Roles and Powers of National Data Protection Authorities

Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?

*Andra Giurgiu and Tine A Larsen**

Safeguarding the rights of the citizens to the protection of their personal data in an era of nearly ubiquitous computing has become increasingly challenging. National data protection authorities (DPAs), central actors in the data protection landscape, face a difficult task when fulfilling their missions and acting as guardians of these rights under the provisions of the outdated Directive 95/46/EC. Critical decisions of the Court of Justice of the European Union illustrate the challenge of 'stretching' the provisions regarding the powers and competences of DPAs under the Directive to make them applicable to current data processing realities. The article points out the existing problems under the current framework with regard to powers and competence of DPAs and examines if and to what extent they are mended by the General Data Protection Regulation (GDPR). It analyses substantive and procedural aspects of the new cooperation model under the one-stop-shop and consistency mechanisms and discusses whether and how these new tools successfully contribute to solve existing problems.

I. Introduction: Data Protection Authorities as a Fundamental Pillar of EU Data Protection Law

The European right to the protection of personal data builds on three main pillars: the obligations of data controllers, the rights of data subjects and the role of data protection authorities (DPAs).[1] The existence and well-functioning of independent DPAs in the Member States constitutes 'an essential component' of European Union (EU) personal data protection.[2] There has been important case-law from the Court of Justice of the European Union (CJEU) on the need to ensure the independence of national DPAs[3] exactly because of their fundamental role as regards monitoring the application and ensuring compliance with data protection law, as well as generally acting as guardians of the rights of citizens as far as the protection of their personal data is concerned.

According to Directive 95/46/EC[4], each Member State has the obligation to set up a national DPA, the mission of which is to monitor the application of the national data protection laws implementing the EU Directive. DPAs derive this mandate from legal in-

* Andra Giurgiu is Post-Doctoral Researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg; for correspondence: <andra.giurgiu@uni.lu>. Tine A Larsen is the President of the National Commission for Data Protection of Luxembourg; for correspondence: <info@cnpd.lu>.

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23 November 1995, recital 62; see also Gloria González Fuster, 'Beyond the GDPR, above the GDPR' (*Internet Policy Review*, 30 November 2015) <http://policyreview.info/articles/news/beyond-gdpr-above-gdpr/385> accessed 18 August 2016.

2 Directive 95/46/EC, recital 62.

3 For the CJEU case-law on the independence of national data protection authorities see also Case C-518/07 *European Commission v Federal Republic of Germany* [2010] ECLI:EU:C:2010:125; Case C- 614/10 *European Commission v Republic of Austria* [2012] ECLI:EU:C:2012:631; Case C-288/12 *Commission v Hungary* [2014] ECLI:EU:C:2014:237; but also Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

4 Directive 95/46/EC, art 28 para 1.

struments of primary law, more specifically, Article 16(2) of the Treaty on the Functioning of the European Union (TFEU) as well as Article 8(3) of the Charter of Fundamental Rights of the European Union. As such, as Hijmans observes, DPAs have a rather hybrid status in the sense that they are 'attached to the constitutional frameworks of the Member States as well as to that of the European Union'.[5] According to the same author, even though they are national bodies that have been established under national law, DPAs exercise their tasks on the basis of primary EU law.[6] This status, between EU and Member State law, has been defining in the way DPAs have performed their role under the general mandate created by Directive 95/46/EC but subject to the constraints of having to take into account the national context of their own Member State law.

Adopted at a time when the Internet was still in its infancy, Directive 95/46/EC proves to be rather difficult to mould to the current realities of ubiquitous computing. It becomes thus clear that a new piece of legislation was much needed to cope with the data protection challenges of today's Internet age. This article will examine the competence and powers of DPAs under the current Directive 95/46/EC, with particular reference to the relevant jurisprudence of the CJEU. It analyses the major changes brought by the General Data Protection Regulation (GDPR)[7] in the way DPAs exercise their role in view of the new, layered competence as well as of the set of clear, homogenous powers they have been endowed with. Furthermore the article discusses the GDPR's new cooperation model under the one-stop-shop and consistency mechanisms. The final considerations address the questions of whether and how these changes successfully manage to solve the existing problems.

II. Data Protection Authorities under Directive 95/46/EC

1. Competence and Powers

The competence of a DPA is determined by the national law of that specific Member State and linked to the territoriality principle. Under the Directive, a DPA, like any other national public authority, can therefore only exercise its powers within the territory of the Member State where it is established and based on the national law of the same state.

A clash between applicable law and competence is however possible especially in today's context of widespread cross-border data processing, enabled by the use of the Internet. In reality, a processing could fall under the law of one Member State, depending on the place of the establishment of the controller, while the competence of the DPA would be determined according to the law of another Member State, such as that where the affected data subjects reside.

Directive 95/46/EC explicitly states that a DPA 'is competent, whatever the national law applicable to the processing in question' is.[8] This general competence leaves it open for a DPA to apply, in limited circumstances[9], the law of another Member State.[10] The issue remains however one of applicable law[11] to the processing in question as the actual powers of the DPA will be determined according to the general rules on competence as set out in its own national law. Such a conflicting situation has been examined by the CJEU in *Weltimmo*[12], a case we will refer to in more detail at a later stage of our analysis.

