(FUTURE) INTERACTION BETWEEN DATA PROTECTION AUTHORITIES AND NATIONAL HUMAN RIGHTS INSTITUTIONS[*]

by Peter J. Hustinx[**]

1. INTRODUCTION

In line with Directive 95/46/EC, all EU Member States have national authorities that monitor compliance with data protection laws. However, the way in which the Directive has been implemented in national laws varies considerably. This has resulted in discrepancies and deficiencies that have been highlighted by the EU Agency for Fundamental Rights, and also in recent case law of the European Court of Justice. In January 2012, the European Commission presented a package of proposals with the aim to update and reinforce the current legal framework for data protection. This review will also have an impact on the scope for useful interaction between data protection authorities and national human rights institutions.

The emergence of the right to the protection of personal data ("data protection") as a separate fundamental right - closely related to the right to respect for private life, but with its own special characteristics - is a typical feature of the European human rights landscape. While similar legislation developed in other regions of the world - based on theories of privacy, fair information processing, consumer protection, or just on the need to create adequate conditions for economic growth - the developments in Europe have been shaped by the early belief that the growth of the Information Society would have such an impact on the exercise of existing fundamental rights and freedoms of citizens that a more proactive and systematic approach was necessary.

The first steps were taken in the context of the Council of Europe. This resulted in the adoption in 1981 of a Convention on Data Protection, also known as Convention 108, with basic principles for the processing of personal data in automated or otherwise structured data files.[1] The term "data protection" was defined as the protection of fundamental rights and freedoms of natural persons, *in particular* their right to privacy, with respect to the processing of personal data.[2] The Convention therefore goes beyond the scope of Article 8 of the European Convention on Human Rights (ECHR),[3] and applies, in principle, to all personal data, regardless of whether the right to privacy is at stake. The principles of Convention 108 provide for substantive requirements for data controllers, some specific rights for data subjects, and arrangements for institutional oversight, enforcement and international cooperation. The Convention has been ratified by more than 40 member states, including all EU Member States.

---

[*] Published in: "National Human Rights Institutions in Europe - Comparative, European and International Pesrpectives", Jan Wouters and Katrien Meuwissen (eds.), Cambridge 2013, p. 157-172.

[**] Mr Hustinx is European Data Protection Supervisor (EDPS). Contact: edps@edps.europa.eu; Website: www.edps.europa.eu

[1] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981 (further: Convention 108).

[2] Convention 108, Art. 1.

[3] Article 8 'Rights to respect for private and family life:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

When Convention 108 was implemented into national law, it quickly became clear that the general wording of its provisions allowed widely divergent national laws on data protection. At the same time, the development of an Information Society required more harmonisation and consistency among national laws than the Convention could provide. This caused the EU to become involved, eventually leading to the adoption of the Data Protection Directive 95/46/EC, which took the Convention as its starting point, but also specified it in different ways, inter alia requiring supervision and enforcement by one or more data protection authorities acting in complete independence.[4]

The next step in this development was the adoption of the EU Charter of Fundamental Rights in 2000,[5] initially as a political document. Although largely based on the ECHR, it also contained some innovations, such as the recognition of a right to the protection of personal data (Article 8), in addition to the right to respect for private and family life (Article 7). Article 8 explicitly mentions some of the main elements of the right to the protection of personal data, as further developed in Directive 95/46/EC:

> **Protection of personal data**
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

The final step was the entry into force of the Lisbon Treaty, at the end of 2009,[6] which turned the Charter into a binding document,[7] and also inserted a horizontal legal basis for legislation on data protection, no longer dependent on the needs of the internal market, but reflecting the nature of data protection as a fundamental right, among the general principles of the Union.[8] This confirmed a legal development of several decades.

2. INDEPENDENT SUPERVISION

The existence of data protection authorities has been a standard feature of European data protection law from the beginning, but it has taken some time before the principle of *independent* supervision developed into a constitutional principle. Article 8 of the Charter provides for it now, as we have just seen, and Article 16 TFEU does the same in very similar terms. Article 28 of Directive 95/46/EC, as we will see,[9] goes in more details on the subject.

