Opinion of the European Data Protection Supervisor

on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"

Table of Content

Opinion of the European Data Protection Supervisor

on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Articles 7 and 8,

Having regard to 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[1],

Having regard to 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[2], and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION

A. GENERAL PART

1. Introduction

1.1. A first and general assessment

1. On 4 November 2010, the Commission adopted a Communication entitled "A comprehensive approach on personal data protection in the European Union" (the "Communication")[3]. The Communication was sent to the EDPS for consultation. The EDPS welcomes the fact that he was consulted by the Commission in accordance with Article 41 of Regulation (EC) No. 45/2001. Already before the adoption of the Communication the EDPS was given the possibility to give informal comments. Some of these comments have been taken into account in the final version of the document.

2. The Communication intends to lay down the Commission's approach for the review of the EU legal system for the protection of personal data in all areas of the Union's activities,

1 OJ 1995, L 281/31.
2 OJ 2001, L 8/1.
3 COM (2010) 609 final.

taking account, in particular, of the challenges resulting from globalisation and new technologies.[4]

3. The EDPS welcomes the Communication in general, as he is convinced that a review of the present legal framework for data protection in the EU is necessary, in order to ensure effective protection in a further developing information society. Already in his Opinion of 25 July 2007 on the Implementation of the Data Protection Directive[5] he concluded that in the longer term, changes of Directive 95/46/EC seem unavoidable.

4. The Communication represents an important step towards such a legislative change which in turn would be the most important development in the area of EU data protection since the adoption of Directive 95/46/EC which is generally considered as the main cornerstone of data protection within the European Union (and wider within the European Economic Area).

5. The Communication gives the right framework for a well targeted review, also because it identifies - generally spoken - the main issues and challenges. The EDPS shares the view of the Commission that a strong system of data protection will still be needed in the future, based on the notion that existing general principles of data protection are still valid in a society which undergoes fundamental changes due to rapid technological developments and globalisation. This requires reviewing existing legislative arrangements.

6. The Communication rightly emphasises that the challenges are enormous. The EDPS fully shares this statement and underlines the consequence that the proposed solutions should be correspondingly ambitious and should enhance the effectiveness of the protection.

1.2. Aim of the opinion

7. This opinion assesses the proposed solutions in the Communication on the basis of these two criteria: ambition and effectiveness. Its perspective is positive in general. The EDPS supports the Communication, but is at the same time critical on aspects where in his view more ambition would lead to a more effective system.

8. The EDPS aims to contribute with this opinion to the further development of the legal framework on data protection. He looks forward to the Proposal of the Commission which is expected by mid 2011 and hopes that his suggestions will be taken into account in the wording of this proposal. He also notes that the Communication seems to exclude certain areas, such as data processing by EU institutions and bodies, from the general instrument. If the Commission would indeed decide to leave out certain areas at this stage – which the EDPS would regret - he urges the Commission to commit itself to realise a fully comprehensive architecture within a short and specified timeframe.

1.3. The building blocks of this opinion

9. This opinion does not stand alone. It is based on earlier positions taken by the EDPS and by the European data protection authorities on various occasions. In particular, it must be underlined that in the already mentioned EDPS Opinion of 25 July 2007 some main

[4] See p. 5 of the Communication, first paragraph.

[5] EDPS Opinion of 25 July 2007 on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, OJ C 255, 27.10.2007, p. 1.

elements for future change were identified and developed.[6] It is also based on discussions with other stakeholders in the areas of privacy and data protection. Their contributions offered a very useful background for both the Communication and this opinion. In this regard, it can be concluded that there exists a level of synergy on how to improve effectiveness of data protection.

10. Another important building block of this Opinion is the document called 'The Future of Privacy', the Joint contribution of the Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation launched by the Commission in 2009 (the "WP document on the Future of Privacy").[7]

11. More recently, at a Press Conference on 15 November 2010, the EDPS gave his first reactions on the present Communication. This opinion elaborates the more general views brought forward during this Press Conference.[8]

12. Finally, this Opinion profits from a number of earlier EDPS Opinions, as well as from documents of the Article 29 Data Protection Working Party. References to those opinions and documents can be found in various places of this opinion, where relevant.

2. Context

13. The review of data protection rules occurs at a crucial historical moment. The Communication describes the context extensively and in a convincing way. Based on this description the EDPS identifies the four main drivers determining the environment in which the review process takes place.

14. The first driver is technological development. Today's technology is not the same as when Directive 95/46 was conceived and adopted. Technological phenomena like cloud computing, behavioural advertising, social networks, road toll collecting and geo-location devices profoundly changed the way in which data are processed and pose enormous challenges for data protection. A review of European data protection rules will have to address these challenges effectively.

15. The second driver is globalisation. The progressive abolition of trade barriers has given businesses an increasing worldwide dimension. Cross border data processing and international transfers have tremendously increased over the past years. Furthermore, data processing has become ubiquitous due to Information and Communication Technologies: internet and cloud computing allowed delocalised processing of large quantities of data on a worldwide scale. The last decade also witnessed an increase in international police and judicial activities to fight terrorism and other forms of international organised crime, supported by an enormous exchange of information for law enforcement purposes. All this calls for a serious consideration of how personal data protection can be ensured

---

6 In particular (see point 77 of the opinion): no need to change existing principles, but a clear need for other administrative arrangements; the wide scope of data protection law applicable to all use of personal data should not change; data protection law should allow a balanced approach in concrete cases and should also allow data protection authorities to set priorities; the system should fully apply to the use of personal data for law enforcement purposes, although appropriate additional measures may be necessary to deal with special problems in this area.

7 Document WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). Its main message is that a legislative change is a good opportunity to clarify some key rules and principles (e.g. consent, transparency), introduce some new principles (e.g. privacy by design, accountability), strengthen the effectiveness by modernising the arrangements (e.g. by limiting existing notification requirements) and include all into one comprehensive legal framework (incl. police and judicial cooperation).

8 The Speaking Points for the Press Conference are available on the EDPS website, at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf.

effectively in the globalised world without substantially hampering international processing activities.

16. The third driver is the Lisbon Treaty. The entry into force of the Lisbon Treaty marks a new era for data protection. Article 16 TFEU not only contains an individual right of the data subject, but also provides a direct legal basis for a strong EU-wide data protection law. Furthermore, the abolition of the pillar structure obliges the European Parliament and Council to provide for data protection in all areas of EU law. In other words, it allows for a comprehensive legal framework for data protection applicable to the private sector, the public sector in the Member States and the EU institutions and bodies. The Stockholm Programme[9] consistently states in this regard that the Union must secure a comprehensive strategy to protect data within the EU and in its relations with other countries.

17. The fourth driver is represented by parallel developments taking place in the context of international organisations. There are various ongoing debates focussing on the modernisation of the current legal instruments for data protection. It is important to mention in this respect the current reflections undertaken in relation to the future revision of Convention 108 of the Council of Europe[10] and of the OECD Privacy Guidelines.[11] Another important development regards the adoption of international standards on the protection of personal data and privacy, which might possibly lead to the adoption of a binding global instrument on data protection. All these initiatives deserve full support. Their common goal should be ensuring effective and consistent protection in a technologically driven and globalised environment.

3. Main perspectives

3.1. Data protection fosters trust and must support other (public) interests

18. A strong framework for data protection is the necessary consequence of the importance given to data protection under the Lisbon Treaty, in particular in Article 8 of the Charter of the Fundamental Rights of the Union and Article 16 TFEU, as well as the strong link with Article 7 of the Charter.[12]

19. However, a strong framework for data protection also serves wider public and private interests in an information society with ubiquitous data processing. Data protection fosters trust, and trust is an essential component of the well functioning of our society. It is essential that arrangements for data protection are construed in a way that they - as much as possible - actively support rather than hamper other legitimate rights and interests.

20. Important examples of other legitimate interests are a strong European economy, the security of individuals, as well as the accountability of governments.

21. Economic development in the EU goes hand in hand with the introduction and the marketing of new technologies and services. In the information society the emergence and successful deployment of information and communications technologies and services

---

9 The Stockholm Programme – An open and secure Europe serving and protecting citizens, OJ C115, 04/05/2010, p. 1-38, at p. 10.

10 Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data, ETS No 108, 28.1.1981.

11 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, published on www.oecd.org.

12 This importance of data protection and the link with privacy in the Charter were underlined by the Court of Justice in its Judgment of 9 November 2010, Joint Cases C-92/09 and C-93/09, *Schecke*, not yet published in ECR.

depends on trust. If people do not trust ICT, these technologies are likely to fail.[13] And people will only trust ICT if their data are efficiently protected. Therefore, data protection should be an integral part of technologies and services. A strong framework for data protection fosters the European economy, provided that this framework is not only strong but also tailored in the right way. Further harmonisation within the EU and minimisation of administrative burdens are in this perspective essential (see Chapter 5 of the opinion).

22. Much has been said in recent years about the need for balancing privacy and security, especially in relation to instruments for data processing and exchange in the area of police and judicial cooperation.[14] Data protection was quite often wrongly characterised as an obstacle to fully protecting the physical security of individuals[15], or at least as an unavoidable condition to be respected by law enforcement authorities. However, this is not the whole story. A strong framework of data protection can sharpen and strengthen security. On the basis of principles of data protection - when applied well - controllers are obliged to ensure that information is accurate and up to date, and that superfluous personal data that are not necessary for law enforcement are eliminated from the systems. One can equally point to obligations to implement technological and organisational measures to ensure the security of systems such as protecting systems against unauthorised disclosure or access, as developed in the field of data protection.

23. Respecting principles of data protection may further ensure that law enforcement authorities operate under the rule of law which triggers trust in their behaviour and therefore fosters in a wider sense trust in our societies. The case law developed under Article 8 of the European Convention of Human Rights ensures that police and judicial authorities can process all data relevant for their work, but not in an unlimited manner. Data protection requires checks and balances (see on police and justice Chapter 9 of the opinion).