There are a few defining points as regards the powers of DPAs under the current Directive 95/46/EC. Firstly, since the Directive is not directly applicable in the Member States, it had to be implemented by transposition into national law. This created differences across the EU and thus legal uncertainty for businesses and data subjects alike. Hence, the need to counter the lack of harmonisation of data protection laws across the EU, which was one of the main

5 Hielke Hijmans, 'The EU as a constitutional guardian of internet privacy and data protection' (PhD thesis, University of Amsterdam, 2016) 287, downloaded from UvA-DARE, the institutional repository of the University of Amsterdam (UvA) <http://hdl.handle.net/11245/2.169421> accessed 18 August 2016.

6 ibid 311.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016, 1–88.

8 Directive 95/46/EC, art 28 para 6.

9 Following the application of art 4 para 1 Directive 95/46/EC.

10 Ulrich Damman and Spiros Simitis, *EG-Datenschutzrichtilinie: Kommentar* (1997) 306.

11 For a more detailed analysis on the matter of applicable law see also Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, WP 179 (10 December 2010); *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain*, WP 179 (update of 16 December 2015).

12 Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] EU:C:2015:639.

objectives of the proposal of the new GDPR,[13] and to create a single set of rules. Time will show if this objective can be fully reached in practice.[14]

Secondly, Directive 95/46/EC could not be overly prescriptive, as it had to leave national legislators room for the implementation. Thus the powers of DPAs are defined only in a general manner. They are grouped into basic categories as: investigative powers, powers of intervention, powers to engage in legal proceedings and to hear claims.[15] Additionally, a DPA has advisory powers and should be consulted by national legislators when they draw up regulations or administrative measures relating to data protection.[16]

The investigative powers include the power to access data and the power to collect information, which the DPA needs for the performance of its duties. A DPA is also endowed with effective powers of intervention, which can be grouped into two categories. Firstly, there are powers of intervention with direct legal effect, such as blocking, erasure, destruction of data, or imposing a ban on processing. Secondly, the powers of intervention can have an indirect effect as in the case of warning or admonishing the controller or referring the matter to national parliaments or other political institutions.[17] Lastly, DPAs can engage in legal proceedings as well as bring violations of national data protection provisions to the attention of judicial authorities.

The lack of harmonisation of national implementation laws with regard to the powers of DPAs can be well exemplified by looking at the way sanctions are regulated in the different Member States. Article 24 of Directive 95/46/EC states that Member States have to 'lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive'. However, the Directive does not clearly and explicitly state that a DPA shall be able to impose fines.[18] This general provision has left it open for the national legislator to determine who can apply the sanctions, following which national law as well as the type of sanctions available. As a consequence, the sanctions for infringing data protection law can be enshrined in criminal or administrative law, they can be applied by courts or national DPAs and their nature can be pecuniary or non-pecuniary. This led to major differences in their application throughout the EU. According to a report of the European Fundamental Rights Agency, in Lithuania sanctions can only take the form of criminal fines imposed by judicial authorities. In Germany, on the other hand, judicial authorities can also order detention and DPAs are themselves endowed with the power to impose administrative fines.[19] The obvious consequence is that some Member State DPAs are 'stronger' while others are 'weaker' in the enforcement of data protection law.

Especially against this background of legal fragmentation cooperation plays a particularly important role. DPAs have a general obligation to cooperate in the performance of their duties, in particular by exchanging all useful information, and may be requested to exercise their powers by an authority of another Member State.[20] This model of 'horizontal cooperation' is characterised by a lack of hierarchy, shared responsibilities, a common interest, good faith and good administration.[21] Under Directive 95/46/EC cooperation is however not 'institutionalised' through clear rules and strict time frames but takes place at a rather informal level.

The Directive creates another layer of cooperation by establishing the Working Party on the Protection of Individuals with regard to the Processing of Personal Data[22] (Article 29 Working Party) which acts like a 'structured network of DPAs'[23]. The Article 29 Working Party (A29 WP) is composed of representatives of the DPAs of each Member State and of the European Data Protection Supervisor. It fulfils an advisory role, mainly by delivering opinions, recom-

13 See Press Release of the European Commission (25 January 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en > accessed 18 August 2016.

14 It has been pointed that despite the formal harmonization, the Regulation still contains many 'flexibilities' which would allow for a divergent transposition of the Regulation by Member States. For a full analysis of these flexibilities see the analysis by European Digital Rights (EDRi), 'Flexibilities in the General Data Protection Regulation' (2016) <https://edri.org/files/GDPR_analysis/EDRi _analysis_gdpr_flexibilities.pdf> accessed 8 August 2016.

15 Directive 95/46/EC, art 28 para 3 and 4.

16 For an analysis of the powers of DPAs see also the European Union Agency for Fundamental Rights, *Data Protection in the European Union: The Role of National Data Protection Authorities* (2010) 20-28.

