ARTICLE 29 Data Protection Working Party

Working Party on Police and Justice

02356/09/EN
WP 168

The Future of Privacy

Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data

Adopted on 01 December 2009

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
The secretariat is provided by Directorate D (Fundamental Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/190.
Website: http://ec.europa.eu/ justice_home/fsj/privacy/index_en.htm

The Working Party on Police and Justice was set up as a working group of the Conference of the European Data Protection Autorities. It is mandated to monitor and examine the developments in the area of police and law enforcement to face the growing challenges for the protection of individuals with regard to the processing of their personal data.

Executive Summary

On 9 July 2009, the Commission launched a Consultation on the legal framework for the fundamental right to protection of personal data. In its consultation the Commission asks for views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation. It wants to have input on the questions whether the current legal framework meets these challenges and what future action would be needed to address the identified challenges. This paper contains the joint reaction of the Article 29 Working Party (WP29) and the Working Party on Police and Justice (WPPJ) to this consultation.

The central message of this contribution is that the main principles of data protection are still valid despite the new technologies and globalisation. The level of data protection in the EU can benefit from a better application of the existing data protection principles in practice. This does not mean that no legislative change is needed. To the contrary, it is useful to use the opportunity in order to:

- Clarify the application of some key rules and principles of data protection (such as consent and transparency).
- Innovate the framework by introducing additional principles (such as 'privacy by design' and 'accountability').
- Strengthen the effectiveness of the system by modernising arrangements in Directive 95/46/EC (e.g. by limiting bureaucratic burdens).
- Include the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters.

Chapter 1 contains an introduction, with a brief overview of the history and context of data protection in the EU.

Chapter 2 proposes the introduction of one comprehensive legal framework. It recognises the need for specific rules (*leges speciales*), provided that they fit within the notion of a comprehensive framework and comply with the main principles. The main safeguards and principles of data protection should apply to data processing in all sectors.

Chapter 3 and 4 discuss the main challenges to data protection.

Chapter 3 on globalisation states that under EU law, data protection is a fundamental right. The EU and its Member States should guarantee this fundamental right for everybody, in so far as they have jurisdiction. Individuals should be able to claim protection, also if their data are processed outside the EU. Therefore, the Commission is called upon to take initiatives towards the further development of international global standards regarding the protection of personal data. In addition, it is necessary to redesign the adequacy process. Furthermore, international agreements can be appropriate instruments for the protection of personal data in a global context, and the future legal framework could mention the conditions for agreements with third countries. The processing of data outside the EU can also be protected by Binding Corporate Rules (BCRs). A provision on BCRs should be further reinforced and included in the new legal framework. Regarding applicable law, the WP29 envisages to advise the Commission on this subject in the course of the upcoming year.

Chapter 4 on the technological changes states that Directive 95/46/EC has stood well the influx of technological developments because of its sound and technologically neutral principles and concepts. These principles and concepts remain equally relevant, valid and applicable in today's networked world. The technological developments have strengthened the risks for individuals' privacy and data protection and to counterbalance these risks, the principle of 'Privacy by Design' should be introduced in the new framework: privacy and data protection should be integrated into the design of Information and Communication Technologies. The application of such principle would emphasize the need to implement privacy enhancing technologies, 'privacy by default' settings and the necessary tools to enable users to better protect their personal data. This principle of 'Privacy by Design' should therefore not only be binding for data controllers, but also for technology designers and producers. On top of that, as the need arises, regulations for specific technological contexts should be adopted which require embedding data protection and privacy principles into such contexts.

Chapters 5, 6 and 7 argue that these main challenges to data protection require a stronger role for the different actors.

The changes in the behaviour and role of the data subject, and the experience with Directive 95/46/EC, require a stronger position for the data subject in the data protection framework. Chapter 5 contains suggestions for empowering the data subject, in order to play a more active role. Empowerment of the data subject requires, among others, the improvement of redress mechanisms: more options for the data subject to execute and enforce his rights, including the introduction of class action procedures, more easily accessible, and more effective and affordable complaints procedures and alternative dispute resolutions. In addition, the new framework should provide alternative solutions in order to enhance transparency and the introduction of a general privacy breach notification. 'Consent' is an important ground for processing which could under certain circumstances empower the data subject. However, at the moment, it is often falsely claimed to be the applicable ground, since the conditions for consent are not fully met. Therefore the new framework should specify the requirements of 'consent'. Furthermore, harmonisation needs to be improved, as the empowerment of the data subject is currently being undermined by the lack of harmonisation amongst the national laws implementing Directive 95/46/EC. Finally, the role of data subjects on the internet is an area of concern and should be further clarified in view of the new legal framework. In any case, whoever offers services to a private individual should be required to provide certain safeguards regarding the security, and as approriate the confidentiality of the information uploaded by users, regardless of whether their client is a data controller.

Chapter 6 aims at strengthening the responsibility of the data controllers. Data protection should first of all be embedded in organizations. It should become part of the shared values and practices of an organization, and responsibilities for it should be expressly assigned. This will also assist national Data Protection Authorities (DPAs) in their supervision and enforcement tasks and therefore strengthen the effectiveness of privacy protections. Data controllers need to take several proactive and reactive measures, mentioned in this chapter. Furthermore, it would be appropriate to introduce in the comprehensive framework an accountability principle, so data controllers are required to carry out the necessary measures to ensure that substantive principles and obligations of the current Directive are observed when processing personal data, and to have the necessary internal mechanisms in place to demonstrate compliance to external stakeholders, including DPAs. Notifications of data processing operations with national

DPAs could be simplified or diminished. It should be explored whether and to what extend notification could be limited to those cases where there is a serious risk to privacy, enabling DPAs to be more selective and concentrate their efforts to such cases, and how notification could be streamlined.

Chapter 7a envisages stronger and clearer roles for national DPAs. At the moment, there are large divergences between the Member States regarding, amongst others, the position, resources and powers of DPAs. The new challenges to data protection require strong supervision by DPAs, in a more uniform and effective way. The new framework should therefore guarantee uniform standards as for independence, effective powers, an advisory role in the legislation making process and the ability to set their own agenda by, in particular, setting priorities regarding the handling of complaints, all on a high and influential level.

Chapter 7b states how the cooperation of the DPAs should be improved. The European DPAs are united in the WP29. As a first priority, it should be ensured that all issues relating to the processing of personal data, in particular in the area of police and judicial cooperation in criminal matters, will be included in the activities of the current WP29. In addition, the working methods of the WP29 should be further improved. Where needed, it should be insisted on that there is a strong commitment of members of the WP29 to implement the views of the WP29 into national practice. Relations between the WP29 and the Commission, that provides for the Secretariat of the WP29, can be further improved by describing the main roles of both players in a Memorandum of Understanding. The WP29 will enter into consultation with the Commission regarding this Memorandum in 2010.