---

[4] 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, *OJL* 281/31, 23 November 1995. See especially its Article 28.

[5] Charter of Fundamental Rights of the European Union (2000/C 364/01), *OJL* 364/1, 18 December 2000 (further: the Charter).

[6] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (2007/C 306/01), *OJL* 306/1, 17 December 2007.

[7] Consolidated Version of the Treaty on European Union, *OJL* C 115/19, 9 May 2008 (further: TEU). See Article 6.

[8] Consolidated Version of the Treaty on the Functioning of the European Union, *OJL* C 115/47, 9 May 2008 (further: TFEU). See Article 16.

[9] See *infra* section 2.

In retrospect, it is surprising to see that, in spite of experience in Germany, Sweden and France, the concept of a "data protection authority" played only a very limited role in the Council of Europe's Convention 108, when it was concluded in 1981. The central obligation of each Party in Article 4 of the Convention was to take 'the necessary measures in its domestic law to give effect to the basic principles for data protection' set out in the Convention. Article 10 provides that each Party must establish 'appropriate sanctions and remedies' for violations of these basic principles. The explanatory report clearly mentioned the need to guarantee *"effective protection"*, but left the way in which this should happen for each Party to decide.[10] The existence of supervisory authorities is only mentioned as a feature of national laws. The drafters of the Convention were obviously reluctant to impose this on all Parties as a basic legal requirement.

This situation changed with adoption of the EU Data Protection Directive 95/46. Article 28 of the Directive introduced an obligation for each Member State to have one or more supervisory authorities responsible for ensuring compliance, and 'acting with complete independence'. Recital 62 underlined that 'the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data'. The words '*acting* with complete independence' were a compromise formula, chosen to ensure some flexibility, but it was difficult to see how "complete independence" could exist without sufficient institutional safeguards. This turned out highly relevant in a case before the ECJ involving Germany, to which we will return.[11]

Article 28 of the Directive also provides that supervisory authorities should have certain powers, such as consultative powers, investigative powers, effective powers of intervention, the power to engage in legal proceedings or bring violations to the attention of judicial authorities, the power to deal with complaints, etc. This seems to assure them a central position. However, they do not decide in last resort, and their decisions may be appealed to the courts.

The adoption of the Directive has led to an Additional Protocol to Convention 108, which basically takes up all elements of Article 28 of the Directive.[12] The preamble of this Additional Protocol clearly states that 'supervisory authorities, exercising their functions in complete independence, are an element of the effective protection of individuals with regard to the processing of personal data'. The explanatory report even concludes that data protection supervisory authorities 'have become an essential component of the data protection supervisory system in a democratic society'.[13] This report also puts a lot of emphasis on the notion of "effective protection" and the role of supervisory authorities in ensuring it.[14]

This all means in the light of Article 8 of the Charter and Article 16 TFEU, that the principle of "independent supervision" and the existence of "independent supervisory authorities" have developed, at least at the European level, into a

[10] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Explanatory Report, para. 60.
[11] See *infra*, section 4.
[12] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, ETS No.: 181, Strasbourg, 8 November 2001 (entry into force: 1 July 2004).
[13] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, ETS No.: 181, Explanatory Report, Preamble, para. 5.
[14] *Ibidem*, Preamble; para 8; para 13; para. 16; para. 17; para. 24.

constitutional element of the right to data protection in a democratic society. This is based on their mission to "ensure compliance" and closely linked to the notion of "effective protection".

3. DIVERSITY AND DEFICIENCIES

In accordance with Directive 95/46/EC, all EU Member States have national authorities that monitor compliance with data protection laws. However, the way in which the Directive has been implemented in national laws varies considerably. This has resulted in discrepancies and deficiencies that have also been highlighted in a report published in May 2010 by the EU Agency for Fundamental Rights (FRA).[15]

As a first comment, it should be noted that some diversity is unavoidable and simply a result of different legal traditions in the Member States. The Directive leaves Member States a large margin to decide on the nature and structure of a supervisory authority in ways that fit them best. Data protection authorities (DPA) therefore exist in different forms and shapes: large or small commissions, single commissioners, elected or appointed, either or not by a national government or parliament, and so on.