17 Damman and Simitis (n 10) 309.

18 See also Lee A. Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014) 172.

19 See also the European Union Agency for Fundamental Rights (n 16) 34.

20 Directive 95/46/EC, art 28 para 6.

21 Hijmans (n 5) 370.

22 Directive 95/46/EC, art 29.

23 Hijmans (n 5) 373.

mendations and reports to promote the uniform application of Directive 95/46/EC in all Member States. As one author remarks, the A29 WP is probably the 'most significant embodiment of regional coordination'.[24] Its role is however limited to giving guidance. Compared to its successor under the GDPR, the European Data Protection Board, the Working Party has a significantly weaker position.

The issues of competence and powers of DPAs play a particularly important role in the context of the widespread and practically borderless Internet use of today. So far, we have discussed the legal framework as well as highlighted some of the theoretical problems as regards competence and powers of DPAs under Directive 95/46/EC. In the following section, this article will examine the challenges of applying this outdated Directive in the current Internet age by referring to some of the most relevant and controversial jurisprudence of the CJEU, which deals with the issues of competence and powers of DPAs.

2. Relevant CJEU Case-Law: Stretching the Powers and Competences of DPAs under Directive 95/46/EC

Today, EU and non-EU companies are constantly offering services to EU residents or are monitoring their behaviour. Under Directive 95/46/EC, data subjects face the difficult task of defending and enforcing the right to the protection of their personal data rights vis-à-vis companies. Especially when the data processing is carried out by strong 'Internet players' with no establishment in the European Union, EU citizens have a particularly disadvantageous position. In such situations, the powers of a DPA, acting as a guardian of citizens' rights, are very limited. The success of its enforcement actions against companies based outside the EU would depend on the companies' willingness to cooperate. The CJEU has however taken an active role in safeguarding the right to the protection of personal data of EU citizens as illustrated by some of its recent decisions concerning the application of Directive 95/46/EC.

In *Google Spain*[25], one of the main issues examined was the territorial scope of application of Directive 95/46/EC. By this judgment the CJEU recognised not only a wide interpretation of the notion of 'establishment', so that Directive 95/46/EC would be applicable to companies from outside the EU (in this case Internet search engine operators), but it also decided on the responsibility of such operators with regard to data subject's right.

The initial case concerned a complaint of a Spanish citizen. The complaint was directed against a daily newspaper, which republished personal information regarding the recovery of old social security debts of the complainant in its online version. The complaint was also directed against Google Spain and Google Inc., which made this information available via the search engine. Whereas the Spanish DPA rejected the complaint against the newspaper it upheld the case against Google Spain and Google Inc. Both Google entities appealed the decision of the Spanish DPA to the Spanish High Court, which joined the two actions and forwarded the case to the CJEU as a reference for a preliminary ruling.

With regard to the territorial scope of application of Directive 95/46/EC the Court found that Google Spain is an establishment within the meaning of Article 4(1)(a) of Directive 95/46/EC because it engages in the effective and real exercise of activity through stable arrangements in Spain, has legal personality and represents a subsidiary of Google Inc. on Spanish territory.[26] Furthermore, the Court found that the processing carried out in the context of search engines operated by a non-EU based company such as Google Inc. with an establishment in a Member State is carried out 'in the context of the activities' of that establishment (in this case Google Spain) if that establishment 'is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable'.[27] The CJEU held that the activities of Google Inc. and Google Spain are 'inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed'.[28]

As regards the responsibility of internet search engine operators and the rights of the data subjects, the

24 Bygrave (n 18) 174.

25 Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] EU:C:2014:317.

26 C-131/12, para 49 of the judgment.

27 C-131/12, para 55 of the judgment.

28 C-131/12, para 56 of the judgment.

Court confirmed that[29], a person has a so-called 'right to be de-listed', according to which he or she can, under certain circumstances, request the removal of links to personal information displayed by search engines following a search based on a person's name. After this decision, the cooperation of DPAs has played an essential role in making sure that the 'right to be de-listed' would be interpreted and applied in a coherent manner. More specifically, DPAs collaborated within the A29 WP on the development of guidelines for the unitary implementation of this judgment. [30]

A year later, the issues of applicable law and powers of DPAs were subject to examination by the CJEU in *Weltimmo*[31]. This case concerned a company registered in Slovakia which ran a website for selling Hungarian properties. For this purpose Weltimmo processed the personal data of the advertisers of those properties. The main two disputed problems were that of applicable law and the competence and powers of DPAs.

The Court analysed the question of which powers a DPA can exercise when the data processing falls under the substantive law of another Member State.[32] The A29 WP already pointed to the increased legal complexity of bridging the possible gap between applicable law and supervisory jurisdiction, back in 2011 when analysing Article 28(2) of Directive 95/46/EC.[33] It is exactly this situation which was addressed by the CJEU in its judgment. The Court found that when the law applicable is that of another Member State, a DPA still can and shall exercise the powers it is endowed with by Article 28(3) of Directive 95/46/EC, in particular its powers of investigation. Such powers are however limited to the territory of its own Member State so that the DPA is not entitled to impose sanctions on a controller established in another Member State. This power belongs to the DPA of the Member State the substantive law of which applies to the processing in question. In this context the cooperation between the two DPAs has to play an important role.[34] This judgment also confirms that the Court is willing to go far in its interpretation of the notion of 'establishment' in order to guarantee efficient protection of affected data subjects. As one author observes, such an interpretation relies more on the notion of activities than on the actual place of establishment.[35] The fact that the controller's activity is directed towards a certain Member State and its residents – affected data subjects – gains more weight than the actual place of establishment.