Finally, Chapter 8 discusses the data protection challenges in the field of police and law enforcement, an area of specific concern. The context of this area within the EU has changed with the entry into force of the Lisbon Treaty. Framework Decision 2008/977/JHA on the protection of personal data in the framework of police and judicial cooperation in criminal matters can be seen as a first step towards a general framework in the former third pillar, but is far from complete. Over the last years, there has been a dramatic increase of the storage and exchange of personal data in relation to activities of the police and justice sector, due to growing needs of the use of information, in order to face new threats resulting from terrorism and organised crime, and stimulated by the technological developments. Against this background, the challenges for data protection are immense, and should be addressed in the future legal framework. Chapter 8 provides the conditions for law and policy making on data protection in the area of police and law enforcement: basing information exchange on a consistent strategy; a periodic evaluation of existing measures, legal instruments and their application; transparency, and addressing access and rectification rights in a cross border context; transparency and democratic control in the legislative process; the architecture of systems for storage and exchange of personal data; a clear framework as a basis for relations with third states, that is binding on all parties and based on the notion of adequacy; special attention for large scale information systems within the EU; properly addressing independent supervision, judicial oversight and remedies; and strengthening cooperation between DPAs.

1. Introduction

The consultation

1. On 9 July 2009, the Commission launched a Consultation on the legal framework for the fundamental right to protection of personal data. In its consultation the Commission asks for views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation. It wants to have input on the questions whether the current legal framework meets these challenges and what future action would be needed to address the identified challenges.

2. This paper contains the joint reaction of the Article 29 Working Party (WP29) and the Working Party on Police and Justice (WPPJ) to this consultation.

History and context

3. The Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)[1] can be considered as the first European legal framework for the fundamental right to protection of personal data. The right to data protection is closely related but not identical to the right to private life under Article 8 of the European Convention for Human Rights. The right to data protection is recognised as an autonomous fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union.

4. The principles of Convention 108 were refined in Directive 95/46/EC[2] which forms the main building block of data protection law within the EU. The (future) effectiveness of the directive is the main object of the consultation of the Commission. Other EU legislative instruments for data protection are Regulation (EC) Nr. 45/2001[3] applicable to data processing by EU institutions and bodies, Directive 2002/58/EC[4] on privacy and electronic communications and Framework Decision 2008/977/JHA[5] on data protection in the area of police and judicial cooperation in criminal matters.

5. Under the Lisbon Treaty, data protection has gained significant importance. Not only has the Charter of Fundamental Rights of the European Union become binding but – also Article 16 of the Treaty on the Functioning of the European Union (TFEU) was introduced as a new legal basis for data protection applicable to all processing of personal data, in the private and in the public sector, including the processing in the area of police and judicial cooperation and common foreign and security policy. Article 16 gives an impetus for data protection.

---

1 ETS No. 108, 28.01.1981.

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

3 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, OJ 2001, L 8, p. 1.

4 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201, p. 37; as revised by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

5 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ 2008 L 350, p. 60., to be implemented in national law before 27 November 2010.

6. In this context, also the 'Stockholm Programme' must be mentioned. This multi-annual programme of the EU dedicates much attention to data protection in an area of Freedom, Security and Justice protecting the citizen.[6]

Central message

7. The consultation by the Commission comes at an appropriate moment, because of the important new challenges provoked by new technologies and globalisation but also in the perspective of the Lisbon Treaty.

8. The central message is that the main principles of data protection are still valid despite these important challenges. The level of data protection in the EU can benefit from a better application of the existing data protection principles in practice. This does not mean that no legislative change is needed. To the contrary, it is useful to use the opportunity in order to:

   - Clarify the application of some key rules and principles of data protection (such as consent and transparency).
   - Innovate the framework by introducing additional principles (such as 'privacy by design' and 'accountability').
   - Strengthen the effectiveness of the system by modernising arrangements in Directive 95/46/EC (e.g. by limiting bureaucratic burdens).
   - Include the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters.

2. One comprehensive framework

The present legal framework

9. Data protection was introduced into the legal framework of the European Union as an internal market related issue. Directive 95/46/EC is based on Article 95 EC. The purpose of this directive is twofold. The establishment and functioning of an internal market requires that personal data should be able to flow freely from one Member State to another, while at the same time a high level of protection of fundamental rights of individuals should be safeguarded.

10. Directive 95/46/EC is meant as a general legal framework, which could be complemented by specific regimes for data protection for specific sectors. Until now, only one specific regime has been adopted, for ePrivacy (currently Directive 2002/58/EC). Moreover, several pieces of sectoral legislation also contain specific rules relating to the processing of personal data ([7] on money laundering, customs legislation or VIS, EURODAC or SIS II legislations).

---

[6] The Stockholm Programme: An open and secure Europe serving and protecting the citizen, to be approved by European Council in December 2009.

[7] E.g. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ 2005, L 309, p. 15 and the various legal instruments for the large scale information systems SIS, VIS and EURODAC.

11. The use of Article 95 EC had a consequence for the scope of application of Directive 95/46/EC. Although the Directive was meant as a general framework for data protection and in many aspects functions as such, it does not cover the processing by EU-institutions, nor processing operations that fall outside of the former first pillar (mainly the former third pillar). For the processing by the EU-institutions (as far as they operate within the former first pillar), Regulation 45/2001 was adopted which is to a large extent similar to Directive 95/46/EC. The current situation in the former third pillar can be described as a patchwork of data protection regimes, which are applicable in different situations. Some differences in these regimes stem from the specificities of the area covered, others are merely the consequence of a different legislative history. Framework Decision 2008/977/JHA can be seen as a first step towards a more general framework.

12. The situation is not satisfactory, in particular for the third pillar:

- Data protection is now increasingly recognised as a general concern of the European Union, not necessarily linked to the internal market. This is for instance reflected in Article 8 of the Charter of Fundamental Rights of the European Union.
- In recent years, and certainly after the terrorist attacks in the USA on 11/9/2001, the exchange of personal data between the Member States has become an essential part of police and judicial cooperation which, of course, requires appropriate protection.
- The former division between the pillars does not reflect the reality of data protection where personal data are used in cross pillar situations, as illustrated by the PNR and Data Retention judgements of the European Court of Justice, on cases of use for law enforcement purposes of information collected originally in a business context. .

The need for a new framework

13. The shortcomings of the present system require a reflection on 'a comprehensive and consistent data protection framework covering all areas of EU competence'[8]. The Lisbon Treaty foresees a new horizontal approach to data protection and privacy and provides for the necessary legal basis (Art. 16 TFEU)[9] to get rid of the existing differences and divergences which prejudice a seamless, consistent and effective protection of all individuals.

14. The main safeguards and principles should apply to data processing in all sectors, ensuring an integrated approach as well as a seamless, consistent and effective protection.

15. Directive 95/46/EC should serve as a benchmark for the comprehensive framework which has as main goal effectiveness and effective protection of individuals. The existing principles of data protection need to be endorsed, and complemented with

[8] Wording used by Commission in COM 262 Final.

[9] Article 16 TFEU does not only extend to the third pillar, but also to the second pillar (common foreign and security policy) as far as EU institutions process personal data. Article 39 TEU provides for a specific legal basis for data processing by the Member States in the second pillar. This all is relevant for instance in relation to the terrorists' lists established by the EU and the Member States, but will not be specifically addressed in this chapter.

measures to execute these principles in a more effective manner (and to ensure a more effective protection of citizens' personal data).

16. The main principles of data protection should be the backbone of a comprehensive framework: key notions (who/data controller - what /personal data) and principles should be reaffirmed, including notably the principles of lawfulness, fairness, proportionality, purpose limitation, transparency, and rights of the data subject, as well as independent supervision by public authorities. Rethinking the framework is also an opportunity to clarify the application of some key concepts, such as:

    - consent: confusion between opt-in and opt-out should be avoided, as well as the use of consent in situations where it is not the appropriate legal basis (see also Chapter 5);
    - transparency: it is a pre-condition to fair processing. It must be clear that transparency does not necessarily lead to consent but is a pre-condition for a valid consent and the exercise of the rights of the data subject (see also Chapter 5).