24. In democratic societies governments are accountable for all their activities, including for their use of personal data for the different public interests they serve. This varies from publication of data on the internet for reasons of transparency, to the use of data as a support of policies in areas like public health, transport or taxation, or the surveillance of individuals for law enforcement purposes. A strong data protection framework allows governments to respect their responsibilities and to be accountable, as part of good governance.

3.2. Consequences for the legal framework on data protection

3.2.1. Further harmonisation is needed

25. The Communication rightly identified that one of the essential shortcomings of the current framework is that it leaves too much discretion to the Member States in the implementation of the European provisions into national law. Lack of harmonisation has a number of negative consequences in an information society where the physical borders between the Member States are less and less relevant (see Chapter 5 of the opinion).

3.2.2. General principles of data protection still remain valid

---

13 See EDPS Opinion of 18 March 2010 on promoting trust in the Information Society by fostering data protection and privacy, OJ C 280, 16.10.2010, p. 1, para 113.

14 See e.g. EDPS Opinion of 10 July 2009 on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen, OJ C 276, 17.09.2009, p. 8

15 Security is a wider notion than physical security, but as an illustration of the arguments at stake it is here used in its more limited sense.

26. A first and more formal reason why the general principles of data protection should and could not be changed is of a legal nature. These principles are laid down in Council of Europe Convention 108 which is binding on all the Member States. This Convention is the basis of data protection in the EU. Moreover, some of the main principles are explicitly mentioned in Article 8 of the Charter of the Fundamental rights of the Union. Changing of these principles would thus require changing the Treaties.

27. However, this is not the full story. There are also substantial reasons not to change the general principles. The EDPS strongly believes that an information society can and should not function without an adequate protection of privacy and personal data of individuals. When more information is being processed, also better protection is needed. An information society where abundant amounts of information about everyone are being processed needs to be built on the concept of control by the individual, in order to allow him or her to act as an individual and to use his freedoms in a democratic society such as the freedoms of expression and speech.

28. Furthermore, it is difficult to imagine control of the individual without obligations on controllers to limit processing in accordance with principles of necessity, proportionality and purpose limitation. It is equally difficult to imagine control by the individual in the absence of recognised data subjects' rights, such as the rights of access, rectification, erasure or blocking of data.

3.2.3. Fundamental rights perspective

29. The EDPS underlines that data protection is recognised as a fundamental right. This does not mean that data protection should always *prevail* over other important rights and interests in a democratic society, but it does have consequences for the nature and scope of the protection that must be given under an EU legal framework, so as to ensure that data protection requirements are always *adequately* taken into account.

30. These main consequences can be defined as follows:
    - Protection must be effective. A legal framework must provide for instruments that make it feasible for individuals to exercise their rights in practice.
    - The framework must be stable over a long period.
    - Protection must be given under all circumstances and not depend on the political preferences in a certain timeframe.
    - Limitations to the exercise of the right may be needed, but they must be exceptional, duly justified and never affect the essential elements of the right itself.[16]

    The EDPS recommends that the Commission take these consequences into account when proposing legislative solutions.

3.2.4. New legislative arrangements are needed

31. The Communication rightly concentrates on the need for strengthening the legislative arrangements for data protection. In this context, it makes sense to recall that in the WP document on the Future of Privacy[17] the Data Protection Authorities emphasised the need

[16] See also the EDPS Opinion of 25 July 2007 on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, para 17, which builds on the case law of the European Court of Human Rights and the Court of Justice.

[17] See footnote 7.

for stronger roles for the different actors in the field of data protection, notably the data subjects, the data controllers and the supervisory authorities themselves.

32. There seems to be a wide consensus amongst stakeholders that stronger legislative arrangements - taking into account technological developments and globalisation - are the key towards ambitious and effective data protection also in the future. As already indicated in point 7, these are the criteria for the assessment of the EDPS of any proposed solutions.

3.2.5. Comprehensiveness as a conditio sine qua non

33. As recalled in the Communication, Directive 95/46 applies to all personal data processing activities in Member States in both the public and the private sectors, with exception of activities which fall outside the scope of former Community law[18]. Whilst this exception was needed under the former Treaty, this is no longer the case after the entry into force of the Lisbon Treaty. Moreover, the exception is contrary to - the text and in any event the spirit of - Article 16 TFEU.

34. According to the EDPS, a comprehensive legal instrument for data protection including police and judicial cooperation in criminal matters must be seen as one of the main improvements a new legal framework can bring. It is a *conditio sine qua non* for effective data protection in future.

35. The EDPS highlights the following arguments in support of this statement:
    - The distinction between activities of the private sector and of the law enforcement sector is blurring. Private sector entities may process data which are ultimately used for law enforcement purposes (example: PNR data[19]), whilst in other cases, they are required to keep data for law enforcement purposes (example: Data Retention Directive[20]).
    - There is no fundamental difference between police and judicial authorities and other authorities delivering law enforcement (taxation, customs, anti-fraud, immigration) subject to Directive 95/46.
    - As accurately described in the Communication, the data protection legal instrument currently applicable to police and judicial authorities (Framework Decision 2008/977[21]) is inadequate.
    - Most Member States have implemented Directive 95/46 and Convention 108 in their national legislations, making them applicable also to their police and judicial authorities.

36. Including police and justice in the general legal instrument would not only offer more guarantees to citizens but also make the task of police authorities easier. Having to apply various sets of rules is cumbersome, needlessly time-consuming and stands in the way of international cooperation (see further Chapter 9 of the opinion). This also argues for

---

18 This opinion will mainly focus on the former 3rd pillar (police and judicial cooperation in criminal matters), since the former 2nd pillar is not only a more complicated area of EU law (as also recognised by Article 16 TFEU and Article 39 EU), but also to a lesser extent relevant for data processing.

19 See e.g. Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM (2010) 492 final.

20 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105/ 54).

21 Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350/60).

including the processing activities by national security services, in so far as this is possible under the current state of EU law.

3.2.6. Technological neutrality

37. The period since the adoption of Directive 95/46 in 1995 can be characterised as technologically turbulent. New technological developments and appliances are introduced on a frequent basis. In many cases this has led to fundamental changes in the way personal data of individuals are being processed. The information society can no longer be considered as a parallel environment where individuals can participate on a voluntary basis, but has become an integrated part of our day to day lives. Just as an example, the concept of an Internet of things[22] establishes links between physical objects and on line information related to them.

38. Technology will further develop. This has its consequences for the new legal framework. It must be effective for a greater number of years, and at the same time not hamper further technological developments. This requires that the legal arrangements are technologically neutral. However, the framework must also bring more legal certainty for companies and for individuals. They must understand what is expected from them and be able to exercise their rights. This requires that the legal arrangements are precise.

39. According to the EDPS, a general legal instrument for data protection must be formulated in a technologically neutral way, as far as possible. This implies that the rights and obligations of the various actors are to be formulated in a general and neutral way so as to remain, in principle, valid and enforceable irrespective of the technology chosen for processing personal data. There is no other choice, given the fast pace of technology advancements nowadays. The EDPS suggests introducing new 'technologically neutral' rights on top of the existing principles of data protection which could have a specific importance in the rapidly changing electronic environment (see mainly Chapters 6 and 7).

3.2.7. Long term: Legal certainty for a longer period

40. Directive 95/46 has been the central piece of data protection in the EU for the last 15 years. It was implemented in the laws of the Member States and applied by the different actors. Over the years the application has profited from practical experiences and from further guidance given by the Commission, the Data Protection Authorities (on the national level and in the framework of the Article 29 Working Party) and national and European Courts.

41. It is good to emphasise that these developments need time and that - especially since we deal with a general framework giving effect to a fundamental right - this time is needed to create legal certainty and stability. A new general legal instrument needs to be drafted with the ambition that it will be able to create legal certainty and stability for a longer period, keeping in mind that it is very difficult to predict how technology and globalisation will further develop. In any event, the EDPS fully supports the aim to create legal certainty for a longer period, comparable to the perspective of Directive 95/46. In short, where technology develops at a fast pace, the law must be stable.

3.2.8. Short term: Make better use of existing instruments

[22] As defined in 'Internet of things - An action plan for Europe', COM (2009) 278 Final.

42. In the short term, it is essential to ensure the effectiveness of existing legislative arrangements, in the first place by concentrating on enforcement, at national and at EU level (see Chapter 11 of this opinion).

B. ELEMENTS OF A NEW FRAMEWORK

4. Comprehensive approach

43. The EDPS fully supports the comprehensive approach on data protection which is not only the title but also the point of departure of the Communication and necessarily includes the extension of the general rules on data protection to police and judicial cooperation in criminal matters.[23]

44. However, he also notes that the Commission does not intend to include all data processing activities in this general legal instrument. In particular, data processing by EU institutions, bodies, offices and agencies will not be included. The Commission only states that it 'will assess the need to adapt other legal instruments to the new general data protection framework'.

45. The EDPS has a clear preference for including processing on the EU level in the general legal framework. He reminds that this was the original intention of the former Art 286 EC which mentioned data protection for the first time on the level of the Treaty. Article 286 EC simply stated that legal instruments on the processing of personal data would apply to the institutions as well. More importantly, one legal text avoids the risk of discrepancies between provisions and would be most suitable for data exchange between the EU level and the public and private entities in the Member States. It would also avoid the risk that, after modifying Directive 95/46, there is no political interest any more in amending Regulation 45/2001 or to give this modification sufficient priority to avoid discrepancies in dates of entry into force.

46. The EDPS urges the Commission - in case it would conclude that the inclusion of processing at the EU level in the general legal instrument would not be feasible - to commit itself to propose an adaptation of Regulation 45/2001 (not to 'assess the need') within the shortest possible timeframe and preferably by the end of 2011.

47. It is equally important that the Commission ensures that other areas do not stay behind, in particular:
    - Data protection in the Common Foreign and Security Policy, on the basis of Article 39 TEU.[24]
    - Sector specific data protection regimes for EU bodies such as Europol, Eurojust and for large scale information systems, in so far as they need to be adapted to the new legal instrument.
    - The ePrivacy Directive 2002/58, in so far as it needs to be adapted to the new legal instrument.