Moreover, in the *Max Schrems*[36] decision the CJEU stressed once again the need to guarantee the independence of DPAs[37], which is meant to ensure the effectiveness and reliability of the monitoring of compliance.[38] The substance of the case concerned data transfers to a third country based on an adequacy decision of the European Commission, namely the Safe Harbour decision. Since its adoption, Safe Harbour has allowed for data transfers to take place from the EU to the United States (US), under the presumption that the US ensures an adequate protection of personal data. This adequacy was indirectly challenged by the complainant Max Schrems. In this context one of the main issues analysed by the Court was whether a DPA has the competence to examine a complaint pertaining to an adequacy decision of the European Commission. The CJEU ruling stressed once again the independence of DPAs as the Court decided that not even a Commission adequacy decision such as Safe Harbour can prevent a DPA from examining a person's claim relating to the protection of its personal data as regards data transfers to third counties. A DPA 'must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive'.[39]

In the case of *Rease and Wullems*, the CJEU was supposed to answer the question whether a DPA is

29 Based on arts 12(b) and 14(a) of Directive 95/46/EC.

30 A29 WP, *Guidelines on the implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Espagnola de Proteccion de Datos (AEPD) and* Mario Costeja Gonzalez" C-131/12, WP 225 (26 November 2014).

31 Case C-230/14 *Weltimmo* (n 12).

32 See also Mark D. Cole and Andra Giurgiu, 'The 'Minimal' Approach: the CJEU on the Concept of 'Establishment' Triggering Jurisdiction for DPAs and Limitations of Their Sanctioning Powers (Case C-230/14, Weltimmo)' (2015) 1 EDPL 310–315.

33 A29 WP, *Advice paper on the practical implementation of the Article 28(6) of the Directive 95/46/EC* (20 April 2011) 1.

34 C-230/14, para 57 of the judgement.

35 Anne Debet, 'Arrêt Weltimmo: un nouvel élargissement par la CJUE de la notion d'établissement' (December 2015) 12 Communication Commerce électronique 37.

36 Case C-362/14 *Schrems* (n 3).

37 The judgment builds on previous CJEU decisions with regard to the independence of DPAs: C-518/07 *Commission v Germany*, C-614/10 *Commission v Austria* and C-288/12 *Commission v Hungary*.

38 C-362/14, para 41 of the judgment.

39 C-362/14, para 57 of the judgment.

obliged in all cases to investigate a complaint. It had to decide on whether a DPA has the margin to set priorities with regard to the enforcement of the protection of individuals that would result 'in such enforcement not taking place in the case where only an individual or a small group of persons submit a complaint alleging a breach'[40] of Directive 96/46/EC. Regrettably, the CJEU did not have the opportunity to clarify this issue as the Dutch Council of State withdrew the reference for a preliminary ruling.

These decisions clearly illustrate how difficult it is to apply a directive adopted at a time when the Internet was still in its infancy to the current data processing realities. New 'updated' data protection legislation was much needed to cope with the challenges of intra and extra European cross-border processing and to create the right premises for national DPAs to fulfil their mission adequately.

II. Competence and Powers of DPAs under the General Data Protection Regulation

The new General Data Protection Regulation (GDPR) replaces the current Directive 95/46/EC[41] with modern rules, better adapted to the Internet age. It is based on the general rules and principles of the current Directive, which it strengthens and extends overall. In contrast to the Directive, the Regulation will be directly applicable across the European Union. It will thus harmonize data protection rules in the EU and eliminate the current legal fragmentation and uncertainty. The ambition of the Regulation was to create data protection rules fit for the Digital Single Market that would alleviate problems companies are currently facing when doing business in the Union. Additionally, they should give individuals more control over their personal data.[42] Most important in the context of this contribution is the fact that the Regulation strengthens the role of national DPAs as guardians of the respect of EU data protection law. It does so by extending their competence, by determining clear and strong powers and by setting up a mechanism for their cooperation in transnational cases. The role of DPAs is thus reinforced and their overall importance in the data protection landscape significantly enhanced.[43]

1. New Extended and Layered Competences for DPAs under the GDPR

The GDPR introduces two different types of competences. These can be characterised as 'single' and 'collaborative'.