However, as the FRA clearly highlighted in its report, the current diversity among Member States goes far beyond the unavoidable, and also involves rather serious deficiencies.[16] The key findings of the report have been summarised by FRA as follows:[17]

> **Rights Awareness**
> 7 in every 10 respondents to a recent Eurobarometer survey were not aware that there was a data protection authority in their country
> **Limited powers**
> Data protection authorities are often not equipped with full powers of investigation and intervention or the capacity to give legal advice or engage in legal proceedings.
> **Lack of compliance**
> In many Member States there is a widespread disregard for the basic duty to register with the data protection authority prior to engaging in data processing operations.
> **Lack of independence**
> The lack of independence from the government of several of the data protection authorities in the EU presents a major problem for their credibility. Legislative reform modifying the nomination/appointment procedure (...) could rectify the problem of lack of independence.
> **Lack of financial resources and staff**
> Data protection authorities in [a number of Member States] are unable to carry out the entirety of their tasks because of the limited economic and human resources available to them.
> **Lack of sanctions and compensation**
> Legislative reform is needed to give data protection authorities an active role in procedures which lead to sanctions and compensation. Where data protection authorities have the relevant powers, they need the resources to effectively use them. (...)

[15] See: FRA, 'Data Protection in the European Union: the role of National Data Protection Authorities, Strengthening the fundamental rights architecture in the EU II', Luxembourg, Publications Office of the European Union, 2010.
[16] *Ibidem*, p. 42-45.
[17] See the website of FRA: http://fra.europa.eu/en/publication/2012/data-protection-european-union-role-national-data-protection-authorities.

The FRA report also mentions some examples of good practices,[18] but both the diversity and deficiencies exposed in the report remain rather worrying.

4. REQUIREMENT OF "COMPLETE INDEPENDENCE"

The European Court of Justice has meanwhile also expressed itself on the requirement of "complete independence" in Article 28 of Directive 95/46.

The Court's judgment of 9 March 2010 in Case-518/07 (*Commission v Federal Republic of Germany*) dealt with the authorities in Germany that supervise the processing of personal data by *non-public bodies* at the regional level. In all States, those authorities were subject to State scrutiny. The European Commission, in Court supported by the European Data Protection Supervisor (EDPS), took the position that "complete independence" in Article 28 of Directive 95/46 means that a supervisory authority must be free from *any* outside influence, regardless from whom.[19] The Federal Republic of Germany felt that it only required *functional* independence - i.e. from those subject to supervision - but did not exclude State scrutiny.[20]

The ECJ decided in favour of the Commission – basically saying that "complete independence" means "complete independence". However, its analysis contains some interesting messages. The Court's starting point is that the meaning of the requirement must be found on the basis of the wording of Article 28 and the aims and scheme of the Directive.

As to the *wording* of Article 28, the Court mentions that in relation to a public body, "independence" normally means 'a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure'.[21] Moreover, according to the Court, the additional emphasis on "*complete* independence" implies 'a decision-making power independent of any direct or indirect external influence on the supervisory authority'.[22]

As to the *objectives* of Directive 95/46, the Court considers that it aims to harmonise national law in an area where the free movement of personal data is liable to interfere with the right to privacy, and seeks to ensure a high level of protection of fundamental rights and freedoms with respect to the processing of personal data. The supervisory authorities provided for in Article 28 are the 'guardians of those fundamental rights and freedoms', and their existence is considered as 'an essential component' of the protection of individuals with regard to the processing of personal data.[23] The Court continues as follows (emphasis added):

> '24. In order to guarantee that protection, the supervisory authorities must ensure a fair balance between, on the one hand, observance of the fundamental right to private life and, on the other hand, the interests requiring free movement of personal data. Furthermore, under Article 28(6) of Directive 95/46, the different national authorities are called upon to cooperate with one another and even, if necessary, to exercise their powers at the request of an authority of another Member State.
>
> 25. The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and

[18] FRA, loc. sit. *supra* note 15, pp. 47-48.
[19] European Court of Justice, Judgment, Case-518/07 *Commission v Federal Republic of Germany*, 9 March 2010, para. 15.
[20] *Ibidem*, para. 16.
[21] *Ibidem*, para. 18.
[22] *Ibidem*, para. 19.
[23] *Ibidem*, para. 23.

must be interpreted in the light of that aim. It was established not to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions. It follows 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*, and not of the influence only of the supervised bodies.'