48. Finally, a general legal instrument for data protection may and probably must be complemented by additional sectoral and specific regulations, for instance for police and

---

[23] See p. 14 of the Communication and Section 3.2.5 of this opinion.

[24] See also EDPS Opinion of 24 November 2010 on the Communication from the Commission to the European Parliament and the Council concerning the EU Counter-Terrorism Policy: main achievements and future challenges, point 31.

judicial cooperation, but also in other areas.[25] Where needed and in conformity with the principle of subsidiarity, those additional regulations should be adopted at EU level. Member States may draw up additional rules, in specific areas where this is justified (see 5.2).

5: Further harmonisation and simplification

5.1. The need for harmonisation

49. Harmonisation is of paramount importance for EU data protection law. The Communication correctly stressed that data protection has a strong internal market dimension, as it must ensure the free flow of personal data between Member States within the internal market. However, the level of harmonisation under the present Directive has been judged as less than satisfactory. The Communication recognises that this is one of the main recurrent concerns of stakeholders. In particular, stakeholders stress the need to enhance legal certainty, reduce the administrative burden and ensure a level playing field for economic operators. As the Commission rightly notes, this is particularly the case for data controllers established in several Member States and obliged to comply with the (possibly diverging) requirements of national data protection laws.[26]

50. Harmonisation is not only important for the internal market but also with a view to ensuring adequate data protection. Article 16 of the TFEU provides that "everyone" has the right to the protection of personal data concerning them. In order for this right to be effectively respected, an equivalent level of protection must be guaranteed throughout the EU. The WP document on the Future of Privacy highlighted that several provisions relating to data subjects' positions have not been implemented or interpreted uniformly in all Member States[27]. In a globalised and interconnected world, these divergences could undermine or limit the protection of individuals.

51. The EDPS believes that further and better harmonisation is one of the principal objectives of the review process. The EDPS welcomes the Commission's commitment to examine the means to achieve further harmonisation of data protection at EU level. However, he notes with some surprise that the Communication does not put forward at this stage any concrete options. He therefore indicates himself a few areas where greater convergence is most urgent (see 5.3). Further harmonisation in these areas should not only be achieved by reducing the margin of manoeuvre for national law, but also preventing incorrect implementation by Member States (see also Chapter 11) and ensuring more consistent and coordinated enforcement (see also Chapter 10).

5.2. Reducing the margin of manoeuvre in the implementation of the Directive

52. The Directive contains a number of provisions that are broadly formulated and that therefore leave significant room for diverging implementation. Recital 9 of the Directive explicitly confirms that Member States are given a certain margin of manoeuvre and that, within this margin, disparities could arise in the implementation of the Directive. Several provisions have been implemented differently by Member States, including some crucial provisions[28]. This situation is not satisfactory and greater convergence should be sought.

---

25 See also WP document on the Future of Privacy (footnote 7), points 18-21.

26 Communication, p. 10.

27 See WP document on the Future of Privacy (footnote 7), point 70. The document refers in particular to liability provisions and the possibility to claim immaterial damages.

28 Some divergent approaches also exist with regard to manual data.

53. This does not mean that diversity should be excluded outright. In certain areas flexibility might be needed in order to preserve justified specificities, important public interests or the institutional autonomy of the Member States. According to the EDPS, room for divergence between the Member States should be limited in particular to the following specific situations:
    - Freedom of expression: under the present framework (Article 9), Member States may provide for exemptions and derogations in relation to the processing of data carried out for journalistic purposes or for the purpose of artistic or literary expression. This flexibility appears well placed, subject of course to limits in the Charter and ECHR, given the different traditions and cultural differences that may exist in this field across Member States. However, this would not stand in the way of a possible update of the current Article 9 in the light of developments on the Internet.
    - Specific public interests: under the present framework (Article 13), Member States may adopt legislative measures to restrict the scope of the obligations and rights when such a restriction constitutes a necessary measure to safeguard important public interest, such as national security, defence, public security, etc. This competence of Member States remains justified. However, where possible, the interpretation of the exceptions should be further harmonised (see Section 9.1). In addition, the current scope for exception to Article 6(1) appears unduly wide.
    - Legal remedies, sanctions and administrative procedures: a European framework should determine the main conditions, but under the current state of EU law the determination of sanctions, legal remedies, procedural rules and the modalities of inspections as applicable at national level must be left to Member States.

5.3. Areas for further harmonisation

54. Definitions (Article 2 of Directive 95/46). Definitions are the cornerstone of the legal system and should be uniformly interpreted in all Member States, with no margin of implementation. Divergences have arisen under the present framework, like for example as to the notion of controller[29]. The EDPS suggests adding further items to the current list in Article 2 in order to provide for more legal certainty, such as anonymous data, pseudonymous data, judicial data, data transfer and data protection officer.

55. Lawfulness of processing (Article 5). The new legal instrument should be as precise as possible with regard to the core elements determining the lawfulness of data processing. Article 5 of the Directive (as well as its Recital 9), mandating Member States to determine more precisely the conditions under which the processing is lawful, may thus be no longer needed in a future framework.

56. Grounds for data processing (Article 7 and 8). The definition of the conditions for data processing is an essential element of any data protection legislation. Member States should not be allowed to introduce additional or modified grounds for processing or to exclude any. The possibility of derogations should be excluded or limited (particularly with regard to sensitive data[30]). In a new legal instrument the grounds for data processing should be clearly formulated, thereby reducing the margin of appreciation in the implementation or enforcement. In particular, the notion of consent may need to be further specified (see Section 6.5). Moreover, the ground based on the legitimate interest of the data controller (Article 7, letter (f)), gives way to widely diverging interpretations, due to

[29] See WP 29 Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169).

[30] Article 8(4) and (5) currently authorize under certain conditions Member States to provide for further derogations with regard to sensitive data.

its flexible nature. Further specification is needed. Another provision that possibly must be specified is Article 8(2)(b), allowing the processing of sensitive data necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law[31].

57. Data subject rights (Articles 10-15). This is one of the areas in which not all elements of the Directive have been consistently implemented and interpreted by Member States. Data subjects' rights are a central element for an effective data protection. As a consequence, the room for manoeuvre should be substantially reduced. The EDPS recommends that the information provided to data subjects by the controller should be uniform across the EU.

58. International transfers (Articles 25-26). This is an area which has given rise to widespread criticism because of the lack of a uniform practice throughout the EU. Stakeholders criticised that the Commission's decisions on adequacy are interpreted and implemented very differently by the Member States. Binding Corporate Rules (BCRs) are a further element where the EDPS recommends further harmonisation (see Chapter 9).

59. National Data Protection Authorities (Article 28). National DPAs are subject to widely diverging rules in the 27 Member States, particularly with regard to their status, resources and powers. Article 28 has partly contributed to this divergence because of its lack of precision[32] and should be further specified, in conformity with the Judgment of the European Court of Justice in Case C-518/07[33] (see further Chapter 10).

5.4. Simplification of the notification system

60. Notification requirements (Article 18-21 of Directive 95/46) are another field where Member States have so far been granted significant freedom. The Communication rightly recognises that a harmonised system would reduce costs as well as administrative burden for data controllers[34].

61. This is an area where simplification should be the main objective. The review of the data protection framework is a unique opportunity to further simplify and/or reduce the scope of the current notification requirements. The Communication recognises that there is a general consensus amongst stakeholders that the current system of notifications is rather cumbersome and does not provide, in itself, added value for the protection of individuals' personal data.[35] The EDPS thus welcomes the Commission's commitment to explore different possibilities for the simplification of the current notification system.

62. In his view, the point of departure of this simplification would be a shift from a system where notification is the rule, save as otherwise provided (i.e., "exemption system"), to a more targeted system. The exemption system proved to be inefficient, as it was implemented in an inconsistent way across Member States.[36] The EDPS suggests considering the following alternatives:

---

31 See, in this regard, the Commission's First Report on the implementation of the Data Protection Directive, cited above, p. 14.

32 WP document on the Future of Privacy, para 87.

33 Case C-518/07, *Commission v. Germany*, not yet published in ECR.

34 Communication, p. 10.

35 Communication, p. 10

36 Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplifications and the role of the data protection officers in the European Union, WP 106, 2005, p. 7.

- Limit the obligation to notify to specific kinds of processing operations entailing specific risks (these notifications could trigger further steps such as prior checking of the processing).
- A simple registration obligation requiring data controllers to register (as opposed to extensive registration of all data processing operations).

In addition, a standard pan-European notification form could be introduced so as to ensure harmonised approaches with regard to the information requested.

63. The review of the current notification system should be without prejudice to improving prior-checking obligations for certain processing obligations likely to present specific risks (such as large scale information systems). The EDPS would favour the inclusion in the new legal instrument of a non-exhaustive list of cases where such prior-checking is required. Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by EU institutions and bodies provides a useful model for this purpose[37].

5.5. A Regulation, not a Directive

64. Finally, the EDPS believes that the review process is also an opportunity to reconsider the type of legal instrument for data protection. A Regulation, a single instrument which is directly applicable in the Member States, is the most effective means to protect the fundamental right to data protection and to create a real internal market where personal data can move freely and where the level of protection is equal independently of the country or the sector where the data are processed.

65. A Regulation would reduce room for contradictory interpretations and for unjustified differences in the implementation and the application of the law. It would also reduce the importance of determining the law applicable to processing operations within the EU, which is one of the most controversial aspects of the present system (see Chapter 9).

66. In the area of data protection a Regulation is all the more justified, since
    - Article 16 TFEU has upgraded the right to the protection of personal data to the Treaty level and envisages – or even mandates - a uniform level of protection of individual throughout the EU.
    - Data processing takes place in an electronic environment where internal borders between the Member States have become less relevant.

