Opinion of the European Data Protection Supervisor

on the data protection reform package

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

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 the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 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],

HAS ADOPTED THE FOLLOWING OPINION

CHAPTER I - INTRODUCTION AND GENERAL REMARKS

I.1. Introduction

I.1.a. Data protection reform package and EDPS consultation

1. On 25 January 2012, the Commission adopted a package for reforming the European data protection framework. The package includes:
   - a Communication entitled 'Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century' ('the Communication');[3]
   - a proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('the proposed Regulation');[4]
   - a proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data ('the proposed Directive').[5]

[1] OJ L281, 23.11.1995, p. 31.
[2] OJ L8, 12.1.2001, p. 1.
[3] COM(2012)9 final.
[4] COM(2012)11 final.
[5] COM(2012)10 final.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

2. The proposed Regulation is supposed to replace Directive 95/46/EC and brings an amendment to Directive 2002/58/EC. The proposed Directive is intended to replace Framework Decision 2008/977/JHA.

3. By letter of 25 January 2012, the EDPS has been asked by the Commission to deliver his Opinion on the package. During the drafting process of the reform package, the EDPS was given the opportunity to submit comments to a previous draft of the proposed texts. Several of these comments have led to changes in the text of the final proposal. The EDPS appreciates having been provided with this opportunity.

4. The reform package of 25 January 2012 is the concretisation of the plans the Commission presented in the Communication 'A comprehensive approach on personal data protection in the European Union', published on 4 November 2010. On 14 January 2011, in reaction to this Communication, the EDPS issued an Opinion setting out his vision for the new data protection framework.[6] The present Opinion builds on the findings presented in that Opinion. It also builds on contributions of the Article 29 Working Party in which the EDPS participates as a member, in particular its opinion of 1 December 2009 on the Future of Privacy.[7]

5. The Article 29 Working Party also intends to issue an opinion on the reform package. The present EDPS opinion and the forthcoming opinion of the Working Party should be considered as the contribution of the supervisory authorities to the legislative process in the European Parliament and the Council.

I.1.b. Context and general assessment

(i) The reasons for a reform of the EU legal framework on data protection

6. The need for data protection has increased in today's world. The importance of having sound rules on data protection has been confirmed by the Lisbon Treaty. This Treaty conferred treaty status on the EU Charter of Fundamental Rights ('the Charter'), and hence on data protection as a binding fundamental right. It enshrined the right to data protection as a right for every individual in Article 16 of the Treaty on the Function of the European Union ('TFEU').

7. Furthermore, the Lisbon Treaty inserted a new, single legal basis for rules on data protection in Article 16 of the TFEU. This single legal basis constitutes the legal impetus for reconsidering the existing EU rules on data protection. However and more importantly: there are several substantial reasons which justify and require a reform of the EU data protection framework.

8. First, technological change: although Directive 95/46/EC has proven its value over the past seventeen years and has never lost its relevance, the rules need an update in light of the rapid development of technological change since its adoption in 1995. This update is also crucial with a view to creating a sustainable environment for further innovation in the years to come.

9. Second, legal certainty: citizens as well as economic actors and public bodies can immensely benefit from modernised data protection rules which create legal certainty

[6] EDPS Opinion on the Communication 'A comprehensive approach on personal data in the European Union' of 14 January 2011, OJ L181, 22.6.2011, p. 1 ('EDPS opinion of 14 January 2011').
[7] See Opinion of the Article 29 Working Party of 1 December 2009 on the future of privacy (WP168).

and regulate data protection in a way which ensures a high level of protection and is effective and efficient at the same time. This also means putting more emphasis on substantive principles and desirable outcomes than on formalities and administrative obligations.

10. Third, harmonisation in the internal market: practice has shown that under the current Directive 95/46/EC, there are still numerous differences between the legislation of Member States which hamper the EU Single Market. Further harmonisation is clearly needed.