As to the *scheme* of the Directive, the Court draws a parallel between Directive 95/46 on one hand, and Regulation 45/2001,[24] which applies to EU institutions and established the EDPS, on the other. Article 28 of the Directive should be interpreted in accordance with Article 44 of the Regulation requiring 'complete independence', but also stating that the EDPS 'may neither seek nor take instructions from anybody'.[25] The Court thus concludes that Article 28 should be interpreted:

> '30. […] as meaning that the supervisory authorities responsible for supervising the processing of personal data [...] must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data.'

The Court then considers whether State scrutiny is consistent with the requirement of independence as defined above, and arrives at the conclusion that this is *not* the case. It also points out:

> '36. [...] that the mere risk that the scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks.'

After further analysis, the Court concluded that by making the authorities responsible for monitoring the processing of personal data by non-public bodies in the different *Länder* subject to State scrutiny, the Federal Republic of Germany had failed to fulfil its obligations under Article 28 of Directive 95/46.

Thus, the Court not only decided that "complete independence" involves the freedom from *any* external influence, but also gave some interesting messages about the role of supervisory authorities: their independence is intended to ensure the *effectiveness* of their mission, and they should act *objectively* and *impartially*, and be

[24] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJL* L 8/1, 12 January 2001.

[25] *Ibidem*, Article 44 'Independence':

1. The European Data Protection Supervisor shall act in complete independence in the performance of his or her duties.
2. The European Data Protection Supervisor shall, in the performance of his or her duties, neither seek nor take instructions from anybody.
3. The European Data Protection Supervisor shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any other occupation, whether gainful or not.
4. The European Data Protection Supervisor shall, after his or her term of office, behave with integrity and discretion as regards the acceptance of appointments and benefits.

free to strike a *fair balance* between observance of the fundamental right to private life and other interests.

We will come back to the question what all this could mean for the interaction between data protection authorities and national human rights institutions.[26] First, it is useful to take a look at the main lines of the current review of the EU legal framework for data protection.

5. PROPOSALS FOR A NEW EU LEGAL FRAMEWORK FOR DATA PROTECTION

5.1. Drivers of EU Review

Why is this review taking place? This is basically for three reasons. The *first* reason is that there is a need to update the current framework, and more specifically Directive 95/46 which is still the key element of the framework. And "updating" means in this case, most of all, ensuring its continued effectiveness in practice. When the Directive was adopted, the Internet barely existed, and we now live in a world where continuous data processing is becoming increasingly relevant, so we also need stronger safeguards that deliver good results in practice. The challenges of new technologies and globalisation really require some imaginative innovation to ensure a more effective protection.

The *second* reason is that the current framework has given rise to increasing diversity and complexity, also in a much wider sense, if only for the reason that a Directive is transposed into national law – that is its nature – and we now have ended up with 27 versions of the same basic principles. That is simply too much, and translates into costs, but also a loss of effectiveness. In other words, there is a need to scale up harmonisation, and make the system not only stronger and more effective in practice, but also more consistent. This will lead to a reduction of *unhelpful* diversity and complexity.

The *third* reason has to do with the new legal framework of the EU. The Lisbon Treaty has put a strong emphasis on fundamental rights. Among them, as we have seen, a special provision on the protection of personal data in Article 8 of the Charter of fundamental rights, and a new horizontal legal basis in Article 16 TFEU providing for comprehensive protection in all EU policy areas, regardless of whether it relates to the internal market, law enforcement, or almost any other part of the public sector.

So, the review of the framework is all about stronger, more effective, more consistent, and more comprehensive protection of personal data.

If we now look at what has been put on the table, we see a package of at least two main proposals: a Directive for - briefly put - the law enforcement area,[27] and a directly binding Regulation for what is now still Directive 95/46, applying to the commercial areas and the public sector, other than law enforcement.[28] The proposed Directive is generally considered as not satisfactory, as its level of protection is substantially lower

[26] See *infra* section 6.