    The objective should be to improve data protection on an international level, in line with the principles and rights defined by Directive 95/46/EC, whilst, at the same time, upholding the current level of protection (see also Chapter 3).

17. The adoption of one comprehensive framework would also allow some useful innovations of the current rules. This might well involve the introduction of the general principle of 'privacy by design' as extension of the current rules on organisational and technical security measures (see also Chapter 4) and the general principle of accountability (see also Chapter 6).

The architecture of a comprehensive framework

18. One comprehensive framework - under the Lisbon Treaty based on a single legal basis - does not necessarily mean that there is no room for flexibility and differences between the sectors and between the Member States, within the scope of the general framework. Specific rules (*leges speciales*) could be complementary and enhance the protection, provided that they fit within the notion of a comprehensive framework and comply with the main principles, as mentioned above.

19. Additional sectoral and specific regulations could be envisaged, for example with regard to:

    - Specific sectors, such as for instance public health, employment or intelligent transport systems.
    - Privacy tools and services, such as seals and audits (see also Chapters 4 and 6).
    - Security breaches (as complement of the security principle; see also Chapters 5 and 6).
    - Police and judicial cooperation, as explicitly foreseen in Declaration 21 attached to the Lisbon Treaty (see further Chapter 8).
    - National security policy, as explicitly foreseen in Declaration 20 attached to the Lisbon Treaty.

20. Additional national regulations could be envisaged, taking into account cultural differences and the internal organisation of the Member States, provided that they do not prejudice the harmonisation, needed within a European Union without internal borders.

21. Further harmonisation is needed as part of an unambiguous and unequivocal legal framework, but this does not exclude that some flexibility can have additional value, as is presently recognised under Directive 95/46/EC for instance if needed because of cultural differences. One could also leave room for national law, to determine the allocation of responsibilities and to recognise different roles of the public and private sectors.

3. Globalisation

Context and present legal framework

22. Under EU law, data protection is a fundamental right, protected under Article 8 of the Charter of Fundamental Rights of the European Union (see also Chapter 1). In other parts of the world, the need for data protection is widely recognised but not necessarily with the status of a fundamental right.

23. The EU and its Member States should guarantee this fundamental right for everybody, in so far as they have jurisdiction. In a globalised world, this means that individuals can claim protection also if their data are processed outside the European Union.

24. Directive 95/46/EC has addressed this need for protection in its Article 4. The directive is applicable to data processing anywhere, and therefore also outside the EU[10] (a) when the controller is established in the EU, and (b) when the controller is established outside the EU but uses equipment in the EU.

25. In addition, Article 25 and 26 of Directive 95/46/EC include a specific regime for the transfer of personal data to third countries. The basic rule of Article 25 is that transfer is only allowed to third countries that ensure an adequate level of protection. Article 26 foresees a number of derogations from this requirement. Well known concepts such as Bindings Corporate Rules (BCRs) and Standard Contractual Clauses implement this provision.

Applicable law

26. The exact scope of Directive 95/46/EC however is not sufficiently clear. It is not always clear whether EU law is applicable, which Member State law is applicable, and what would be the law(s) applicable in case of multiple establishments of a multinational in different Member States. Article 4 of the directive, determining when the directive is applicable to data processing, leaves room for different interpretation.

27. Moreover, there are situations which fall outside the scope of application of the directive. This is the case where non-EU established controllers direct their activities to EU residents which result in the collection and further processing of personal data.

[10] In this context, EU should be understood as including the EFTA-countries.

For example, this is the case of on-line vendors and the like using specific advertisement with local flavor, websites that directly target EU citizens (by using local languages, etc). If they do so without using equipment in the EU, then Directive 95/46/EC does not apply.

28. At the moment, the WP29 is writing an opinion on the concept of applicable law. The WP29 envisages advising the European Commission on this topic in the course of the upcoming year. This advice might include further recommendations for a future legal framework.

International standards and the Madrid Resolution

29. Global standards regarding data protection are becoming indispensable. Global standards would also facilitate transborder data flows which, due to globalisation, are becoming the rule rather than the exception. As long as global standards do not exist, diversity will remain. Transborder data flows have to be facilitated whilst, at the same time, ensuring a high level of protection of personal data when they are transferred to and processed in third countries.

30. The 'Madrid Resolution', a Joint Proposal on International Standards for the Protection of Privacy which has been adopted by the International Conference of Data Protection and Privacy Commissioners on 6 November 2009, deserves support. The Joint Proposal contains a draft of a global standard and brings together all the approaches possible in the protection of personal data and privacy, integrating legislation from five continents. It includes a series of principles, rights and obligations that should be the basis for data protection in any legal system all over the world, and demonstrates that global standards providing an adequate level of data protection are feasible in due course.

31. The Commission is called upon:

    - To take initiatives towards the further development of international global standards regarding the protection of personal data with a view to promote an international framework for data protection and therefore facilitate transborder data flow while ensuring an adequate level of protection of data subjects. These initiatives should include investigating the feasibility of a binding international framework.
    - In the absence of global standards, to promote the development of data protection legislation providing an adequate level of protection, and the foundation of independent DPAs, in countries outside the European Union. The basic principles for data protection, as laid down in the 'Madrid Resolution', should be the universal basis for such legislation.

    These specific tasks of the Commission should be mentioned in the future legal framework.

Improving adequacy decisions

32. Ever more processing operations of personal data take place in a globalised environment. Ensuring the free flow of personal data, while guaranteeing the level of protection of individuals' rights, is an increasing demand. Thus, it is necessary to redesign the adequacy process:

- Defining more precisely the criteria for reaching the legal status of 'adequacy', paying due attention to the approach of the WP29[11] and various other approaches to data protection around the world, and especially to the rights and principles laid down in the Joint Proposal of International Standards on the Protection of Privacy.
- Streamlining the procedures for the analysis of the legal regimes of third countries in order to take more decisions on the adequate level of protection.

The future legal framework should specify these issues.

International agreements

33. Note has been taken of the activities of the EU-US High Level Contact Group on information sharing and privacy and personal data protection. These activities might lead to a transatlantic agreement with common principles for privacy and data protection applicable to the exchange of information with the United States for the fight against terrorism and serious transnational crime.[12].

34. International agreements are appropriate instruments for the protection of personal data in a global context, provided that the level of protection afforded is at least equivalent to the global standards mentioned above, that every individual has an easy and effective redress, including judicial redress, and that specific safeguards are included relating to the purpose for which the personal data will be used.

35. Under those conditions the foreseen transatlantic agreement could serve as a model for exchange with other third countries and for other purposes. The future legal framework could mention the conditions for agreements with third countries.

36. Furthermore, the EU should encourage the cooperation between international data protection authorities, for example on a transatlantic level. Such cooperation is a successful means to promote data protection outside the EU.

Binding Corporate Rules / Accountability

37. The processing of data outside the EU can also be protected by Binding Corporate Rules (BCRs), international codes of conduct for multinationals, allowing for the worldwide transfer within a multinational corporation. BCRs have been introduced by the WP29 in 2003. Both DPAs and multinationals are of the opinion that BCRs are a good means to facilitate international data flows whilst guaranteeing the protection of personal data. However, Directive 95/46/EC did not expressly take account of BCRs. As a result the process for adoption of BCRs, which is based on Article 26 (2) of Directive 95/46/EC, requires the approval of all Member States concerned by a BCR. As a result, assessing and approving BCRs takes a long time. The WP29 has devoted considerable effort to promote and facilitate the use and the approval of BCRs within the current legal framework. In order to improve the process, so far, nineteen DPAs have agreed to a procedure on the approval of BCRs called 'Mutual Recognition'.