67. The choice for a Regulation as a general instrument allows, where necessary, provisions directly addressed to Member States where flexibility is needed. It also does not influence the competence of Member States to adopt additional rules for data protection, where needed, in conformity with EU law.

6. Strengthening the rights of individuals

6.1. The need for strengthening the rights

68. The EDPS fully supports the Communication where it proposes strengthening individuals' rights, since existing legal instruments do not fully deliver the effective protection that is needed in an increasingly complex digitalized world.

[37] See Article 27 of the Regulation, OJ 2001, L 8/1.

69. On the one hand, the development of a digitalized world entails a sharp growth in the collection, use and further transfer of personal data in an extremely complex and non transparent way. Individuals are often not aware or do not understand how this happens, who collects their data, nor how to exercise control. An illustration of this phenomenon is the monitoring by ad network providers of individuals' web browsing activities, using cookies or similar devices, for the purposes of targeted advertising. When users visit web sites, they do not expect that an out of sight third party logs such visits and creates users' records, based on information revealing their life style, or what they like or dislike.

70. On the other hand, the development stimulates individuals pro-actively sharing their personal information, for example on social networks. Increasingly young people are part of a social network and interact with their peers. It is doubtful whether (young) people, are aware of the breadth of their disclosure and of the long term effects of their actions.

6.2. Increasing transparency

71. Transparency is of paramount importance in any data protection regime, not only because of its inherent value but also because it enables other data protection principles to be exercised. Only if individuals know about the data processing, they will be able to exercise their rights.

72. Several provisions in Directive 95/46 deal with transparency. Article 10 and 11 contain an obligation to give information to individuals about the collection of their personal data. Moreover, Article 12 recognizes the right to receive a copy of one's own personal data in an intelligible form (right of access). Article 15 recognises the right to have access to the logic on which automated decisions producing legal effects are made. Last but not least, Article 6.1(a) requiring the processing to be fair also entails a transparency requirement. Personal data cannot be processed for any hidden or secret reasons.

73. The Communication suggests adding a general principle of transparency. In reaction to this suggestion, the EDPS underlines that the notion of transparency is already an integral part of the present legal framework on data protection, albeit in an implicit way. This can be deduced from the various provisions dealing with transparency, as mentioned in the preceding paragraph. According to the EDPS, it could have added value to include an *explicit* principle of transparency, either or not linked to the existing provision of fair processing. This would increase legal certainty and also confirm that a controller should under all circumstances process personal data in a transparent way, not only on request or when a specific legal provision requires him to do so.

74. However, it is perhaps more important to reinforce the existing provisions dealing with transparency, such as the existing Articles 10 and 11 of Directive 95/46. Those provisions specify the information elements that must be provided, but are not precise on the modalities. More concretely, the EDPS suggests strengthening the existing provisions by:
    - A requirement for a controller to provide information on data processing in a manner which is easily accessible and easy to understand, and in clear and plain language[38]. The information should be clear, conspicuous and prominent. The provision could also encompass the obligation to ensure easy understanding of the information. This obligation would render illegal privacy policies which are opaque or difficult to understand.

[38] See Communication, p. 6.

- A requirement to render the information easily and directly to data subjects. The information should also be permanently accessible, and not after a very short time disappear from an electronic medium. This would help users to store and reproduce information in the future, enabling further access.

6.3. Support for an obligation to report security breaches

75. The EDPS supports the introduction of a provision on personal data breach notification in the general instrument, which extends the obligation which was included in the revised ePrivacy Directive for certain providers to all data controllers, as proposed in the Communication. Under the revised ePrivacy Directive the obligation only applies to providers of electronic communication services (providers of telephony (including VoIP) service and Internet access). Other data controllers are not covered by the obligation. The reasons that justify the obligation fully apply to data controllers other than providers of electronic communication services.

76. Security breach notification serves different purposes and aims. The most obvious one, highlighted by the Communication, is to serve as an information tool to make individuals aware of the risks they face when their personal data are compromised. This may help them to take the necessary measures to mitigate such risks. For example, when alerted of breaches affecting their financial information, individuals will be able, among other things, to change passwords or cancel their accounts. In addition, security breach notification contributes to the effective application of other principles and obligations in the Directive. For example, security breach notification requirements incentivize data controllers to implement stronger security measures to prevent breaches. Security breach is also a tool to strengthen the responsibility of data controllers and, more in particular to enhance accountability (see Chapter 7). Finally, it serves as a tool for the enforcement by DPAs. The notification of a breach to DPAs may lead to an investigation of the overall practices of a data controller.

77. The specific rules on security breach in the amended ePrivacy Directive were broadly discussed during the parliamentary phase of the legislative framework that preceded the adoption of the ePrivacy Directive. In this debate, the opinions of the Article 29 Working Party and EDPS were taken into consideration together with the views of other stakeholders. The rules reflect the views of different stakeholders. They represent a balance of interests: while the criteria triggering the obligation to notify are, in principle, adequate to protect individuals, they do so without imposing overly cumbersome, not useful requirements.

6.4. Reinforcing consent

78. Article 7 of the Data Protection Directive lists six legal bases for processing personal data. Consent of the individual is one of them. A data controller is allowed to process personal data to the extent in which individuals have given informed consent to have their data collected and further processed.

79. In practice, often users have limited control in relation to their data, particularly in technological environments. One of the methods that is sometimes used is implied consent, which is consent that has been inferred. It can be inferred from an action of the individual (e.g. the action consisting in using a web site is deemed as consenting to log user's data for marketing purposes). It can also be inferred from silence or inaction (not un-clicking a ticked box is deemed to be consent).

80. According to the Directive, for consent to be valid it must be informed, freely given and specific. It must be an informed indication of the individuals' wishes by which he signifies his agreement to personal data relating to him being processed. The way in which consent is given must be unambiguous.

81. Consent that has been inferred by an action and more particularly by silence or inaction is often not an unambiguous consent. However, it is not always clear what constitutes true, unambiguous consent. Some data controllers exploit this uncertainty by relying on methods not suitable to deliver true, unambiguous consent.

82. In light of the above, the EDPS supports the Commission on the need to clarify the limits of consent and to make sure that only consent that is construed in a solid way is taken as such. In this context, the EDPS suggests as follows[39]:
    - It could be considered to broaden the situations where express consent is required, currently limited to sensitive data.
    - Adopt additional rules for consent in the on-line environment.
    - Adopt additional rules for consent to process data for secondary purposes (i.e., the processing is secondary to the main processing or not an obvious one).
    - In an additional legislative instrument, either or not adopted by the Commission under Article 290 TFEU, determine the type of consent needed, for example, to specify the level of consent on the processing of data from RFID tags on consumer products or on other specific techniques.

6.5. Data portability and the right to be forgotten

83. Data portability and the right to be forgotten are two connected concepts put forward by the Communication to strengthen data subjects' rights. They are complementary to the principles already mentioned in the Directive, providing for a right for the data subject to object to the further processing of his/her personal data, and an obligation for the data controller to delete information as soon as it is no longer necessary for the purpose of the processing.

84. These two new notions have mostly added value in an information society context, where more and more data are automatically stored and kept for indefinite periods of time. Practice shows that, even if data are uploaded by the data subject himself, the degree of control he effectively has on his personal data is in practice very limited. This is all the more true in view of the gigantic memory the Internet represents today. Besides, from an economic perspective, it is more costly for a data controller to delete data than to keep them stored. The exercise of the rights of the individual therefore goes against the natural economic trend.

85. Both data portability and the right to be forgotten could contribute to shift the balance in favour of the data subject. The objective of data portability would be to give more control to the individual on his information, while the right to be forgotten would ensure that the information automatically disappears after a certain period of time, even if the data subject does not take action or is not even aware the data was ever stored.

86. More specifically, data portability is understood as the users' ability to change preference about the processing of their data, in connection in particular with new technology

[39] The WP 29 is currently working on an opinion on 'consent'. This opinion might lead to additional suggestions.

services. Increasingly, this applies to services that entail the storage of information, including personal data, such as mobile telephony and, services that store pictures, emails, and other information, sometimes using cloud computing services.

87. Individuals must easily and freely be able to change the provider and transfer their personal data to another service provider. The EDPS considers that existing rights set forth in Directive 95/46 could be reinforced by including a portability right in particular in the context of information society services, to assist individuals in ensuring that providers and other relevant controllers give them access to their personal information while at the same time ensuring that the old providers or other controllers delete that information even if they would like to keep it for their own legitimate purposes.

88. A newly codified "right to be forgotten" would ensure the deletion of personal data or the prohibition to further use them, without a necessary action of the data subject, but at the condition that this data has been already stored for a certain amount of time. The data would in other words be attributed some sort of expiration date. This principle is already affirmed in national court cases or applied in specific sectors, for instance for police files, criminal records or disciplinary files: under some national laws, information about individuals is automatically deleted or not to be further used or disseminated, especially after a fixed period of time, without need for a prior analysis on a case by case basis.

89. In this sense, a new "right to be forgotten" should be connected to data portability. The added value it would bring is that it would not require efforts or insistence from the data subject to have his data deleted, as this should be done in an objective and automated way. Only in very specific circumstances, where a specific need to keep data longer could be established, could a data controller be entitled to keep the data. That "right to be forgotten" would thus reverse the burden of proof from the individual to the data controller and constitute a "privacy by default" setting for the processing of personal data.

90. The EDPS considers that the right to be forgotten could prove especially useful in the context of information society services. An obligation to delete or not further disseminate information after a fixed period of time makes sense especially in the media or the internet, and notably in social networks. It would also be useful as far as terminal equipments are concerned: data stored on mobile devices or computers would be automatically deleted or blocked after a fixed period of time, when they are no more in the possession of the individual. In that sense the right to be forgotten can be translated in a "privacy by design" obligation.

91. In sum, the EDPS is of the opinion that data portability and the right to be forgotten are useful concepts. It could be worthwhile to include them in the legal instrument, but probably limited to the electronic environment.