[27] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, Brussels, 25 January 2012.

[28] 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 final, Brussels, 25 January 2012 (further: Proposal for a General Data Protection Regulation).

than in the proposed Regulation. However, in the present context, it is also less relevant.

5.2. Continuity and change

If we now focus on the proposed Regulation[29], there are some main messages which need to be kept in mind.

The first one is that – in spite of all innovation – there is a lot of continuity. All basic concepts and principles that we have now will continue to exist, subject to some clarification and some innovation.[30] Where the real innovation comes in, it is mainly about "making data protection more effective in practice". This implies, as we will see, a strong emphasis on implementation of principles, and on enforcement of rights and obligations, to ensure that protection is delivered in practice.

At the same time, the Regulation provides for simplification and reduction of costs. The prior notification of processing operations to the DPA has been eliminated. This is only required in situations of specific risks.[31] The Regulation also provides for a one-stop-shop for companies with establishments in different member states.[32] This involves the introduction of a "lead DPA", which is the DPA of the main establishment who will be first responsible, in close cooperation with other competent DPAs.[33]

A directly binding Regulation will of course also bring much greater harmonisation – in principle: one single applicable law in all Member States – and greater consistency. In itself, this will also bring an important simplification and reduction of costs for companies operating in different member states.

Finally, the proposed Regulation has a general scope: it will apply both in the private and in the public sector. This is completely consistent with the situation under the present Directive 95/46. The possibility of a systematic distinction in this Directive between the public and the private sector was explicitly considered in the 1990's and rejected.

This approach is reinforced by the fact that Article 8 of the EU Charter provides for an explicit recognition of the right to the protection of personal data, and that Article 16 TFEU provides an explicit horizontal legal basis for the adoption of rules on the protection of personal data, both at EU level and in the Member States, when they are acting within the scope of EU law.

5.3. Substance of the Proposed Regulation

If we now come to the substance of the Regulation, it strengthens the roles of the key players: the data subject, the data controller, and the data protection authorities. A brief look at the first two is important to better understand the role of the DPA.

5.3.1. Data subject

[29] Further references are to this Regulation (see footnote 28).
[30] An example of innovation is that there is now a stronger emphasis on data minimisation: i.e. not more data than strictly necessary (Article 5 sub c). Another example is the recognition of "Privacy by Design" as a general principle (Article 23).
[31] See Article 34 on prior consultation, for instance where impact assessment indicates a high degree of specific risks.
[32] See Explanatory Memorandum, p. 12, para 3.4.6.2.
[33] See Article 51.2.

The first perspective could also be seen as enhancing 'user control': the possibility for data subjects to influence what happens to their personal data. The current rights of the data subject have been confirmed, but strengthened and extended. It will also be easier to exercise these rights in practice.[34]

The requirement of consent has been clarified: *when* you need it, it needs to be real and robust consent.[35] There is also a stronger right to object.[36] There are stronger means to ensure that the rights of the data subject are respected in practice. There is more emphasis on transparency.[37] There is a provision introducing a collective action, not a class action in US style, but still for organisations acting on behalf of their members or constituencies.[38]

There is also much talk about the "right to be forgotten", but at further analysis, it is basically an emphasis on deleting data when there is not a good enough reason to keep them.[39] The right to data portability[40] is basically also a specification of the present right to require a copy of personal data, in a particular format.

5.3.2. Data controller

The biggest change is a much greater emphasis on real responsibility of responsible organisations. Responsibility is not a concept that only comes at the end, when something has gone wrong. Instead, it comes as an obligation to develop good data management in practice. This appears in language such as *taking all appropriate measures to ensure compliance*, and *verifying and demonstrating that these measures continue to be effective.* [41]

This is one of the major shifts. It also implies that the burden of proof is in many cases on the responsible organisation, i.e. to demonstrate that there is an adequate legal basis, that consent is real consent, and that measures continue to be effective. This means that DPAs will be more involved 'ex-post', and will be able to require from data controllers adequate evidence of their compliance status.