---

[11] See in particular WP 29 Working Document 12: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, adopted on 24 July1998

[12] In this regard, the transatlantic problem regarding redress remains to be solved.

38. Against this background a provision on BCRs should be further reinforced and included in the new legal framework, which would serve several purposes:

- Recognising BCRs as appropriate tool to provide adequate safeguards.
- Defining the main substantive and procedural elements of BCRs, following the WP29 Opinions on the subject.

39. Moreover, from a general point of view, a new provision could be included in the new legislative framework pursuant to which data controllers would remain accountable and responsible for the protection of personal data for which they are controllers, even in the case the data have been transferred to other controllers outside the EU (see on 'accountability' more in general Chapter 6).

Final remark

40. This chapter discusses globalisation as such. However, in one way or another, all chapters of this contribution deal with this subject. Often, when one thinks of 'globalisation', one thinks of business. However, increasingly processing operations of personal data take place in a globalised world. Even though the individual often lives a local life, he can more and more be found on line where his data are processed globally. Globalisation therefore is linked to technology (Chapter 4), the position of the data subject (Chapter 5), data controller (Chapter 6), DPAs / WP29 (Chapter 7) and law enforcement (Chapter 8).

4. Technological changes; Privacy by Design as a new principle

41. The basic concepts of Directive 95/46/EC were developed in the nineteen seventies, when information processing was characterized by card index boxes, punch cards and mainframe computers. Today computing is ubiquitous, global and networked. Information technology devices are increasingly miniaturized and equipped with network cards, WiFi or other radio interfaces. In almost all offices and family homes users can globally communicate via the Internet. Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects.

42. Directive 95/46/EC has stood well the influx of these technological developments because it holds principles and uses concepts that are not only sound but also technologically neutral. Such principles and concepts remain equally relevant, valid and applicable in today's networked world.

43. While it is clear that technological developments described above are generally good for society, nevertheless they have strengthened the risks for individuals' privacy and data protection. To counterbalance these risks, the data protection legal framework should be complemented. First, the principle of 'privacy by design' should be introduced in the new framework; second, as the need arises, regulations for specific technological contexts should be adopted which require embedding data protection and privacy principles into such contexts.

Privacy by design principle

44. The idea of incorporating technological data protection safeguards in information and communication technologies ('ICT') is not completely new. Directive 95/46/EC already contains several provisions which expressly call for data controllers to implement technology safeguards in the design and operation of ICT. This is the case of Article 17 which lays down the data controllers' obligation to implement appropriate technical and organizational measures. Recital 46 calls for such measures to be taken, both at the time of the design of the processing system and at the time of the processing itself. Article 16 establishes the confidentiality of processing, a rule which is mirrored and complemented in regulations regarding IT security. Apart from these articles, the principles relating to data quality as contained in Article 6 (lawfulness and fairness, purpose limitation, relevance, accuracy, time limit of storage, responsibility) also apply.

45. Whereas the above provisions of the Directive are helpful towards the promotion of privacy by design, in practice they have not been sufficient in ensuring that privacy is embedded in ICT. Users of ICT services – business, public sector and certainly individuals – are not in a position to take relevant security measures by themselves in order to protect their own or other persons' personal data. Therefore, these services and technologies should be designed with privacy by default settings.

46. It is for these reasons that the new legal framework has to include a provision translating the currently punctual requirements into a broader and consistent principle of privacy by design. This principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems. Providers of such systems or services as well as controllers should demonstrate that they have taken all measures required to comply with these requirements.

47. Such principle should call for the implementation of data protection in ICT (privacy by design or 'PbD') designated or used for the processing of personal data. It should convey the requirement that ICT should not only maintain security but also should be designed and constructed in a way to avoid or minimize the amount of personal data processed. This is in line with recent case law in Germany.[13]

48. The application of such principle would emphasize the need to implement privacy enhancing technologies (PETs), 'privacy by default' settings and the necessary tools to enable users to better protect their personal data (e.g., access controls, encryption). It should be a crucial requirement for products and services provided to third parties and individual customers (eg. WiFi-Routers, social networks and search engines). In turn, it would give DPAs more powers to enforce the effective implementation of such measures.

---

[13] Recently the German Constitutional Court (Judgment of 27 February 2008 – 1 BvR 370/07; 1 BvR 595/07 –) created a constitutional right in the confidentiality and integrity of information technology system. Systems that are able to create, process or store sensitive personal data require special protection. The protective scope of the fundamental right in confidentiality and integrity of information technology system is applied to systems which alone, or in their technical interconnectedness, can contain personal data of the person concerned to such a degree and in such a diversity that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of their personality. These systems are for example personal computers and laptops, mobile phones and electronic calendars.

49. Such principle should be defined in a *technologically neutral* way in order to last for a long period of time in a fast changing technological and social environment. It should also be *flexible* enough so that data controllers and DPAs will, on a case by case basis, be able to translate it in concrete measures for guaranteeing data protection.

50. The principle should emphasize, as current Recital 46 does, the need for such principle to be applied *as early as possible*: 'At the time of the design of the processing system and at the time of the processing itself'. Safeguards implemented at a late stage are inconsistent and insufficient as regards the requirements of an effective protection of the rights and freedoms of the data subjects.

51. Technological standards should be developed and taken into consideration in the phase of system analysis by hardware and software engineers, so that difficulties in defining and specifying requirements deriving from the principle of 'privacy by design' are minimized. Such standards may be general or specific with regard to various processing purposes and technologies.

52. The following examples demonstrate how PbD can contribute to a better data protection:

    - Biometric identifiers should be stored in devices under control of the data subjects (i.e. smart cards) rather than in external data bases.
    - Video surveillance in public transportation systems should be designed in a way that the faces of traced individuals are not recognizable or other measures are taken to minimize the risk for the data subject. Of course, an exception must be made for exceptional circumstances such as if the person is suspected of having committed a criminal offence.
    - Patient names and other personal identifiers maintained in hospitals' information systems should be separated from data on the health status and medical treatments. They should be combined only in so far as it is necessary for medical or other reasonable purposes in a secure environment.
    - Where appropriate, functionality should be included facilitating the data subjects' right to revoke consent, with subsequent data deletion in all servers involved (including proxies and mirroring).

53. In practice, the implementation of the privacy by design principle will require the evaluation of several, concrete aspects or objectives. In particular, when making decisions about the design of a processing system, its acquisition and the running of such a system the following general aspects / objectives should be respected:

    - Data Minimization: data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all or as few personal data as possible.
    - Controllability: an IT system should provide the data subjects with effective means of control concerning their personal data. The possibilities regarding consent and objection should be supported by technological means.
    - Transparency: both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access / information should be enabled.

- User Friendly Systems: privacy related functions and facilities should be user friendly, i.e. they should provide sufficient help and simple interfaces to be used also by less experienced users.
- Data Confidentiality: it is necessary to design and secure IT systems in a way that only authorised entities have access to personal data.
- Data Quality: data controllers have to support data quality by technical means. Relevant data should be accessible if needed for lawful purposes.
- Use Limitation: IT systems which can be used for different purposes or are run in a multi-user environment (i.e. virtually connected systems, such as data warehouses, cloud computing, digital identifiers) have to guarantee that data and processes serving different tasks or purposes can be segregated from each other in a secure way.