The single competence of a DPA to deal alone with a case is mainly based on the territoriality principle.[44] It can be 'absolutely single' (exclusive) or not. The Regulation provides that the competence is fully exclusive when the processing is carried out by public authorities and public bodies or when it concerns operations of courts acting in their judicial capacity.[45] For such types of processing operations concerning national matters no other DPA should be able to interfere. There is a presumed and thus 'relative' single competence when a DPA receives a complaint which concerns only an establishment in its own Member State or which relates to data subjects that are affected only in the Member State of that DPA.[46] Normally, the DPA should deal with the case alone, with no interference from a foreign DPA as the matter appears to be purely local. For the sake of ensuring consistency however, in case the interest in the matter might exceed the local context, the Regulation states that the DPA has to inform the DPA in charge of supervising the main or single establishment of the controller or processor which can then decide whether or not to participate in the case.[47] The competence could then become 'collaborative' if this DPA also decides to engage in the case.

In addition to the general rule based on the territoriality principle, the GDPR also introduces a 'col-

40 C-192/15 Rease and Wullems, request for a preliminary ruling from the Raad van State (Netherlands) lodged on 24 April 2015 (withdrawn).

41 The Regulation will enter into force on 24 May 2016 and shall apply from 25 May 2018.

42 See also Andra Giurgiu and Gérard Lommel, 'A new Approach to EU Data Protection – More Control over Personal Data and Increased Responsibility' (2014) 1 Critical Quarterly for Legislation and Law (CritQ) 10-27.

43 Peter Blume and Christian Wiese Svanberg, 'The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Private/Public Sector Divide and the Bureaucratic Apparatus' (January 2013) 15 Cambridge Yearbook of European Legal Studies 27-46.

44 GDPR, art 55 para 1.

45 GDPR, art paras 2 and 3.

46 GDPR, art 56 para 2.

47 GDPR, art 56 para 3.

laborative' competence. Such a competence is triggered in cases of 'cross-border processing,'[48] when a DPA has to cooperate with other DPAs.

Under the 'collaborative' competence a DPA can be a 'concerned' or the 'lead' authority. The lead competence of a DPA is determined according to the place of the main, respectively of the single establishment of the controller or processor in the European Union.[49] The competence as concerned DPA can be triggered by the fact that the controller or the processor is established on the territory of the Member State of that DPA, because data subjects in its territory are substantially affected or likely to be substantially affected by the processing[50] or because a complaint has been lodged with it.[51] Thus, if a company has several establishments in the European Union, the DPA of the Member State of the main establishment will have the lead competence, while the DPAs of the States of the other establishments will act as concerned DPAs. If a company has only one establishment in the Union but the processing affects data subjects in other Member States, the DPA of the State of the single establishment will have the lead, while DPAs of the States of the affected data subjects are considered to be concerned.

Thus the controversy partially solved by the CJEU in *Google Spain* and *Weltimmo* is settled as Member States' DPAs gain clear competence as 'concerned' DPAs when companies are targeting their citizens. Moreover, the competence is made independent of the existence of an establishment of the company in the Member State of the DPA, if data subjects residing in that State are affected by the processing.

For the purpose of finding a structured way of cooperation between DPAs and consistency in the application of the Regulation, the GDPR has introduced a so-called 'one-stop-shop' mechanism. It regulates the way in which DPAs exercise their shared competence in cross-border cases with a wider impact in the EU and will be discussed further below. Previously, the next section will introduce the novelties regarding the powers of DPAs and explain how these powers will be exercised under the one-stop-shop.

2. A Homogenous and Clear Set of Powers for DPAs

As opposed to Directive 95/46/EC, the Regulation now foresees a set of clearly defined tasks and powers equally applicable to all European DPAs. The tasks circumscribe their fundamental duties, such as monitoring and enforcing the application of the Regulation, promoting awareness, dealing with complaints, cooperating with other DPAs etc.[52]. The powers represent the means to perform these tasks.[53] The powers of DPAs are now grouped into three main categories, namely investigative powers, corrective powers as well as authorisation and advisory powers.[54]

The investigative powers mainly refer to the powers of DPAs to carry out investigations in the form of data protection audits or to review certifications issued pursuant to the Regulation. They also include the powers of DPAs to receive from the controller or processor the access to data and to the premises, equipment and information needed for the purpose of carrying out the investigation.[55]

In exercising their authorisation and advisory powers, DPAs can issue opinions directed at the national legislator, advise controllers or processors as well as, among others, authorise certain types of processing operations which require prior authorisation. They can approve codes of conduct and binding corporate rules, accredit certification bodies or adopt standard contractual clauses.[56]

But probably the strongest and most coercive function of future DPAs lies within the exercise of their corrective powers. These range from the application of milder sanctions like issuing warnings to the con-

48 The first situation of cross-border processing requires the presence of two or more establishments of the controller or processor in the EU, provided the processing takes place in the context of the activities of the establishments. Secondly, there will be cross-border processing when there is only one establishment in the Union, with the additional requirement that the processing substantially affects or is likely to substantially affect data subjects in more than one Member State. The Regulation itself does however not determine any threshold or give any indications under which circumstances data subjects are 'substantially' affected. For the definition of the term 'cross-border processing of personal data', see art 4 para 23 GDPR.