The Regulation also provides for a number of specific requirements, such as the need for a privacy impact assessment,[42] the keeping of documentation,[43] and the appointment of a data protection officer.[44] These are important elements of good data management in organisations. Data protection officers can help organisations to comply and also act as contact points for DPAs.

Some of those provisions, especially on documentation, are overly detailed and would require some modification to make them more appropriate. Some exceptions in the

[34] Articles 15-17
[35] Article 4 sub 8 and Article 7.
[36] Article 19.
[37] Article 5 sub a and Articles 11 and 14.
[38] Article 73.2 and Article 76.1
[39] Article 17
[40] Article 18
[41] Article 22
[42] Article 33
[43] Article 28
[44] Articles 35-37

same provisions may not be fully justified. A better balance in this part of the proposal may in fact solve both problems.

A general provision on security breach notification is also included.[45] EU law now provides for such a notification only in the case of telecommunication providers.

5.3.3. Supervision and enforcement

A third main emphasis in the Regulation is on more effective supervision and enforcement by DPAs. The safeguards for complete independence of data protection authorities have been strengthened fully in line with the ECJ judgment in the case *Commission vs Germany*.[46]

The Regulation also provides for regulators with strong enforcement powers in all Member States, involving both investigation powers, ordering powers and imposition of administrative sanctions.[47] Presently, under Directive 95/46/EC, Member States have a very large discretion, as result of which quite a few DPAs now have weak powers and none has the full range of powers as laid down in the proposed Regulation.

Administrative fines of millions of euros - competition size fines – catch a lot of attention, but the message is: if this is important, it should be dealt with accordingly. This will drive "data protection" higher on the agenda of corporate boardrooms, which is welcome and likely to result in better data management and better delivery of data subject's rights.

International cooperation among data protection authorities is also strongly encouraged and facilitated, including mutual assistance and joint operations.[48] The introduction of a "lead authority" for companies with multiple establishments[49] is welcome, but this lead authority will not be acting on its own, but as part of a network of close cooperation with other competent authorities. This EU wide dimension is also explicitly mentioned among the tasks of data protection authorities.[50]

Very important in this perspective is the introduction of a consistency mechanism in the context of a European Data Protection Board,[51] which is to be built on the basis of the present group of EU data protection authorities ("Article 29 Working Party").[52] This mechanism, involving all independent authorities, will ensure consistent outcomes of supervision and enforcement in all Member States. Its secretariat will be provided by the EDPS.[53]

5.3.4 Global Privacy

[45] Articles 30-32
[46] Article 47
[47] Articles 53 and 79
[48] Articles 55-56
[49] See *infra* section 5.2
[50] See Article 46.1
[51] Articles 57-58 and 64-72
[52] This Working Party, established by Article 29 of Directive 95/46/EC, has been active since 1996 and is now composed of representatives of all national DPAs and the EDPS. It gives advice to the European Commission, either or not at its request, and develops "soft law" guidance on different matters, but with substantial authority in practice.
[53] Article 71

A final element is the wider international dimension of the Regulation, in two ways. The scope of the Regulation has been clarified and extended. These provisions now apply not only to all processing in the context of an establishment in the EU, but also when from a third country, goods or services are delivered on the European market, or when the behaviour of Europeans is being monitored online.[54]

This is a reality on the Internet nowadays. At the same time, it is a realistic approach that builds on an increasing synergy of thinking on data protection around the world. It means that European DPAs will be more and more involved in issues with international dimensions, including third countries outside the EU.[55]

International cooperation is therefore also developing among data protection authorities in a wider context – e.g. between the Federal Trade Commission in the US and DPAs in the EU – in a global network (GPEN). This will make it better possible to deal with global actors on the Internet.[56]

6. INTERACTION BETWEEN DPAS AND NHRIS

So, what does all this mean for the interaction between data protection authorities and national human rights institutions?

First of all, there is an important time factor. The Commission's proposals are presently under discussion in the Council and the Parliament. This is obviously not a matter of months. Present estimates are that we will see some conclusions in the course of 2013, probably under the Irish Presidency. In any case by 2014, the proposed Regulation may well be adopted, subject to some improvements on various details. On that basis, the Regulation is likely to enter into force in 2016. In other words, the Member States and all other stakeholders will have time to prepare for transition. Until then, the current framework, and national laws implementing it, will continue to apply, only subject to partial amendments, for instance to respond to ECJ case law.