Regulations for specific technological contexts

54. The privacy by design principle may not be sufficient to ensure, in all cases, that the appropriate technological data protection principles are properly included in ICT. There may be cases where a more concrete 'hands on approach' may be necessary. To facilitate the adoption of such measures, a new legal framework should include a provision enabling the adoption of specific regulations for a specific technological context which require embedding the privacy principles in such context.

55. This is not a new concept; Article 14 (3) of the ePrivacy Directive, contains a similar provision: '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 standardization in the field of information technology and communications)'.

56. The above would facilitate the adoption, in specific cases, of specific legislative measures embedding the concept of 'privacy by design' and ensuring that adequate specifications are provided. For example, this may be the case with RFID technology, social networks, behavioral advertisement, etcetera.

Final remarks

57. The increasing significance of data protection when creating and operating IT-systems is posing additional requirements to IT-specialists. This causes the need to firmly incorporate data protection into the curricula of IT-professions.

58. The technological data protection principles and the ensuing concrete criteria should be used as a basis for awarding labels of quality (certification schemes) in a framework of a data protection audit.[14]

5. Empowering the Data Subject

59. The potential of the position of the data subject in Directive 95/46/EC has not been fully used. In addition, both the behaviour of citizens and the role of data subjects with respect to data protection have changed, amongst others due to sociological

[14] For example, this is the case with the EuroPriSe project.

changes and new ways of data collection (for instance for profiling purposes). Data subjects can be careless with their own privacy, are sometimes willing to trade privacy for perceived benefits. On the other hand, they still have high expectations of those with whom they do business. Also, data subjects themselves more and more play an active role in the processing of personal data, in particular on the internet.

60. Changes in the behaviour and role of the data subject and the experience with Directive 95/46/EC require a stronger position for the data subject in the data protection framework.[15] Further empowerment of the data subject in order to be able to play a more active role is essential.

Improving redress mechanisms

61. Empowerment of the data subject requires giving the data subject more options to execute and enforce his rights. As court proceedings can sometimes be very difficult and bear a financial risk, the possibility for class action procedures should be introduced in Directive 95/46/EC.[16]

62. In addition, data controllers should provide for complaints procedures which are more easily accessible and more effective and affordable (see also Chapter 6). If these procedures do not resolve the dispute between data subject and data controller, the data subject should be able to turn to alternative dispute resolutions, primarily provided for by the industry.[17] These options should be included in the new legislative framework.

Transparency

63. Transparency is another fundamental condition, as it gives the data subject a say in the processing of personal data, *'ex ante'*, prior to processing. Profiling, data mining, and technological developments which ease the exchangeability of personal data make it even more important for the data subject to be aware by whom, on what grounds, from where, for what purposes and with what technical means data are being processed. It is important that this information is understandable. However, the duty to inform the data subject (Articles 10 and 11 of Directive 95/46/EC) is not always properly put into practice. A new legal framework should provide alternative solutions, in order to enhance transparency. For example, new ways to inform data subjects could be developed in relation to behavioural advertising.

64. In addition, transparency requires that affected individuals should be notified when a privacy breach which is likely to adversely affect their personal data and privacy occurs. That would enable the data subjects to try and control the damage that has been inflicted upon them (in certain cases authorities should be notified as well, see also Chapter 6). A general privacy breach notification should be introduced in the new legal framework (see also Chapter 6).[18]

---

[15] This is especially the case when it concerns children. When taking decisions about their personal data, their best interest needs to be a primary consideration, as stated in the UN Convention on the Rights of the Child (http://www2.ohchr.org/english/law/crc.htm) and other specific international instruments and national law.

[16] Class actions for example exist in environmental law.

[17] This may of course not deprive an individual from a proper redress before a Court or a DPA.

[18] In 'Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)' the WP29 has noted a recommended approach to the issue of the specific privacy breach notifications which are taken on board in the ePrivacy Directive. The same recommendations apply to the introduction of general privacy breach notifications.

Consent

65. In the Directive, consent of the data subject is a legitimate ground for data processing (Article 7 and 8 of Directive 95/46/EC). It is and continues to be an important ground for processing, which could under certain circumstances empower the data subject. However, consent needs to be freely given, informed and specific (Article 2 (h) of Directive 95/46/EC).

66. There are many cases in which consent can not be given freely, especially when there is a clear unbalance between the data subject and the data controller (for example in the employment context or when personal data must be provided to public authorities).

67. In addition, the requirement that consent has to be informed starts from the assumption that it needs to be fully understandable to the data subject what will happen if he decides to consent to the processing of his data. However, the complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual's ability or willingness to make decisions to control the use and sharing of information through active choice.[19]

68. In both hypotheses, consent is an inappropriate ground for processing but nevertheless often falsely claimed to be the applicable ground. The technological developments also ask for a careful consideration of consent. In practice, Article 7 of Directive 95/46/EC is not always properly applied, particularly in the context of the internet, where implicit consent does not always lead to unambiguous consent (as required by Article 7 (a) of the Directive). Giving the data subjects a stronger voice *'ex ante'*, prior to the processing of their personal data by others, however requires explicit consent (and therefore an opt-in) for all processing that is based on consent.[20]

69. The new legal framework should specify the requirement of consent, taking into account the observations made above.

Harmonisation

70. Currently the empowerment of data subjects is being undermined by the lack of harmonisation amongst the national laws implementing Directive 95/46/EC. Several elements of the Directive which are of essence to the position of data subjects, such as the liability provision and the possibility to claim immaterial damages,[21] have not been implemented by all Member States. Besides these differences in the implementation of Directive 95/46/EC, the interpretation of the Directive in the Member States is not always uniform. As globalisation increases, these differences

---

[19] See 'Data Protection Accountability: The essential Elements – A Document for Discussion', Centre for Information Policy Leadership, as Secretariat to the Galway Project, October 2009, p.4.

[20] Regarding consent and opt-in / opt-out, see also chapter 2, where it is stated that confusion between opt-in and opt-out should be avoided, as well as the use of consent in situations where it is not the appropriate legal basis.

[21] In the majority of cases in which damage has been inflicted upon the data subject, the damage consists of immaterial damage such as the sense no longer to be able to move through the public and private sector without being watched. This problem increases in the current 'surveillance society'.

more and more weaken the position of the data subject. It is therefore of great importance that harmonisation be improved (see also Chapter 7b), if needed by specifying legislative provisions.

The role of data subjects on the internet

71. Increasingly, individuals upload their own personal data into the internet (social networks, cloud computing services, etc). However, Directive 95/46/EC does not apply to the individual who uploads the data for 'purely personal' purposes or 'in the course of a household activity'.[22] Arguably it does not apply either to the organization that provides the service, i.e. hosts and makes available the information uploaded by the individual (unless the service processes data for its own purposes) insofar as the service provider may not be deemed to be a controller.[23] The result is a situation of lack of safeguards which may need to be addressed, particularly given the increase in the number of such situations. In this context, whoever offers services to a private individual should be required to provide certain safeguards regarding the security, and as appropriate the confidentiality of the information uploaded by users, regardless of whether their client is a data controller. In addition, thought should be given to the question whether data subjects should be given more means to execute their rights on the internet, including the protection of rights of third parties whose personal data may be object of processing (e.g. social networks). As there are many more unresolved issues in this context,[24] the role of the data subject on the internet should be further clarified, in view of a new legal framework.