49 GDPR, art 56 para 1.

50 As a novelty, the GDPR will have an extraterritorial effect. It will apply also to companies based outside the EU, which offer goods or services to data subjects in the Union or which monitor the data subjects' behaviour, see art 3 para 2 GDPR.

51 GDPR, art 4 para 22.

52 For an exhaustive list see art 57 GDPR.

53 Although this is not explicitly stated in the GDPR, the distinction results from Recital 63 Directive 95/46/EC.

54 GDPR, art 58.

55 ibid para 1.

56 ibid para 3.

troller or processor or ordering the compliance with data subjects' requests to more severe ones like ordering the erasure of the data, imposing a ban on processing or suspending data flows to a third country.[57] Most importantly, the position of DPAs is strengthened by the fact that supervisory authorities are now clearly – in the GDPR itself as opposed to leaving it to be defined by the national laws - endowed with the power to impose administrative fines.[58] These can go as high as €20 million, or for undertakings - up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[59]

During the long legislative process, which precluded the adoption of the GDPR, one of the main points of discussion concerned exactly the powers of DPAs and the way in which these should be divided among supervisory authorities in the process of their cooperation under the one-stop-shop mechanism, which will be discussed below.

3. A Structured Way of Cooperation for DPAs under the One-Stop-Shop

Under Directive 95/46/EC, a company doing business in several Member States has to deal and comply with the national rules as implemented and interpreted by various DPAs, each competent for supervising the processing activities of the same company. This situation is not only burdensome for businesses in the EU but also detrimental for the rights of the data subjects. It leads to a lack of harmonisation in the application of EU data protection rules by DPAs which have to act under different implementing laws of Directive 95/46/EC.

Under the new Regulation however such companies will have a single DPA as a contact point. If a company is conducting business in more than one Member State and has at least one establishment in the EU, it will have to deal with a single DPA (lead DPA). Under the new[60] 'one-stop-shop' mechanism, the lead DPA will coordinate the supervision of all the processing activities of that business throughout the EU, in collaboration with other 'concerned' DPAs.[61] Moreover, the Regulation now also sets out clear time frames and responsibilities for this model of collaboration between DPAs.

The one-stop-shop mechanism provides that in transnational matters the lead DPA will have to involve all concerned DPAs before adopting a measure. It has to communicate all relevant information as well as submit draft decisions to other concerned DPAs. Thus other DPAs are given the possibility to object to the submitted draft within a time frame of four weeks. If the lead DPA agrees to the possible objections of the other DPAs it will have to resubmit a draft decision for opinion within the shorter time frame of two weeks. After agreement has been reached, it is up to the lead DPA to adopt and notify the decision to the main or single establishment of the company and to inform the other concerned authorities as well as the European Data Protection Board (EDPB) - which will be discussed further, together with the consistency mechanism - and, if necessary, the authority of the complainant.

If such a decision concerns a complaint, the following three situations can be distinguished as regards its adoption and its notification to the relevant parties. Firstly, when a complaint is admitted and all DPAs agree on the decision, it shall be adopted by the lead DPA, which will also notify the company, whereas the local DPA shall inform the complainant. Secondly, if a complaint is rejected or dismissed, the local DPA of the complainant shall adopt the decision, notify the complainant and inform the controller. And thirdly, a complaint can be only partially dismissed or rejected. In such a case the responsibility for taking action is shared between the lead and the local DPA. For the part of the complaint which is re-

57 ibid para 2.

58 GDPR, art 53 para 1(b).

59 GDPR, art 83 paras 4 and 5.

60 The one-stop-shop has triggered a lot of debate during the negotiation process. Intensive discussions revolved around the issue of division of powers between DPAs and how the cooperation should work in practice. The main questions were whether the competence of the lead DPA should be exclusive or not with regard to other DPAs and whether this exclusivity should concern all or only some of the powers DPAs are endowed with.
As initially proposed by the European Commission, the one-stop-shop had a more conflictive character as it was supposed to offer a solution in cases when DPAs did not manage to come to an agreement as regards the adoption of a certain measure with a transnational impact. At the end of the institutional trilogue however, the GDPR provided for a one-stop-shop that relies on the consensus of the DPAs. For conflictual situations between DPAs the Regulation foresees a consistency mechanism. If DPAs do not manage to come to an agreement, consistency will be triggered, so that the question of exclusivity of powers under the one-stop-shop does not raise issues any longer. See also Andra Giurgiu, Gertjan Boulet and Paul De Hert, 'EU's One-Stop-Shop Mechanism: Thinking Transnational' (2015) 137 Privacy Laws and Business, International Report 16-17.