6.6. Processing of personal data related to children

92. Under Directive 95/46 there are no particular rules regarding the processing of children's personal data. This does not recognise the need for a specific protection of children in specific circumstances, because of their vulnerability, and because it causes legal uncertainty, particularly in the following areas:
    - the collection of children's data and the way they must be informed about the collection;
    - the way children's consent is obtained. Because there are no specific rules on how to obtain children's consent and on the age under which children should be

considered as such, these subject are dealt with under national law, which differs from Member State to Member State[40];

- the way and conditions under which children or their legal representatives can exercise their rights under the Directive.

93. The EDPS considers that children's particular interests would be better protected if the new legal instrument contained additional provisions, specifically addressed to the collection and further processing of children's data. Such specific provisions would also provide legal certainty in this specific area and they would be to the benefit of data controllers who are currently exposed to different legal requirements.

94. The EDPS suggests including the following provisions in the legal instrument:
    - A requirement for information to be adapted to children insofar as this would make it easier for children to understand what it means when data from them are collected.
    - Other information requirements adapted to children, on the manner in which the information must be provided and possibly also on the content.
    - A specific provision protecting children against behavioural advertising.
    - The purpose limitation principle should be reinforced as far as children's data are concerned.
    - Some categories of data should never be collected from children.
    - An age threshold. Below such threshold, generally speaking information from children should be collected only with explicit and verifiable parental consent.
    - If parental consent is necessary, it would be necessary to establish rules on how to authenticate the age of the child, in other words, how to know that the child is a minor and how to verify parental consent. This is an area where the EU can draw inspiration from other countries such as the United States[41].

6.7. Collective redress mechanisms

95. Strengthening the substance of individuals' rights would be pointless, in the absence of effective procedural mechanisms to enforce such rights. In this context, the EDPS recommends the introduction in the EU legislation of collective redress mechanisms for breach of data protection rules. In particular, collective redress mechanisms empowering groups of citizens to combine their claims in a single action might constitute a very powerful tool to facilitate the enforcement of the data protection rules.[42] This innovation is also supported by the Data Protection Authorities in the WP document on the Future of Privacy.

96. In cases with smaller impact, it is unlikely that the victims of a breach of data protection rules would bring individual actions against the controllers, given the costs, delays,

---

40 Consent is usually linked to the age when children can enter into contractual obligations. This is the age when children are supposed to have reached a certain level of maturity. For example, Spanish law requires parental consent to collect children data for children who are not yet **14** years old. Above this age, children will be deemed to be able to consent. In the United Kingdom, the Data protection Act does not refer to a particular age or threshold. However, the UK Data protection Authority has interpreted that children **above 12** can provide consent. Conversely, children under **12** cannot provide consent and in order to obtain their personal data first it is necessary to obtain the permission of a parent or guardian.

41 In the US, COPPA requires operators of commercial websites or online services directed to children under 13 to obtain parental consent before collecting personal information and operators of commercial general audience websites to have actual knowledge that specific visitors are children.

42 See also EDPS Opinion of 25 July 2007 on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, OJ C 255, 27.10.2007, p. 10.

uncertainties, risks and burdens they would be exposed to. These difficulties could be overcome or substantially alleviated if a system of collective redress were in place, empowering the victims of breaches to bundle their individual claims in a single action. The EDPS would also favour the empowerment of qualified entities, such as consumer associations or public bodies, to bring actions for damages on behalf of victims of data protection breaches. These actions should be without prejudice to the right of data subject to bring individual actions.

97. Not only are collective actions important for ensuring full compensation or other remedial action; they also perform indirectly a deterrence enhancing function. The risk of incurring expensive collective damages in such actions would multiply the controllers' incentives to effectively ensure compliance. In this regard, an enhanced private enforcement by means of collective redress mechanisms would complement public enforcement.

98. The Communication does not take a position regarding this topic. The EDPS is aware of the ongoing debate at European level on the introduction of consumer collective redress. He is also conscious of the risk of excesses that these mechanisms may bring about on the basis of the experience in other legal systems. However, these factors do not constitute in his view sufficient arguments to reject or postpone their introduction in the data protection legislation, in light of the benefits that they would entail[43].

7. Strengthening the role of organisations/controllers

7.1. General

99. The EDPS is of the opinion that, in addition to reinforcing individuals' rights, a modern legal instrument for data protection must contain the necessary tools that enhance the responsibility of data controllers. More particularly, the framework must contain incentives for data controllers in the private or public sector to pro-actively include data protection measures in their business processes. These tools would in the first place be helpful because, as said before, technological developments resulted in a sharp growth in the collection, use and further transfer of personal data which heightens the risks for the privacy and protection of personal data of individuals which should be compensated in an effective way. In the second place, the current framework lacks - except in a few, well-defined provisions (see below) - such tools and data controllers may take a *reactive* approach to data protection and privacy, and only act after a problem has arisen. This approach is reflected in statistics that show poor compliance practices and data losses as recurring problems.

100. According to the EDPS, the existing framework is not enough to protect personal data effectively under present and future conditions. The higher the risks, the higher the need to implement concrete measures that protect information at a practical level and deliver effective protection. Unless these pro-active measures are *de facto* implemented, mistakes, mishaps and negligence are likely to continue, endangering individuals' privacy in this increasingly digital society. To achieve this, the EDPS proposes the following measures.

7.2. Reinforcing data controllers' accountability

101. The EDPS recommends inserting a new provision in the legal instrument requiring data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the legal instrument and demonstrate this on request.

[43] Some national laws already provide for similar mechanisms.

102. This type of provision is not entirely new. Article 6 (2) of the Directive 95/46 refers to the principles relating to data quality and mentions that "It shall be for the controller to ensure that paragraph 1 is complied with". Equally, Article 17 (1) requires data controllers to implement measures, of both a technical and organisational nature. However, these provisions have a limited scope. Inserting a general provision on accountability would stimulate controllers to put into place proactive measures in order to be able to comply with all the elements of data protection law.

103. A provision on accountability would have the consequence that data controllers are required to put in place internal mechanisms and control systems ensuring compliance with the principles and obligations of the framework. This would require, for example, involving the highest management in data protection policies, mapping procedures to ensure proper identification of all data processing operations, having binding data protection policies which should also be continually reviewed and updated to cover new data processing operations, complying with the principles of data quality, notice, security, access, etc. It would also require that controllers keep evidence to demonstrate compliance to authorities on request. Demonstrating compliance to the public at large should, in certain cases, also be made mandatory. This could be done for instance, by requiring controllers to include data protection in public (annual) reports, when such reports are mandatory on other grounds.

104. Obviously, the types of internal and external measures to be implemented must be appropriate and depend on the facts and circumstances of each particular case. It makes a difference whether a controller processes a few hundred customer records consisting merely of names and addresses or if he processes records of millions of patients, including their medical history. The same applies to the specific ways in which the effectiveness of the measures must be assessed. There is a need for scalability.

105. The general comprehensive data protection legal instrument should not lay down the specific requirements of accountability but only its essential elements. The Communication foresees certain elements to reinforce the responsibility of data controllers, which are very welcome. More particularly, the EDPS fully supports making data protection officers and privacy impact assessments mandatory, under certain threshold conditions.

106. Additionally, the EDPS recommends delegating powers to the Commission under Article 290 TFEU to supplement the basic requirements necessary to meet the accountability standard. Using these powers would enhance data controllers' legal certainty and harmonize compliance throughout the EU. In developing such specific instruments, the Article 29 Working Party and the EDPS should be consulted.

107. Finally, the concrete accountability measures to be implemented by data controllers could also be imposed by data protection authorities in the context of their enforcement powers. To do so, data protection authorities should be given new powers enabling them to impose remedial measures or sanctions. Examples should include setting up internal compliance programs, to implement privacy by design in specific products and services, etc. Remedies should only be imposed in so far as they are appropriate, proportionate and effective to ensure compliance with applicable and enforceable legal standards.

7.3. Privacy by design

108. Privacy by design refers to the integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data. According to the EDPS privacy by design is an element of accountability. Accordingly, data controllers would also be required to demonstrate that they had implemented privacy by design, where appropriate. Recently, the 32nd International Conference of Data Protection and Privacy Commissioners issued a resolution recognising privacy by design as an essential component of fundamental privacy protection.[44]

109. Directive 95/46 contains some provisions encouraging privacy by design[45], but does not recognize such obligation explicitly. The EDPS is pleased with the Communication's endorsement of privacy by design as a tool towards ensuring compliance with the data protection rules. He suggests including a binding provision setting forth a "privacy by design" obligation, which could build on the wording of Recital 46 of Directive 95/46. More specifically, the provision would explicitly require data controllers to implement technical and organization measures, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to ensure the protection of personal data and prevent any unauthorized processing.[46]

110. On the basis of such a provision data controllers would be required - inter alia - to ensure that data processing systems are designed to process as little personal data as possible, to implement privacy by default settings, for example in social networks, to keeping individual's profiles private from others by default and to implement tools enabling users to better protect their personal data (e.g. access controls, encryption).

111. The advantages of a more explicit reference to privacy by design can be summarised as follows:

- It would highlight the importance of the principle *per se*, as a tool towards ensuring that processes, products and services are designed from the outset with privacy in mind.
- It would reduce privacy abuses and it would minimize the unnecessary collection of data and empower individuals to exercise real choices as their personal data.
- It would avoid having to put "band aids" later on in an attempt to fix problems that may be difficult to repair if not impossible.
- it would also facilitate the effective application and enforcement of this principle by data protection authorities.

112. The combined effect of this obligation would result in a stronger demand for privacy by design products and services, which should give more incentives to industry to meet such demand. It should be considered, on top of that, to create a separate obligation addressed to designers and manufacturers of new products and services with likely impact

---

44 Resolution on Privacy by Design, adopted by the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem 27-29 October 2010.

45 The Directive includes provisions which indirectly, in different situations, demand the implementation of privacy by design. In particular, Article 17 requires that data controllers implement appropriate technical and organization measures to prevent unlawful data processing. The ePrivacy Directive is more explicit. Article 14.3 provides that "*Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications)*".