6. Strengthening Data Controllers' Responsibility

72. Under Directive 95/46/EC, the data controller is the key actor to ensure compliance with the principles and obligations aimed at safeguarding the protection of personal data of individuals. The Directive, implicitly and in many cases explicitly, requires the data controller to respect data protection principles and fulfil certain specific obligations.[25] Examples of the latter include notifying and prior checking of data processing operations with national authorities.[26] Furthermore, ensuring respect for individuals' data protection rights requires the imposition of corresponding duties upon the data controller such as the provision of information.[27]

---

[22] For a better understanding of whether an activity is covered or not by this 'household exemption', see Opinion 5/2009, on online social networking (WP 163).

[23] This problem does not arise where organizations - either in public or private sector - make use of cloud computing applications, since the Directive applies to them and their processing operations where "carried out in the context of the activities of an establishment of the controller" in the EU (see Article 4.1.a). Chapter 5 thus applies to them, regardless of whether the service provider is established in the EU or not.

[24] Regarding, for example, the consent of children and/or their parents, access requests by law enforcement, access rights to internet accounts by heirs of deceased people, and third party applications.

[25] Article 6 (2) explicitly provides that "it shall be for the controller to ensure that paragraph 1(which refers to the main principles relating to data quality) "is complied with".

[26] See Articles 18-21 of Directive 95/46.

[27] Other examples of data subjects' rights include the right to access, rectification, erasure and blocking, and to object to the processing of personal data (Articles 10-12 and 14). These rights entail obligations for the controller to satisfy them.

73. These obligations also apply - directly or indirectly - to data processors when/if data controllers have entrusted all or part of the data processing operations to them. To provide guidance on the concept of data controller and processor, the WP29 is currently engaged in drafting an interpretative opinion. The WP29 envisages to soon advise the Commission on this topic. This advice might include further recommendations for a future legal framework.

Embedding data protection in organisations

74. The relevant provisions of Directive 95/46/EC form an undeniably solid base for the protection of personal data and should be maintained. Nonetheless, compliance with existing legal obligations often is not properly embedded in the internal practices of organizations. Frequently, privacy is not embedded in information processing technologies and systems. Furthermore, management, including top level managers, generally are not sufficiently aware of and therefore actively responsible for the data processing practices in their own organizations. The data protection scandals that have taken place in some Member States in the last few years support this concern.

75. Unless data protection becomes part of the shared values and practices of an organization, and unless responsibilities for it are expressly assigned, effective compliance will be at risk and data protection mishaps will continue. In turn, this may undermine public trust and confidence in business and public administrations alike. Moreover, embedding data protection in organizations' cultures will assist national DPAs in their supervision and enforcement tasks, as further developed in Chapter 7, strengthening the effectiveness of privacy protections.

76. The principles and obligations of Directive 95/46/EC should permeate the cultural fabric of organizations, at all levels, rather than being thought of as a series of legal requirements to be ticked off by the legal department. The Directive's requirements should result in concrete data protection arrangements being applied on a day-to-day basis. Privacy controls should be integrated into the design of information technologies and systems (see also Chapter 4). Furthermore, within the organizations, both in public and private sectors, internal responsibility for data protection should be properly recognized, strengthened and specifically assigned.

77. The effectiveness of the provisions of Directive 95/46/EC is dependent on data controllers' effort towards achieving these objectives. This requires the following proactive measures:

- *Adoption by data controllers of internal policies and processes* to implement the requirements of the Directive for the particular processing operations carried out by the controller. Such internal policies and processes should be approved at the highest level within the organization and therefore be binding for all staff members.
- *Putting in place mechanisms executing the internal policies and processes, including complaints procedures (see also Chapter 5),* in order to make such policies effective in practice. This may include creating data protection awareness, staff training and instruction.
- *Drafting compliance reports and carrying out audits, obtaining third-party certification and/or seals* to monitor and assess whether the internal measures adopted to ensure compliance effectively manage, protect, and secure personal data (see also Chapter 4).

- Carrying out *privacy impact assessments*, particularly for certain data processing operations deemed to present specific risks to the rights and freedoms of data subjects, for example, by virtue of their nature, their scope or their purpose.
- *Assignment of responsibility for data protection* to designated persons with direct responsibility for their organizations' compliance with data protection laws.
- *Certification of compliance by top level company executives* confirming that they have implemented appropriate safeguards to protect personal data.
- *Transparency of these adopted measures* vis-à-vis the data subjects and the public in general. Transparency requirements contribute to the accountability of data controllers (e.g. publication of privacy policies on the internet, transparency in regard to internal complaints procedures, and publication in annual reports).

78. Article 17 (1) of Directive 95/46/EC, to some extent, already requires data controllers to implement measures, of both technical and organizational nature (the data controller must *"implement appropriate technical and organizational measures to protect personal data against.... unlawful forms of processing").* These measures may include some of the above measures. However, in practice Article 17 (1) has not been successful in making data protection sufficiently effective in organizations, also due to different approaches taken in the national implementing measures.

Accountability principle[28]

79. To address this problem, it would be appropriate to introduce in the comprehensive framework an accountability principle. Pursuant to this principle, data controllers would be required to carry out the necessary measures to *ensure* that substantive principles and obligations of the current Directive *are observed* when processing personal data. Such provision would reinforce the need to put in place policies and mechanisms to make effective the substantive principles and obligations of the current Directive. It would serve to reinforce the need to take effective steps resulting in an internal effective implementation of the substantive obligations and principles currently embedded in the Directive. In addition, the accountability principle would require data controllers to have the necessary internal mechanisms in place to *demonstrate compliance* to external stakeholders, including national DPAs. The resulting need to provide evidence of adequate measures taken to ensure compliance will greatly facilitate the enforcement of applicable rules.

80. In any event, the measures expected from data controllers should be scalable and take into consideration the type of company, whether large or small, and of limited liability, the type, nature and amount of the personal data by the controller, among other criteria.

More options: proactive or reactive

81. Some of the measures described above could be deemed as standard good practice, thus fulfilling the accountability principle if carried out in practice. A built-in reward structure could be foreseen in law to induce organizations to implement them.

[28] See on accountability also Par. 39.

82. An alternative solution could be more prescriptive. For example, Article 17 (1) could be elaborated in order to specify additional proactive measures, such as those outlined above, to be implemented by data controllers. These measures should be orientated towards achieving specific outcomes and should be technologically neutral.

83. Other measures would be of a more reactive nature. They would apply when there has been an unlawful processing of personal data and might, inter alia, involve the following:

- *Setting up a mandatory security breach notification obligation* (see also Chapters 2 and 5).
- *Reinforcement of enforcement powers of DPAs*, including the imposition of concrete requirements to ensure an effective protection (see also Chapter 7a).

Simplification of notifications

84. Notifications of data processing operations with national DPAs could be simplified or diminished. In this context, the link between compliance with the requirements mentioned above and the possibility to further nuance the administrative requirements, in particular the notification of data processing activities with national DPAs, should be explored.

85. Notification contributes to the awareness of the data processing operations and data protection practices within organizations.[29] It also gives DPAs an overview of data processing activities. However, better data governance and accountability requirements may achieve the same purposes. Those mechanisms might help to carry out the necessary measures to observe the substantive principles and obligations currently embedded in the Directive and to produce evidence of such compliance.