61 GDPR, art 60.

jected, the responsibility to adopt that part of the decision, notify the complainant and inform the controller or processor belongs to the local DPA of the complainant. In this case the lead DPA is responsible for adopting the part of the decision that concerns actions with regard to the controller or processor, for his notification as well as for informing the complainant. It is generally the responsibility of the controller or processor to ensure the decision is implemented in all establishments involved in the processing and to inform the lead DPA of the measures it has taken.[62]

The Regulation also provides for a derogation from the application of the one-stop-shop, by setting up an urgency procedure for exceptional circumstances when a DPA considers that it is urgent to act so as to protect the interests of data subjects.[63]

4. Mandatory Consistency and the European Data Protection Board as a Gatekeeper in Matters with a Transnational Impact

The new consistency mechanism is a fundamental pillar, which together with co-operation and mutual assistance is meant to ensure a harmonized application of the Regulation throughout the Union in cases of cross-border relevance. A central actor in this scheme, aside from the concerned and lead DPAs, is the EDPB.[64] It replaces the current A29 WP group, and unlike its predecessor, will actually have legal personality as well as the power to adopt binding decisions. This makes the EDPB, unlike the A29 WP, a significantly stronger player in the enforcement of EU data protection rules.

The consistency mechanism is explicitly mandatory in two situations. Consistency is compulsory when a DPA plans to adopt a measure intended to produce legal effects in relation to processing operations that substantially affect a significant number of data subjects in several Member States. The Regulation lists in Article 64(1) a number of clearly defined measures for the adoption of which a DPA has to submit a draft decision to the EDPB, requesting its prior opinion. These measures concern for example the adoption of a list of processing operations that require a data protection impact assessment or the approval of binding corporate rules. When expressly mandatory, consistency is also a precondition for the lawfulness of these measures.[65] For these cases the Regulation does not explicitly give the EDPB direct binding powers. It states however that when a DPA does not follow the opinion of the EDPB any authority concerned or the Commission may communicate the matter to the European Data Protection Board[66] thus triggering consistency and indirectly giving the EDPB the final word.

In the second situation listed in Article 65(1) of the GDPR, consistency fulfils the role of a dispute resolution mechanism, in which the EDPB functions as a dispute resolution body. When the concerned DPAs cannot reach an agreement under the one-stop-shop mechanism or when there are conflicting views on which of the concerned supervisory authorities is competent for the main establishment (lead DPA), consistency should be triggered and the EDPB should intervene with binding decisions.

The Regulation provides however that as long as a matter is of general application or produces legal effects in more than one Member State, any supervisory authority (regardless of competence), the Chair of the EDPB or the Commission can request that a matter is dealt with under the consistency mechanism.[67]

As regards the procedural aspects, EDPB decisions are adopted either by a simple majority of its members for the list of mandatory cases mentioned in Article 64(1)[68] or by two-third majority when the EDPB functions as a dispute resolution body[69]. The decisions have to be notified to the concerned DPAs and to the Commission as well as be published on the EDPB website. To ensure proximity[70] to the data subject, the EDPB decisions have to be adopted by the lead, respectively by the concerned DPA, 'without undue delay and at the latest by one month' after their notification by the EDPB and notified to the relevant

62 GDPR, art 60 para 10.

63 GDPR, art 60 para 11 and art 66 GDPR.

64 GDPR, arts 68-76.

65 GDPR, Recital 138.

66 GDPR, art 65 para 1(c).

67 GDPR, art 64 para 2.

68 ibid para 3.

69 GDPR, art 65 para 2.

70 Proximity refers to the possibility for 'individual data subjects to have redress before a DPA within the Member State where they reside and to have access to justice in this same Member State, directly and upon appeal against a decision of this DPA', see Hijmans (n 5) 387.

parties following the general procedure as foreseen for the one-stop-shop[71]. They can be challenged by bringing an action for annulment before the CJEU under the conditions of Article 263 TFEU.[72]

In view of the procedure, one might conclude that the EDPB has the final word in actually all cases in which individual DPAs might disagree. This could call into question the matter of sovereignty and independence of national DPAs. As already pointed out by one author 'where the EDPB uses these [binding] powers, the national DPAs are no longer sovereign to ensure the control of the EU rules on data protection'.[73] As a consequence, DPAs might tend to avoid 'outsourcing' their powers to the EDPB and try to solve the issues through cooperation within the one-stop-shop mechanism rather than triggering consistency.

Given its binding powers it could be furthermore questioned, like the same author pointed out, whether the EDPB still qualifies as a structured network of national authorities rather than as a DPA within the meaning of Article 16(2) TFEU and Article 8(3) Charter. In this latter case it could be argued that the EDPD has to fulfil the requirements of independence as laid down in the CJEU case law just like a national DPA.[74]

The aim of the Regulation to create the same level of data protection all over the EU through the direct applicability of the GDPR with the strong position of the EDPB might also raise issues of a possible race 'towards' the bottom. This could especially be the case for countries with a strong data protection culture forced to succumb to perhaps more moderate opinions of the EDPB that would ensure consistency at the cost of having a lower level or protection. This might be the price that will have to be paid for harmonisation through a regulation instead of having a directive which allows more flexibility in its transposition by Member States.

71 GDPR, art 65 para 6.

72 GDPR, Recital 143.

73 Hijmans (n 5) 386.

74 ibid 381.