46 Under the present framework, Recital 46 encourages controllers implementing such measures, but a recital does of course not have binding force.

on data protection and privacy. The EDPS suggests including such a separate obligation which could further enable data controllers to comply with their own obligation.

113. The codification of privacy by design could be complemented by a provision setting forth general privacy by design requirements applicable across sectors, products and services, such as for example, ensuring user's empowerment measures, to be adopted pursuant to the principle.

114. Additionally, the EDPS recommends delegating powers to the Commission under Article 290 TFEU to - where appropriate - supplement the basic requirements of privacy by design for selected products and services. Using these powers would enhance data controllers' legal certainty and harmonize compliance throughout the EU. In developing such specific instruments, the Article 29 Working Party and the EDPS should be consulted (see in the same way point 106 on accountability).

115. Finally, the data protection authorities should be given the power to impose remedial measures or sanctions, under similar restrictive conditions as already mentioned in point 107, where controllers have clearly failed to take concrete steps in cases where this would be required.

7.4. Certification services

116. The Communication recognizes the need to explore the creation of EU certification schemes for privacy compliant products and services. The EDPS fully supports this aim and suggests including a provision providing for their creation and possible effect across the EU, which may be further developed later on in additional legislation. The provision should complement the provisions on accountability and privacy by design

117. Voluntary certification schemes would enable verification that a data controller has put in place measures to comply with the legal instrument. Furthermore, data controllers - or even products or services - enjoying the benefit of a certification label are likely to gain a competitive advantage over others. Such schemes would also help data protection authorities in their supervision and enforcement role.

8. Globalisation and applicable law

8.1. A clear need for more consistent protection

118. As mentioned earlier in Chapter 2, the transfer of personal data beyond the EU borders has exponentially grown as a consequence of the development of new technologies, the role of multinational companies and the increased influence of governments in the processing and sharing of personal data on an international scale. This is one of the main reasons justifying the revision of the current legal framework. Consequently, this is one of the areas where the EDPS asks for ambition and effectiveness, since there is a clear need for more consistent protection where data are processed outside the EU.

8.2. Investing in international rules

119. According to the EDPS more investment is needed in the development of international rules. More harmonisation with regard to the level of protection of personal data across the world would considerably clarify the substance of the principles to be complied with, and the conditions for transfers of data. These global rules would need to reconcile the

requirement for a high standard of data protection - including core EU data protection elements - with regional specificities.

120. The EDPS supports the ambitious work done so far in the framework of the International Conference of Data Protection Commissioners to develop and disseminate the so called "Madrid standards", with a view to integrate them into a binding instrument and possibly initiate an intergovernmental conference.[47] He calls on the Commission to take the necessary initiatives to facilitate the realisation of this objective.

121. In the view of the EDPS it is also important to ensure consistency between this initiative for international standards, the current review of the EU data protection framework and other developments such as the current revision of the OECD Privacy Guidelines and of Convention 108 of the Council of Europe which is open to signature by third countries (see also point 17). The EDPS considers that the Commission has a specific role to play here, in specifying how it will promote such consistency in the negotiations in the OECD and the Council of Europe.

8.3. Clarifying applicable law criteria

122. Since full consistency can not easily be achieved, there will - at least in the near future - remain some diversity between the laws within the EU and a fortiori beyond EU borders. The EDPS considers that a new legal instrument will need to clarify the criteria determining applicable law, and to ensure streamlined mechanisms for data flows as well as accountability of actors involved in data flows.

123. In the first place the legal instrument should ensure that EU law is applicable when personal data are processed outside the borders of the EU, but where there is a justified claim of applying EU law. The example of non European cloud computing services targeted to EU residents is an illustration why this is needed. In an environment where data are not physically stored and processed in a fixed location, where service providers and users located in different countries have interfering influence on data, it is very difficult to identify who is responsible for complying with which data protection principles. Guidance is being given, especially by data protection authorities, on how to interpret and apply Directive 95/46 in such cases, but guidance alone is not enough to ensure legal certainty in this new environment.

124. Within the territory of the EU the need for more precision in the legal framework and a simplified criterion to determine the law applicable has been emphasised by the Article 29 Working Party in a recent opinion.[48]

125. According to the EDPS, the preferred option would be to lay down the legal instrument in a Regulation which would lead to identical rules applicable in all Member States. A regulation would make the need of determining applicable law less important. This is one of the reasons why the EDPS strongly favours the adoption of a Regulation. However, also a Regulation could allow some margin of manoeuvre for the Member States. If some significant margin of manoeuvre is kept in the new instrument, the EDPS would support the suggestion from the Working Party for a shift from a distributive application of different national laws to a centralised application of a single legislation in all Member States where a controller has establishments. He also pleads for more

47 As suggested by Resolution on International Standards, adopted by the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem 27-29 October 2010.

48 WP29 Opinion 8/2010 on applicable law, WP 179

cooperation and coordination between Data Protection Authorities in transnational cases and complaints (see Chapter 10).

8.4. Streamlining mechanisms for data flows

126. The need for consistency and for a high level benchmark must be taken into account not only with a view to global data protection principles, but also with regard to international transfers. The EDPS fully supports the objective of the Commission to streamline current procedures for international data transfers and ensure a more uniform and coherent approach vis-à-vis third countries and international organisations.

127. The mechanism of data flows includes both private sector transfers, in particular via contractual clauses or Binding Corporate Rules (BCRs), and transfers between public authorities. BCRs are one of the elements where a more coherent and streamlined approach would be desirable. The EDPS recommends addressing conditions for BCRs in an explicit way in the new legal instrument[49], by:

- recognizing explicitly BCRs as tools that provide adequate safeguards;
- providing for the main elements/ conditions for the adoption of BCRs;
- setting forth cooperation procedures for the adoption of BCRs, including criteria for the selection of a leading supervisory authority (one stop shop).

9. The Area of police and justice

9.1. The general instrument

128. The Commission has repeatedly highlighted the importance of strengthening data protection in the context of law enforcement and crime prevention where the exchange and use of personal information has significantly intensified. Also the Stockholm Programme, approved by the European Council, refers to a strong data protection regime as the main prerequisite for the EU Information Management Strategy in this area.[50]

129. The review of the general data protection framework is the perfect occasion to make progress in this respect, in particular since the Communication rightly describes Framework Decision 2008/977 as inadequate.[51]

130. The EDPS argued in section 3.2.5 of this Opinion why the area of police and judicial cooperation should be included in the general instrument. Inclusion of police and justice has a number of additional advantages. It means that the rules will no longer only apply to cross-border data exchanges[52], but also to domestic processing. Adequate protection in the exchange of personal data with third countries will be better guaranteed, also with regard to international agreements. Furthermore, DPAs will have the same extensive and harmonised powers vis-à-vis police and judicial authorities as they have vis-à-vis other data controllers. Finally, the current Article 13, providing for the Member States' power to adopt specific legislation to restrict obligations and rights under the general instrument for specific public interests, will have to be applied in the same restrictive way as it applies in other areas. In particular, the specific safeguards provided for under the general

---

49 On international transfers, see also Chapter 8 of the opinion.

50 See on this EDPS Opinion of 30 September 2010 on the Communication from the Commission to the European Parliament and the Council - "Overview of information management in the area of freedom, security and justice", paras 9-19.

51 See Section 3.2.5 above.

52 This is currently the limited scope of Framework Decision 2008/977.

instrument in this field will have to be respected also in national legislation adopted in the area of police and judicial cooperation.

9.2. Additional specific rules for police and justice

131. However, such an inclusion does not exclude special rules and derogations, which duly take account of the specificities of this sector, in line with Declaration 21 attached to the Lisbon Treaty. Limitations to the rights of data subjects may be foreseen, but they have to be necessary, proportionate and not alter the essential elements of the right itself. It should be emphasized in this context that Directive 95/46, including its Article 13, currently applies to law enforcement in various areas (e.g. taxation, customs, antifraud) that are not fundamentally different from many activities in the area of police and justice.

132. In addition, specific safeguards need also to be put in place, in order to compensate the data subject by giving him additional protection in an area where the processing of personal data may be more intrusive.

133. In light of the above, the EDPS considers that the new framework should include at least the following elements, in line with Convention 108 and Recommendation No R (87) 15:

- A distinction between different categories of data and files in accordance with their accuracy and reliability, endorsing the principle that data based on facts should be distinguished from data based on opinions or personal assessment.
- A distinction between various categories of data subjects (criminal suspects, victims, witnesses, etc.) and files (temporary, permanent and intelligence files). Specific conditions and safeguards need to be foreseen for the processing of data of non-suspects.
- Mechanisms to ensure periodic verification and rectification in order to safeguard the quality of the data being processed.
- Specific provisions and/or safeguards may be devised in relation to the (increasingly relevant) processing of biometric and genetic data in the field of law enforcement. Their use should be limited only to cases where no less intrusive means are available which may ensure the same effect.[53]
- Conditions for transfers of personal data to non competent authorities and private parties, as well as for access and further use by law enforcement authorities of personal data collected by private parties.

9.3. Sector specific data protection regimes

134. The Communication states that "the Framework Decision does not replace the various sector-specific legislative instruments for police and judicial co-operation in criminal matters adopted at EU level, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), which either contain particular data protection regimes, and/or which usually refer to the data protection instruments of the Council of Europe".

135. In the view of the EDPS, a new legal framework should be, as far as possible, clear, simple and consistent. When there is a proliferation of different regimes applying to for instance Europol, Eurojust, SIS and Prüm, compliance with the rules remains or even

[53] In this direction, see WP document on the Future of Privacy, point 112.

becomes more complicated. That is one of the reasons why the EDPS favours a comprehensive legal instrument for all sectors.