86. It should be explored whether and to what extent notification could be limited to those cases where there is a serious risk to privacy, enabling DPAs to be more selective and concentrate their efforts to such cases. Even in such cases, notification could be streamlined, for example, by providing the results of privacy impact assessments, or the outcome of third-party auditing. This could be combined with a registration system whereby all data controllers would be enrolled in a registry maintained by the DPA, to ensure the easy identification of organizational entities for efficient and effective enforcement when necessary.

7. Stronger and clearer roles for DPAs and their cooperation within the EU

7a. Data Protection Authorities

87. At the moment, there are big differences regarding the position of the DPAs in the 27 Member States. This is due to the differences in history, case law, culture and the internal organization of the Member States, but also because Article 28 of Directive

[29] These views are further confirmed by the WP's report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union (WP 106), adopted on 18 January 2005.

95/46/EC lacks precision in several aspects. On top of that, the Directive has, to a certain extent, been poorly implemented in some jurisdictions. This has resulted in large divergences between the Member States regarding, amongst others, the position, resources and powers of DPAs.

88. The new challenges to data protection (globalisation and the technological changes, Chapters 3 and 4) require strong supervision by DPAs, in a more uniform and effective way. As a consequence, the new framework should guarantee uniform standards as for independence, effective powers, an advisory role in the legislation making process and the ability to set their own agenda by, in particular, setting priorities regarding the handling of complaints, all on a high and influential level.

89. DPAs need to be fully and truly independent. The current Article 28 (1) of Directive 95/46/EC is unclear in this respect as is demonstrated by Case C-584/07 (Commission v. Germany), currently before the European Court of Justice. In the new legal framework DPAs should have:

- complete institutional independence and not be subordinated to any other government authority.
- functional independence and not be subject to instructions by the controlled, in relation to the contents and extent of its activity.
- material independence. They should have an infrastructure which is suited to the smooth conduct of their activities, in particular adequate funding. Sufficient resources should be allocated to the DPAs.

90. The enforcement role of DPAs is becoming increasingly important. DPAs need to be able to be strong and bold, and strategic on intervention and enforcement. The current wording of article 28 of Directive 95/46/EC has resulted in widely diverse enforcement powers. The new framework should require a more uniform approach from Member States in giving the DPAs the necessary powers and it should be more specific in this regard than Directive 95/46/EC. The necessary powers should, amongst others, include the power to impose financial sanctions on controllers and processors.

91. The advisory role of DPAs in the legislation making process is indispensable, as the knowledge that DPAs acquire from investigation and enforcement actions often is necessary in order to improve (data protection) legislation. The advisory role should involve all measures and regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, not just 'administrative measures and regulations'[30]. DPAs should be asked for advice before the draft legislation is adopted. In addition, the new framework should ensure that DPAs have an advisory role towards their national Parliaments and/or other national competent institutions, at the time when the latter are involved in the drafting process of new EU legislation.

92. DPAs need to be able to fix their own agenda when setting priorities with regard to, inter alia, the handling of complaints, including the manner in which complaints are handled.[31] DPAs should in any case be able to take into account whether the

[30] Article 28 (2) of Directive 95/46/EC.

[31] The possibility to be selective can be put in practice in different ways, e.g. by establishing 'fast track' procedures to deal with minor claims.

handling of a certain complaint will sufficiently contribute to the protection of personal data.[32] The new framework should enable the DPAs to 'be selective to be effective'.

93. On the other hand, DPAs need to be accountable for the way they make use of their stronger supervisory role. They should be transparent in this regard and publicly report on the way they operate and the priorities they set. The current wording of Article 28 (5) of Directive 95/46/EC needs to be specified in this regard in the new framework.

7b. Cooperation of Data Protection Authorities

The present legal framework

94. Article 29 of Directive 95/46/EC has set up the Working Party on the protection of individuals with regard to the processing of personal data (WP29) as the institutional body for cooperation among national DPAs. The WP29 has an advisory status and acts independently. Its tasks are set forth in Article 30 (1) of the Directive and include contributing to the uniform application of the Directive, by examining questions covering the application of the national measures, giving opinions on the level of protection in the Community and in third countries, as well as advising (also on its own initiative) on proposals for Community legislation having an impact on data protection or any other matters relating to the protection of persons with regard to the processing of personal data in the Community. The Commission is a member of the WP29 and provides for the Secretariat.

95. The WP29 fulfils its task within the scope of Directive 95/46/EC, as specified in its Article 3 (2). In the area of police and judicial cooperation, the European DPAs have established in 2007 the Working Party on Police and Justice (WPPJ) which fulfils a similar role as WP29, but without a legal basis and a secretariat provided for by an EU Institution. Framework Decision 2008/977/JHA, which introduces data protection principles in that area, does not provide for any institutionalised cooperation of DPAs.

The functioning of the WP29

96. The WP29 now functions for over 10 years and has significantly contributed to achieve the goals of Article 30 of Directive 95/46/EC. The result of many of its activities can be found on its website.[33]

97. The WP29 has constantly worked on how to improve its effectiveness and should continue to pay attention to its own functioning.
Special points of consideration are:

- how can the WP29 effectively contribute to the uniform implementation of EU legislation in national laws and to the uniform application of national law?

---

[32] Criteria which can be applied to determine whether a complaint should be handled are for example whether the complaint relates to a situation which affects a large number of people, concerns a breach of data protection legislation which is not of little importance and probably not an incidental phenomenon, and whether handling the complaint is likely to be successful and does not require disproportionate efforts.

[33] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm?refer=true&theme=blue

- how can it improve its effectiveness vis-à-vis the EU institutions and in particular the Commission, also taking into account the hybrid role of the Commission as member of the WP29, as its secretariat as well as the addressee of many of the opinions of the WP29?

Consequences for the future

98. As a first priority, it should be ensured that all issues relating to the processing of personal data, in particular in the area of police and judicial cooperation in criminal matters, will be included in the activities of the current WP29. A comprehensive legal framework should include a comprehensive advisor and an effective cooperation between supervisory authorities. In a transitional period, before a legislative change is realized, appropriate forms for the WP29 to work closely together with the WPPJ must be found.

99. Other improvements do not require a legislative change.

- The uniform application of national law implementing Directive 95/46 can be achieved within the present legal framework, by further improving the working methods of the Working Party and, where needed, by insisting on a strong commitment by the members of the WP29 to implement the views of the WP29 into national practice.
- In accordance with Article 29 of Directive 95/46/EC, the Secretariat of the WP29 is provided by the Commission. The Secretariat should work in close cooperation with the Presidency of the WP29 and its staff. The tasks of the Secretariat and the Presidency are complementary and they should closely work together in order to enable the WP29 to fulfill its missions in the most efficient manner. While the Secretariat deals with all the logistical aspects of the work of the WP29 and assists the WP29 in preparing its opinions and documents, the Presidency (and the Vice-Presidency) focus mainly on the decision-making process and on the strategy of the WP29.
- Relations with the Commission can be further improved by describing the main roles of both players in a Memorandum of Understanding between the WP29 and the Commission. This Memorandum should also address the resources available for the WP29 so that it can use its full capacity in assuming its assignments. Finally, it should address the functioning of the Secretariat, in order to ensure that both the WP29 and the Secretariat itself have sufficient resources to prepare the opinions and working documents of the WP29. The WP29 will enter into consultation with the Commission on the above in 2010.