75 A29 WP, *Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)*, WP 236 (2 February 2016) 2.

76 See also Paul de Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (July 2016) International Data Privacy Law 1-14.

III. Conclusions: Stronger and More 'European' DPAs as Guardians of Consistency?

The application of the already outdated data protection rules of Directive 95/46/EC has hitherto been 'stretched' in order to cope with an era of ubiquitous computing. It was high time for this new piece of legislation, better suited to address the challenges of the current data processing realities, to step in. The Regulation is definitely not a total game changer, as it is still relying in many ways on the current Directive, but it does bring significant innovations within the data protection landscape for all the actors involved. The main worry expressed is how these changes will affect companies and data subjects. However, one cannot answer this question without examining the way in which DPAs will work in the future under the new rules. While first analysing the drawbacks of the current Directive 95/46/EC with a view to the relevant CJEU case-law, this article pointed out the existing problems under the current framework before examining if and to what extent these are mended by the GDPR.

The new competences and powers of DPAs under the GDPR are definitely putting national data protection authorities in a stronger position to enforce EU data protection law. The enlarged scope of application of the Regulation, a clear set of powers for DPAs, the one-stop-shop and the consistency mechanism coupled with DPAs' possibility to apply high fines in cases of infringements will ensure a higher and more consistent level of protection of EU residents in relation to both EU and non-EU based companies. The A29 WP refers in its action plan for the implementation of the GDPR to a 'brand new governance model' [75], consisting of distributed governance built on three pillars namely, national DPAs, their cooperation and the EDPB for ensuring consistency.

The recent CJEU jurisprudence under Directive 95/46/EC already tackled some important issues as regards applicable law as well as competences and powers of DPAs. Here the Court confirmed a wide scope of application of EU data protection law according to the 'effects principle' rather than mere territoriality, especially with regard to non-EU companies.[76] This principle is however not absolute and necessitates a case-by-case assessment. Some essential questions, such as the applicable law to an EU-based company operating in several Member States, are still

unclear.[77] Is it only the law of the State of the headquarters of the company acting as a controller or also the laws of the other Member States where the company has establishments, a problem not clarified in *Weltimmo*.[78]

The majority of the questions examined by the CJEU in its latest jurisprudence under the old and for the Internet era unfitted Directive 95/46/EC have been envisaged and solved by the new GDPR. Non-EU companies conducting business in the EU and processing data of EU residents will in future fall under EU data protection law and EU DPAs will have clear competence. Internet-enabled cross-border data processing is better addressed through one single EU-wide applicable Regulation under which several 'concerned' DPAs will have the duty to cooperate using the one-stop-shop mechanism. If they don't manage to come to an agreement, consistency can be triggered with the possible involvement of the EDPB as a 'consistency gatekeeper'[79].

However, as promising as the new provisions sound in theory, the future practical application of the enforcement rules in a consistent and effective manner will prove to be essential. Concern was expressed that consensual decision-making, involving all concerned DPAs, 'does not necessarily guarantee the most prompt and hence, effective response'.[80] Although a legitimate fear, we consider that the Regulation addresses this problem by setting clear and fixed deadlines which DPAs will have to respect when taking action. Conversely, under the current Directive 95/46/EC, cooperation took place on an informal level, providing DPAs with no clear institutionalized framework under which they could force a timely response from their peers when dealing with transnational matters.

Aside from the issue concerning the practical functionality of DPA cooperation, the new rules also raise concerns as regards more subtle issues such as that of independence and sovereignty of national DPAs under the Regulation.

We have seen that already under Directive 95/46/EC, DPAs have a hybrid position in between national law and EU law. Under the new Regulation, they become even more 'European' and thus more trapped between their own national rules and the EU law. This becomes even clearer when DPAs have to implement EDPB decisions. They are liable before national courts for decisions they are not sovereign in taking[81]. The A29 Working Party raised the concern already in 2012, that consistency should be applied 'only there where it is necessary' and that it 'should not encroach upon the independence of national supervisory authorities and should leave the responsibilities of the different actors where they belong'.[82]

Since the adoption of Directive 95/46/EC, DPAs have acted as the main guardians of the rights of individuals and will continue to do so under the new GDPR. As such, they will be responsible for monitoring and enforcing compliance with the new data protection rules of the Regulation. The effectiveness of DPAs will have a direct impact on the level of protection of citizen's rights as well as on the day-to-day business of companies and will thus play a significant role in the success of the GDPR. It is therefore also important to acknowledge and highlight the need of making sure that DPAs benefit from adequate resources in terms of staffing and financial means so as to be able to successfully carry out their missions.

---

77 As regards the missed opportunity by the CJEU to address the possible application of several national laws depending on the various stages of processing see also Cole and Giurgiu (n 32) 313.

78 See also A29 WP, *Update of Opinion 8/2010 on applicable law* (n 11).

79 Paul de Hert, Vangelis Papakonstantinou, *The new General Data Protection Regulation: Still a sound system for the protection of individuals?*, in Computer Law & Security Review 36/2016, p 193.

80 Hijmans (n 5) 386.

81 With regard to the issue of independence of DPAs see also Hijmans (n 5) 311, 343-344 and 380.

82 A29 WP, *Opinion 01/2012 on the data protection reform proposals*, WP 191 (23 March 2012) 20.