136. However, the EDPS understands that aligning the rules from the different systems will require considerable work, which has to be carried out carefully. The EDPS considers that a gradual approach as mentioned in the Communication makes sense as long as the commitment to ensuring a high level of data protection in a consistent and effective way remains clear and visible. To be more concrete:

- In a first stage, the general legal instrument for data protection should be made applicable to all processing in the area of police and judicial cooperation, including the adjustments for police and justice (as meant in 9.2).
- In a second stage, the sector specific data protection regimes should be aligned with this general instrument. The Commission should commit itself to adopt proposals for this second stage, within a short and specified timeframe.

10. DPAs and the Cooperation between DPAs

10.1. Reinforcing the role of DPAs

137. The EDPS fully supports the objective of the Commission to address the issue of the status of data protection authorities (DPAs), and more explicitly to strengthen their independence, resources and enforcement powers.

138. The EDPS also insists on the need to clarify in the new legal instrument the essential notion of independence of DPAs. The European Court of Justice has recently taken a decision on this issue in Case C-518/07[54], where it emphasised that independence means the absence of any external influence. A DPA may seek nor take instructions from anybody. The EDPS suggests explicitly codifying these elements of independence in the law.

139. In order to exercise their tasks the DPAs must be given sufficient human and financial resources. The EDPS suggests including this requirement in the law.[55] He finally stresses the need to make sure that authorities have fully harmonised powers in terms of investigation and imposing sufficiently deterring and remedial measures and sanctions. This would enhance legal certainty for data subjects and for data controllers.

140. Strengthening the independence, resources and powers of DPAs should go together with reinforced cooperation at multilateral level, especially in view of the growing number of data protection issues on a European scale. The main infrastructure to be used for this cooperation is obviously the Article 29 Working Party.

10.2. Strengthening the role of the Working Party

141. History shows that, from its start in 1997 until today, the functioning of the group has evolved. It has grown towards more independence and may not qualify any more, in practice, as a simple advisory working party to the Commission. The EDPS suggests further improvements of the functioning of the Working Party, including of its infrastructure and its independence.

---

54 Case C-518/07, *Commission v. Germany*, not yet published in ECR.

55 See, for example Article 43 (2) of Regulation 45/2001, which contains such requirement for the EDPS.

142. The EDPS believes that the strength of the group is intrinsically linked with the independence and powers of its members. The autonomy of the Working Party should be ensured in the new legal framework, in accordance with the criteria developed for a complete independence of DPAs by the European Court of Justice in case C-518/07. The EDPS considers that the Working Party should also be provided with sufficient resources and budget and a reinforced secretariat, to support its contributions.

143. With regard to the secretariat of the Working Party, the EDPS values the fact that it is integrated in the Data Protection Unit of DG Justice, with the advantage that the Working Party itself can benefit from efficient and flexible contacts and up-to-date information on data protection developments. On the other hand, he questions the fact that the Commission (and more specifically the Unit) is at the same time member, secretariat and addressee of the Working Party's opinions. This would justify more independence of the secretariat. The EDPS encourages the Commission to assess - in close consultation with stakeholders - how this independence can best be ensured.

144. Finally, reinforcing the powers for DPAs also requires stronger powers for the Working Party, with a structure including better rules and safeguards and more transparency. This will be developed for the advisory role as well as for the enforcement role of the Working party.

10.3. The advisory role of the Working Party

145. The positions of the Working Party must be effectively implemented when it comes to its advisory role to the Commission, especially in relation to the interpretation and application of the principles of the Directive and other data protection instruments, in other words to ensure the authoritative character of the Working Party positions. Further discussion is needed amongst DPAs in order to identify how to include this in the legal instrument.

146. The EDPS recommends solutions which would make opinions of the Working Party more authoritative without modifying substantially its way of functioning. The EDPS suggests including an obligation for the DPAs and the Commission to *take utmost account of opinions and common positions* adopted by the Working Party, based on the model adopted for the positions of the Body of European Regulators for Electronic Communications (BEREC)[56]. Furthermore, the new legal instrument could give the Working Party the explicit task to adopt "interpretative recommendations". These alternative solutions would give the positions of the Working Party a stronger role, also before the Courts.

10.4. Coordinated enforcement by the Working Party

147. Under the present framework the enforcement of data protection law in the Member States is left to 27 Data Protection Authorities with little coordination as regards the handling of specific cases. When it comes to cases involving more than one Member State or having clearly a global dimension, this multiplies costs for undertakings, which are forced to deal with different public authorities for the same activity, and it enhances the risk of inconsistent application: in exceptional cases, the same processing activities may be considered lawful by one DPA and prohibited by another.

[56] Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L337, 9 18.12.200, p. 1.

148. Some cases have a strategic dimension which should be addressed in a centralised way. The Article 29 Working Party facilitates coordination and enforcement actions between DPAs[57] in major data protection issues with such international implications. This was the case with social networks and search engines[58], as well as with regard to coordinated inspections conducted in different Member States on telecommunication and health insurance issues.

149. There are however limits to the enforcement actions that the Working Party can undertake under the present framework. Common positions can be taken by the Working Party, but there is no instrument to ensure that these positions are effectively implemented in practice.

150. The EDPS suggests including in the legal instrument additional provisions that could support coordinated enforcement, in particular:

- An obligation to ensure that DPAs and the Commission *take utmost account of opinions and common positions* adopted by WP 29.[59]
- An obligation for DPAs to faithfully cooperate with each other and with the Commission and the WP 29[60]. As a practical illustration of a faithful cooperation, a procedure could be set up by which DPAs inform the Commission or the Working Party in case of national enforcement measures with a cross border element, in analogy to the procedure applicable in the present framework with regard to national adequacy decisions.
- Specifying the voting rules to increase the commitment of DPAs to implement the decisions of the Working Party. It could be provided that the Working Party envisages deciding on the basis of consensus and when consensus could not be reached takes enforcement only with a qualified majority. In addition to this, a recital could foresee that those DPAs casting a positive vote on a document have an obligation or policy commitment to implement it at national level.

151. The EDPS would put a caveat against introducing stronger measures, such as giving binding force to WP29 positions. This would undermine the independent status of individual DPAs, which has to be guaranteed by the Member States under national law. Would the Working Party decisions have a direct impact on third parties such as data controllers, new procedures should be foreseen including safeguards such as transparency and redress, including possibly appeal before the European Court of Justice.

10.5. Cooperation between the EDPS and the Working Party

152. The way in which the EDPS and the Working Party cooperate could also be fine-tuned. The EDPS is a member of the Working Party, and he contributes within the group to positions on the main strategic EU developments, while ensuring consistency with his own positions. The EDPS notes the increasing number of privacy issues, both in the private as well as in the public sector, which have implications at national level in many Member States, and where there is a specific role for the Working Party to play.

---

57 Beside the Article 29 Working Party, the European Conference of Data Protection Commissioners has created about ten years ago a permanent workshop aimed at addressing cross-border complaints in a coordinated way. Although this workshop presents undeniable added value in terms of exchange between DPAs' staffs and offers a reliable network of contact points, it can not be considered as a coordination mechanism for decision making.

58 See the letters of WP 29 of 12.05.2010 and 26.05.2010, published on the WP29 website (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

59 As mentioned above, a similar obligation is laid down in Regulation (EC) No 1211/2009 which specifies the role of the Body of European Regulators for Electronic Communications (BEREC)..

60 See, in this regard, Article 3 of Regulation (EC) No 1211/2009, cited above.

153. The EDPS has a complementary task to advise on the developments in the context of the EU, which should be maintained. As a European body, he exercises this advisory competence towards EU Institutions in the same way as national DPAs advise their governments.

154. The EDPS and the Working Party act from a different but complementary perspective. There is for these reasons a need to preserve and maybe improve coordination between the Working Party and the EDPS, to make sure that they work together on the main data protection issues, for instance by coordinating agendas on a regular basis[61], and by ensuring transparency on issues which have a more national or specific EU aspect.

155. Coordination is not mentioned in the present Directive for the simple reason that the EDPS did not exist at the time where the Directive was adopted, but after six years of existence the complementarities of the EDPS and the Working Party are visible and could be formally recognised. The EDPS recalls that under Regulation 45/2001 he has the duty to cooperate with the national DPAs and to participate in the activities of the Working Party. The EDPS recommends to explicitly mention cooperation in the new legal instrument, and to structure it where necessary, for instance by laying down a procedure for cooperation.

10.6. Cooperation between the EDPS and the DPAs in supervision on EU systems

156. These considerations also apply to areas where the supervision must be coordinated between the European and national level. This is the case for EU bodies that process significant amounts of data delivered by national authorities or for large scale information systems with a European and a national component.

157. The existing system for some EU bodies and large scale information systems - for instance, Europol, Eurojust and the first generation Schengen Information System (SIS) have Joint Supervisory Bodies with representatives of national DPAs - is a remnant of intergovernmental cooperation in the pre-Lisbon era and does not respect the institutional structure of the EU of which Europol and Eurojust are now an integral part, and in which the "Schengen acquis" has now also been integrated[62].

158. The Communication announces that the Commission will launch in 2011 a consultation of stakeholders on the revision of these supervision systems. The EDPS urges the Commission to take as soon as possible (within a short and specified timeframe, see above) position in the ongoing discussion on supervision. He will take - in this discussion - the following viewpoint.

159. As a point of departure, it should be guaranteed that all supervisory bodies fulfil the indispensable criteria of independence, resources and enforcement powers. Furthermore, it should be ensured that the perspectives and expertise that exists on the EU level is taken into account. That means that cooperation should take place not only between the national authorities but also with the European DPA (currently the EDPS). The EDPS finds it necessary to follow a model that fulfils these requirements.[63]

---

61 E.g. on the basis of the Inventory of legislative activities published annually and updated regularly, which is available on the EDPS website.

62 Under Regulation 45/2001, the EDPS has a duty to cooperate with these bodies.

63 For Eurojust, a model should also take into account that the data protection supervision respects the independence of the judiciary, in so far as Eurojust process data in the context of criminal proceedings.