For the present, this means that some diversity will continue to exist among national data protection authorities. However, a similar diversity exists for national human rights institutions. The "Paris Principles" discussed elsewhere in this publication,[57] lay down certain standards concerning the competences, responsibilities, composition, and methods of operation of the national institutions, but no specific structure, mandate, or shape is required. This means that the way in which DPAs and NHRIs are now interacting, may be quite different in the various Member States, depending on prevailing conditions, including political culture and other traditions.

So it may well be that in some Member States, data protection authorities, just like equality bodies and national ombudsmen, are among the key stakeholders of NHRIs, and also contribute actively to their agenda, while this may not be the case in other Member States. In those cases where there is a lively interaction between data protection authorities and national institutions, it is likely that cooperation is closest in

[54] See Article 3

[55] Recent examples are investigations against Google by the French CNIL, and against Facebook by the Irish Data Protection Commissioner, in which most other European DPAs have been involved, as well as competent authorities in Canada and the US.

[56] This is based on a growing convergence of data protection principles and practices around the world, involving not only formal standards, developed by OECD, Council of Europe, EU, APEC, ISO and other organisations, but also other instruments, such as codes of conduct, binding corporate rules, and so on.

[57] See in particular G. De Beco, 'Assessment of the Paris Principles and the ICC Sub-Committee on Accreditation', Chapter 11 in this volume.

the general field of awareness raising and education, as these activities are less dependent on formal powers and procedures. In the case of complaint handling and inspection, a lively interaction would seem to be somewhat less likely. However, it may well be that national institutions have done useful work in exposing structural problems or specific issues that could be the subject of a complaint or an inspection, or even that they act as the initiating party of a complaint, either or not in the general interest.

In the future, all this may continue to be the case, but the key difference will be that the current great diversity among national DPAs has disappeared or substantially been reduced. This will be the result of *directly* binding requirements in the Regulation, not only for the independent position, but also for the tasks and powers of supervisory authorities. There may well be national rules providing further details, particularly on the composition and internal structure of supervisory authorities, but the main elements will be visible in the Regulation and have direct EU wide application.

Much more than now, the situation will be that national DPAs will not only be competent to play their role within the scope of their own jurisdiction, but also be an integral part of EU wide cooperation on cross border and other common issues, and moreover be part of an EU wide consistency mechanism that is designed to ensure consistent outcomes. It is no doubt a paradox that institutional safeguards for independence will be stronger, and that at the same time arrangements are made to avoid unhelpful diversity among independent authorities. Finding the right balance in this area will of course be a key concern. Even if the appropriate legal arrangements have been made in the Regulation, once it is adopted, there will always be a need to develop effective procedures in practice. The existing Article 29 Working Party, as the current platform of DPAs in the EU, could do much in preparing the way into this direction.

For the interaction with NHRIs, this will probably not lead to major changes, but most certainly to a more consistent and predictable landscape. In any case, it would seem that the requirement of "complete independence" and the need to avoid "any external influence" will not prevent national DPAs from entering into appropriate relationships with NHRIs, especially in the general field of awareness raising and education, with a view to giving both more impact. Indeed, under the Paris Principles, similar standards will apply to the national institutions. It will thus be up to both parties to develop and structure mutual relationships to their best common benefit.

One additional element may still need to be considered. If the Regulation is adopted in its present form, it will also allow ‘any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data’ and which has been properly constituted according to national law, the ‘right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects’, if it considers that a data subject's rights under the Regulation have been infringed as a result of the processing of personal data.[58] A similar right will apply in the context of court proceedings.[59] This will give more scope for collective actions, also in Member States where this possibility does not yet exist, and thus contribute to a more active enforcement of data protection rules. It remains to be seen to which extent this would allow NHRIs or their constituencies to become more directly engaged in data protection issues than they have been so far.

[58] Proposal for a General Data Protection Regulation , *supra* note 28, Art. 73.
[59] Proposal for a General Data Protection Regulation , *supra* note 28, Art. 76.