the reform could have clarified whether data subjects can obtain monetary reparation simply by addressing the DPA.[116] Moreover, the GDPD could have introduced a detailed set of sanctions in order for the data subject to obtain relief in case of unlawful or illegitimate processing of police and criminal data (as the GDPR does). Although one cannot find these provisions in the GDPR and GDPD, it is noteworthy that the ECrtHR recognises that the claimant should be provided 'sufficient just satisfaction' for the immaterial damage descending from data protection violations.[117] More concrete forms of assessment of damages resulting from data protection violations would have helped Member States (and all relevant actors in society) to take on their responsibilities in a systematic way.[118]

---

114 P. De Hert, 'The EU data protection reform and the (forgotten) use of criminal sanctions, *International Data Privacy Law*, op. cit.

115 A denied-boarding compensation system for instance is established for air passengers under EU law. See Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91 [*OJ* L 46, 17.2.2004]. See P. De Hert & R. Bellanova, 'Mobility should be fun. A consumer (law) perspective on border check technology', op. cit.

116 In Greece for instance while the DPA is authorised to impose administrative (also monetary) penalties, the only way for data subjects to receive monetary reparation for infringement of their data protection rights is to refer the matter to civil courts (Art. 664-676 of the Greek Civil Procedure Code). V. Papakonstantinou, *Information Technology Law* (Sakkoulas publications 2010), 206.

117 See *I v. Finland* (App. 20511/03), ECrtHR, judgment of 17 July 2008, para. 55.

118 P. De Hert, 'From the principle of accountability to system responsibility. Key concepts in data protection law and human rights discussions' (2011), International Data Protection Conference, 88-120.

As illustrated in this section, several issues are not addressed or solved by the reformed data protection package which hence (still) prefers to leave the Member States with discretion, while keeping differences among data protection regimes in the former pillars.[119] In our view, they represent missed opportunities for strengthening the right to an effective remedy in data protection law and data subjects' rights. As the above-mentioned creative ideas confirm, there is still room for the EU legislator to improve provisions on data protection remedies, liability and sanctions.

## 10 Conclusion: a Proceduralisation Process with some Room for Improvement

Without being able to illustrate how data protection violations are remedied in all EU Member States, in this paper we identified the remedial system of data protection violations under EU law. Directive 95/46/EC rolls out a 3-layer system of remedies in all Member States: a) data subjects are given a set of detailed subjective and empowering rights in order to make control of use of their data that is in the hands of others; b) DPAs are set up in all Member States with a set of powers that depend on the national legal system. They provide support to data subjects that face difficulties with enforcing their subjective rights (in all countries) and impose administrative fines for data protection violations (in some countries); and c) court remedies before civil, administrative and criminal law courts. We discussed differences in the organisation of the court procedures and noted the efforts of some Member States to add devices for facilitating access to courts (through the reversal of the burden of proof and swift procedures for instance) on top of what has been imposed by Directive 95/46/EC. Moreover, we referred to remedial regimes established for criminal, police and judicial data.

We found that there is a growing grip on remedies and procedures for remedying data protection violations by the EU legislator. There is, firstly, the case law of the European Court of Justice and of the European Court of Human Rights that concerns making the exercise of access rights more effective and at safeguarding the effectiveness and independence of the administrative bodies set up by the Member States. Also, there is the upcoming data protection reform. The reform is aiming to proceduralise data protection remedies in the EU. The new regulation (for general processing activities) and the new directive (for data processing by the police and judiciary) will introduce more and more detailed

[119] P. De Hert, V. Papakonstantinou, D. Wright & S. Gutwirth, 'The proposed Regulation and the construction of a principles-driven system for individual data protection' [2013/26/1-2] *Innovation: The European Journal of Social Science Research*, 133-144.

norms to regulate data protection breaches, also harmonising administrative sanctions. The new remedial system of data protection violations will increasingly rely on procedures and principles which govern judicial proceedings (that is, the principle of *ne bis in idem*). Moreover, the data protection reform will introduce new provisions aimed at encouraging cooperation among national DPAs, among national judicial authorities and between DPAs and judicial authorities (such as through the one-stop-shop mechanism). There is no doubt that the proceduralisation process promoted by the reform will result in a certain loss of procedural autonomy by Member States. Yet, the ability of EU data protection to have a trans-border impact will lead to a far-going harmonisation and integration.

We noted a systematic lack of attention in the reform to layer 1 (individual remedies sought before the data controller (or processor)) and lack of efforts to improve layer 3 (court remedies). As far as the processing of police, judicial and criminal data is concerned, no firm mechanism to allow direct access *whenever possible*, is introduced. Many EU texts with specific arrangements on data protection remedies do not foresee concrete guidelines explaining where individuals should go and whom they should address their claim to, with Schengen being a notable exception. Also, with regard to court remedies no efforts have been made to improve access to courts and to incorporate best practices developed by Member States concerning the burden of proof and the swiftness of procedures. It would be unrealistic to shift civil, administrative and criminal procedure law from the competence of Member States to the EU, but it would be just as unreasonable to argue that data protection violations could be remedied only by the EU courts. In fact, as pointed out, the remedial system provided by the ECrtHR is characterised by several shortcomings which would not guarantee an effective remedy to the data subject.[120] Hence, there is no other solution than proceduralising data protection remedies while at the same time improving the current administrative and court system. Although DPAs represent a legitimate alternative to judicial authorities in the enforcement of data protection, they cannot replace the role of the courts. Although improvements made by the data protection reform are remarkable, there is still room to develop and improve the EU remedial system for data protection violations, possibly by looking at best practices developed in Member State law and at certain remedial systems such as Schengen, as well as by identifying best practices in EU law (such in the case of passengers' rights).

120 C. Morgan, 'Where are we now with EU procedural rights?' [2012] *European Human Rights Law Review* 427.