8. Data protection challenges in the field of police and law enforcement

100. Data protection in the field of police and justice is a specific subject which requires specific attention, taking into account the complex relation between the activities of the State to ensure security and the protection of the personal data of the individual. The specificity of this area is not only the result of the former pillar structure of the previous EU-Treaties, but is more widely recognised (see for instance the exceptions of Article 13 of Directive 95/46/EC and Declaration 21 attached to the Lisbon Treaty).

Changing context within the EU

101. With the entry into force of the Lisbon Treaty, new perspectives will be created for law making in the field of data protection. The pillar structure will be abolished and with Article 16 TFEU a single legal basis is created for data protection in almost all areas of EU law (see Chapter 2). This does not necessarily mean that the implementation of data protection principles for police and justice should be the same as the rules in other parts of society. Declaration 21, attached to the Lisbon Treaty claims that specific rules for law enforcement area 'may prove to be necessary'.

102. Data protection and data exchange will be important focuses in the Stockholm Programme. Decision making will be based on the notion of the right balance between the needs of law enforcement and the requirements of data protection. New measures should only be taken after a proper evaluation of the existing legal framework.

103. Framework Decision 2008/977/JHA on the protection of personal data in the framework of police and judicial cooperation in criminal matters must be implemented by the Member States before 27 November 2010. This Framework Decision can be seen as a first step towards a general framework in the former third pillar but is far from complete. It is only applicable in cross border situations. It seems to lack essential elements and tools to effectively deal with the changing working methods in the area of law enforcement.

Changing emphasis in law enforcement

104. The last years have shown a shift of emphasis in working methods of the police and the judicial authorities, as far as the use of (personal) information is concerned. This shift was the result of growing needs of the use of information, in order to face new threats resulting from terrorism and organised crime and was stimulated by the technological developments over the last years.

105. The shift of emphasis has several dimensions:

- The use of information focuses on earlier stages in the chain: in addition to the traditional use of information for the investigation and the detection of a specific crime, information is gathered and exchanged in order to prevent possible criminal acts ('preventive policing').
- The use of information focuses on a wider group of persons. Information is gathered and exchanged, not only on persons that are directly related to a crime such as suspects or witnesses, but also on wider groups of the population who are not involved in an investigation (e.g. travellers, users of payment services, etc.).
- The information that is used is more and more technology based. Technology even links disparate factors to predict future behaviour of individuals by means of automated tools (data mining, profiling).
- The information that is used is of a different nature. Information use relies not only on objectively determined information (hard data) but also on information based on evaluation and analysis in the framework of an investigation (soft data). Besides, the distinction between the two may vary depending on the Member States.

- The increased use for preventive purposes of personal information originating from the private sector, like for instance banking/financial data, and passenger data collected by air carriers and CRS.
- Information that is collected for a given, legitimate purpose is increasingly used for different, at times incompatible purposes and tends to growingly converge. Interoperability between systems is an important development but is not a purely technical issue, in particular in view of the risks of interconnection of databases having different purposes.
- More authorities are involved in the use of information, not just police and judicial authorities *strictu sensu* but also other public authorities like authorities responsible for border control and tax authorities, but also national security services.

106. This changing emphasis in law enforcement has led to a dramatic increase of the storage and exchange of personal data in relation to activities of the police and justice sector. The technological possibilities to easily combine information may have a profound impact on the privacy and data protection of all citizens and on the very possibility for them to really enjoy and be able to exercise their fundamental rights, in particular whenever freedom of movement, freedom of speech, and freedom of expression are at issue.

Challenges for data protection

107. Against this background, the challenges for data protection are immense. A future legal framework should in any event address the following phenomena:

- Tendencies may lead towards a more or less permanent surveillance of all citizens, often referred to as the surveillance society. An example would be the combined use of intelligent CCTV-camera's and other tools, like an Automatic Number Plate Recognition, registering all cars entering and exiting a certain area.
- Databases may be used for data mining, and risk assessments of individuals can be composed on the basis of profiling of individuals. This might stigmatize persons with certain backgrounds.
- Analyses made on the basis of general criteria run the risk of high inaccuracies, leading to a high number of false negatives and false positives.
- The processing of personal data of non-suspects becomes more important. Specific conditions and safeguards are needed in order to assess their legitimacy and proportionality and to avoid prejudice for persons that are not (actively) involved in a crime.
- There is an increased use of biometric data, including DNA, which presents specific risks.

Conditions for law and policy making

108. The growing number of sector-specific initiatives adopted or planned may easily lead to overlapping or even distortion measures. Therefore, there may be added value in basing information exchange on a consistent strategy, provided that data protection is fully considered and is an integrated part of this strategy.[34]

[34] A European Information Management Strategy, as currently elaborated by the Council, may - if done correctly - in this context prove to be a useful instrument.

109. The need for evaluation of the existing legal instruments and their application is of utmost importance and should take into account the costs for privacy. Evaluation of existing measures should take place before taking new measures. Additionally, a periodic review of existing measures should take place.

110. Transparency is an essential element. Clear information should be available to data subjects on the use of the information collected and the logic underlying the processing and should only be limited if necessary in individual cases to not jeopardise investigations and for a limited period of time. Access and rectification rights of the data subject should be addressed in a cross border context to avoid that the data subject looses control.

111. Special attention is needed for transparency and democratic control in the legislative process. Privacy impact assessments, appropriate forms of consultation of data protection authorities and an effective parliamentary debate, at national and EU level, should play an important role.

112. The architecture of any system for storage and exchange of personal data should be well elaborated. Some general considerations are:

- Privacy by design and PETS (certification scheme) should determine the architecture. In the area of freedom, security and justice where public authorities are the main actors and every initiative aimed at increasing surveillance of individuals and increasing the collection and use of personal information could have a direct impact on their fundamental right to privacy and data protection, those requirements could be made compulsory.
- Purpose limitation and data minimization should remain guiding principles.
- Access to large databases must be configured in such a way that in general no direct access on line to data stored is allowed, and a hit/no hit system or an index system is in general considered preferable..
- The choice between models with central storage, meaning systems with a central database on EU-level and decentralised storage should be made on transparent criteria and in any event ensure a solid arrangement providing for a clear definition of the role and responsibilities of the controller/s and ensuring the appropriate supervision by the competent data protection authorities.
- Biometric data should only be used if the use of other less intrusive material does not present the same effect.

113. The external dimension. It should be avoided that the stringent regime for the exchange of personal data within the EU will be circumvented. The relations with third states should be based on a clear framework, binding on all parties and on the notion of adequacy. The adequacy regime should be assessed following an evaluation by the national DPAs, if necessary through common mechanisms ensuring consistent implementation and effectiveness.

114. Special attention - including where necessary tailor made safeguards for data protection - is needed for large scale information systems within the EU.

115. Independent supervision, as well as judicial oversight and remedies should be properly addressed. This includes in any event adequate resources and competences for independent supervision.

116. Cooperation between DPAs in charge of ensuring lawfulness of data processing should be strengthened in all matters and integrated in the legal framework, also by envisaging stable mechanisms similar to those currently applying to first pillar matters, in order to foster a harmonised approach across the EU and beyond.

For the Art 29 Working Party

The Chairman

Alex Türk

For the Working Party on Police and Justice

The Chairman

Francesco PIZZETTI