160. In recent years the model of "coordinated supervision" was developed. This model of supervision, as now operational in Eurodac and parts of the Customs Information System, will soon be expanded to the Visa Information System (VIS) and the second generation Schengen Information System (SIS II). This model has three layers: (1) supervision at national level is ensured by DPAs; (2) supervision at EU level is ensured by the EDPS; (3) coordination is ensured by way of regular meetings convened by the EDPS acting as the secretariat of this coordination mechanism. This model has proven to be successful and effective and should be envisaged in the future for other information systems.

C. HOW TO IMPROVE APPLICATION OF PRESENT FRAMEWORK?

11. The short term

161. Whilst the review process is ongoing, efforts should be devoted to ensure full and effective implementation of the current rules. These rules will still be applicable until the future framework is adopted and then implemented into national laws of the Member States. In this direction, several lines of actions may be identified.

162. First, the Commission should continue monitoring Member States compliance with Directive 95/46 and, where necessary, use its powers under Article 258 TFEU. Recently, infringement proceedings have been opened for a failure to correctly implement Article 28 of the Directive with regard to the requisite of independence of DPAs[64]. Also in other areas full compliance needs to be monitored and enforced.[65] The EDPS thus welcomes and fully supports the Commission's commitment in the Communication to pursue an active infringement policy. The Commission should also continue the structural dialogue with Member States on implementation.[66]

163. Second, enforcement at national level must be encouraged so as to ensure practical application of data protection rules, including with respect to new technological phenomena and global players. DPAs should make full use of their investigative and sanctioning powers. It is also important that the existing rights of data subjects, particularly the rights of access, are fully implemented in practice.

164. Third, greater coordination in the enforcement seems necessary in the short term. The role of the WP29 and its interpretative documents in this regard is crucial, but also DPAs should do their most to put them in practice. Diverging outcomes in EU-wide or global cases need to be avoided and common approaches can and should be reached within the Working Party. EU-wide coordinated investigations under the auspices of the Working Party can also bring significant added value.

165. Fourth, data protection principles should be "built-in" proactively in new regulations which may have an impact, directly or indirectly, on data protection. At the EU level, the EDPS makes considerable efforts to contribute to better European legislation and these efforts must be undertaken also at national level. Data protection authorities should therefore make full use of their advisory powers to ensure such a proactive approach. Data protection authorities, including the EDPS, can also play a proactive role in monitoring technological developments. Monitoring is important with a view to identifying at an

64 See Case C-518/07, cited above and Commission Press Release of 28 October 2010 (IP/10/1430).

65 The Commission has opened an infringement proceeding against the UK for an alleged breach of various data protection provisions, including the requirement of confidentiality of electronic communications in respect of behavioural advertising. See Commission Press Release of 9 April 2009 (IP/09/570).

66 See Commission's First Report on the implementation of the Data Protection Directive, cited above, p. 22 et seq.

early stage emerging trends, highlighting possible data protection implications, supporting data protection-friendly solutions and raising the awareness of stakeholders.

166. Finally, further cooperation between the various actors at international level needs to be actively pursued. It is therefore important to reinforce the international instruments of cooperation. Initiatives like the Madrid standards and the ongoing work within the Council of Europe and the OECD deserve full support. In this context, it is very positive that also the US Federal Trade Commission has now joined the family of Privacy and Data Protection Commissioners in the framework of their International Conference.

D. CONCLUSIONS

General observations

167. The EDPS welcomes the Commission's Communication in general, as he is convinced that the review of the present legal framework for data protection is necessary, in order to ensure effective protection in an increasingly developing and globalised information society.

168. The Communication identifies the main issues and challenges. The EDPS shares the view of the Commission that a strong system of data protection will still be needed in the future, based on the notion that existing general principles of data protection are still valid in a society which undergoes fundamental changes. The EDPS shares the statement in the Communication that the challenges are enormous and underlines the consequence that the proposed solutions should be correspondingly ambitious and enhance the effectiveness of the protection. As a result he asks for a more ambitious approach on a number of points.

169. The EDPS fully supports the comprehensive approach to data protection. However, he regrets that the Communication excludes certain areas, such as the data processing by EU institutions and bodies, from the general legal instrument. If the Commission were to decide to leave out these areas, the EDPS urges the Commission to adopt a proposal for the EU level within the shortest possible timeframe, but preferably by the end of 2011.

Main perspectives

170. The points of departure of the review process for the EDPS are as follows:

- Arrangements for data protection must as far as possible actively support rather than hamper other legitimate interests (such as European economy, the security of individuals and accountability of governments).
- The general principles of data protection should not and cannot be changed.
- Further harmonisation should be one of the key objectives of the review.
- The fundamental rights perspective should lie at the heart of the review process. A fundamental right aims to protect citizens under all circumstances.
- The new legal instrument must include the police and justice sector.
- The new legal instrument must be formulated in a technologically neutral way as much as possible and must aim to create legal certainty over the longer term.

Elements of a new framework

Harmonisation and simplification

171. The EDPS welcomes the Commission's commitment to examine the means to achieve further harmonisation of data protection at EU level. The EDPS determines areas where further and better harmonisation is urgent: definitions, grounds for data processing, data subjects' rights, international transfers and data protection authorities.

172. The EDPS suggests considering the following alternatives to simplify and/or reduce the scope of the notification requirements:
- Limit the obligation to notify to specific kinds of processing operations entailing specific risks.
- A simple registration obligation requiring data controllers to register (as opposed to extensive registration of all data processing operations).
- The introduction of a standard pan-European notification form.

173. According to the EDPS a Regulation, a single instrument which is directly applicable in the Member States, is the most effective means to protect the fundamental right to data protection and to achieve further convergence in the internal market.

Strengthening the rights of individuals

174. The EDPS supports the Communication where it proposes strengthening individuals' rights. He makes the following suggestions:
- A principle of transparency could be included in the law. However, it is more important to reinforce the existing provisions dealing with transparency (such as the existing Articles 10 and 11 of Directive 95/46).
- A provision on personal data breach notification, which extends the obligation included in the revised ePrivacy Directive from certain providers to all data controllers, should be introduced in the general instrument.
- The limits of consent should be clarified. Broadening the cases where express consent is required should be considered as well as adopting additional rules for the online environment.
- Additional rights should be introduced such as data portability and the right to be forgotten, especially for information society services on the internet.
- Children's interests should be better protected with a number of additional provisions, specifically addressed to the collection and further processing of children's data.
- Collective redress mechanisms for breach of data protection rules should be introduced in the EU legislation, in order to empower qualified entities to bring actions on behalf of groups of individuals.

Strengthening the obligations of organisations/controllers

175. The new framework must contain incentives for data controllers to pro-actively include data protection measures in their business processes. The EDPS proposes the introduction of general provisions on accountability and "privacy by design". A provision on privacy certification schemes should also be introduced.

Globalisation and applicable law

176. The EDPS supports the ambitious work in the framework of the International Conference of Data Protection Commissioners to develop the so called "Madrid standards", with a view to integrate them into a binding instrument and possibly initiate an intergovernmental conference. The EDPS calls on the Commission to take concrete steps in this direction in close cooperation with the OECD and the Council of Europe.

177. A new legal instrument must clarify the criteria determining applicable law. It should be ensured that data that are processed outside the borders of the EU do not escape EU jurisdiction where there is a justified claim for applying EU law. If the legal framework would have the form of a Regulation there would be identical rules in all Member States and it would become less relevant to determine applicable law (within the EU).

178. The EDPS fully supports the objective to ensure a more uniform and coherent approach vis-à-vis third countries and international organisations. Binding Corporate Rules (BCRs) should be included in the legal instrument.

The area of police and justice

179. A comprehensive instrument including police and justice may allow for special rules which duly take account of the specificities of this sector, in line with Declaration 21 attached to the Lisbon Treaty. Specific safeguards need to be put in place, in order to compensate data subjects by giving them additional protection in an area where the processing of personal data is by nature more intrusive.

180. The new legal framework should be, as far as possible, clear, simple and consistent. A proliferation of different regimes applying to, for instance, Europol, Eurojust, SIS and Prüm, should be avoided. The EDPS understands that aligning the rules from the different systems will have to be carried out carefully and gradually.

DPAs and the cooperation between DPAs

181. The EDPS fully supports the objective of the Commission to address the issue of the status of data protection authorities (DPAs), and to strengthen their independence, resources and enforcement powers. He recommends:

- Codifying in the new legal instrument the essential notion of independence of DPAs, as specified by the ECJ.
- Stating in the law that DPAs must be given sufficient resources.
- Giving authorities harmonised investigation and sanctioning powers.

182. The EDPS suggests further improvements of the functioning of the Article 29 Working Party, including its independence and infrastructure. The Working Party should also be provided with sufficient resources and a reinforced secretariat.

183. The EDPS suggests reinforcing the advisory role of the Working Party by introducing an obligation for DPAs and the Commission to *take the utmost account of opinions and common positions* adopted by the Working Party. The EDPS is not in favour of giving binding force to Working Party positions, particularly because of the independent status of individual DPAs. The EDPS recommends that the Commission introduce specific provisions to enhance cooperation with the EDPS in the new legal instrument.

184. The EDPS urges the Commission to take a position as soon as possible on the issue of supervision of EU bodies and large scale information systems, taking into consideration that all supervisory bodies should fulfil the indispensable criteria of independence, sufficient resources and enforcement powers and that it should be ensured that the EU perspective is well represented. The EDPS supports the model of 'coordinated supervision'.

Improvements under the present system:

185. The EDPS encourages the Commission to:

- Continue monitoring Member States' compliance with Directive 95/46 and, where necessary, using its enforcement powers under Article 258 TFEU.
- Encourage enforcement at the national level and the coordination of enforcement.
- Build data protection principles pro-actively into new regulations which may have an impact, directly or indirectly, on data protection.
- Actively pursue further cooperation between the various actors at international level.

Brussels, 14 January 2011

(**signed**)

Peter HUSTINX
European Data Protection Supervisor