11. Fourth, need for change in the area of police and judicial cooperation: at the moment the EU legal framework on data protection in this area constitutes a patchwork of specific EU instruments for data protection. Furthermore, there are differences in the level of data protection with the general data protection rules, currently contained in Directive 95/46/EC. With Article 16 TFEU in place, these rules can now be incorporated in a comprehensive legal framework covering all EU policy areas.

12. Fifth, the global dimension: cross-border data processing and international transfers have tremendously increased over the past years. The international dimension of the current EU rules needs refinement in order to prevent unnecessary obstacles as those experienced today. The EU rules on international data transfer should ensure that there is adequate protection of personal data without an unnecessary restriction of international trade and cooperation.

13. The reform of the EU rules goes in parallel with the modernisation of data protection rules adopted in other international organisations. Currently, in parallel to the EU, the Council of Europe is assessing how the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108') could be amended to face today's challenges.[8] The same exercise is taking place regarding the OECD Privacy Guidelines.[9]

14. This means that the reform of EU rules comes at a crucial point in time and opens a window of great opportunities. If these opportunities are used well, this will reinforce the legal frameworks in the EU and achieve more global privacy at the same time.

15. In light of all this, the EDPS has on several occasions called on the Commission to propose a robust and comprehensive system which would be ambitious and enhance the effectiveness and coherence of data protection in the EU, so as to ensure a sound environment for further development in the years to come.[10]

(ii) General assessment of the reform package

16. The reform package adopted on 25 January 2012 fulfils many of the above expectations. As the EDPS already stated in his reaction on the day of the publication of the package, the proposed Regulation constitutes a huge step forward for data protection in Europe.[11]

---

[8] See Proposals for the Modernisation of Convention 108, T-PD-BUR(2012)01EN, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2012_01_EN.pdf.

[9] See OECD report on The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines, 6 April 2011, available at http://www.oecd.org/dataoecd/22/25/47683378.pdf, see also the Seoul Declaration for the Future of the Internet Economy, 18 June 2008, available at http://www.oecd.org/dataoecd/49/28/40839436.pdf.

[10] See in particular the EDPS Opinion of 14 January 2011.

[11] See press release of 25 January 2012, to be found on the EDPS website (www.edps.europa.eu).

17. The proposed rules in the Regulation will strengthen the rights of individuals and make controllers more accountable for what they do with personal data. Furthermore, the role and powers of national supervisory authorities (alone and jointly) are effectively reinforced. Although the EDPS comments in this opinion on several provisions of the proposed Regulation, he wishes to underline that in general the level of ambition and the overall approach of the Proposal are very positive.

18. The EDPS is particularly pleased to see that the Commission has proposed the instrument of a *regulation* for the general rules on data protection. The EDPS is convinced that a regulation is the right instrument for achieving more effective and coherent data protection in the EU, which will contribute to the further establishment of the EU internal market.[12] The proposed Regulation would be directly applicable in the Member States and will do away with many complexities and inconsistencies stemming from the different implementing laws of the Member States currently in place. The same law would be applicable to the processing of personal data in all Member States. This also means that the Regulation will be a vital cornerstone of the EU 2020 strategy for smart, sustainable and inclusive growth.

19. That being said, the EDPS is seriously disappointed with the proposed Directive for data protection in the law enforcement area. A positive element of the proposed Directive is the fact that, contrary to Framework Decision 2008/977/JHA, domestic processing will also be covered by the EU instrument. However, this widening of the scope of application only has added value if the Directive substantially increases the level of data protection in this area, which is not the case. Compared to the proposed Regulation, many provisions in the proposed Directive are weak, without any evident justification.

20. The EDPS regrets that the Commission has chosen to regulate this matter in a self-standing legal instrument which provides for an inadequate level of protection, by far inferior to the proposed Regulation. This discrepancy will clearly not contribute to the comprehensiveness of the new EU data protection framework, and might also have a negative impact on future initiatives that have been postponed by the Commission to a later stage (see part I.2.a and b below).

21. In the present opinion, the EDPS will analyse the two legislative proposals in greater detail. Chapter II will deal with the proposed Regulation, Chapter III with the proposed Directive. The remainder of the present Chapter is dedicated to a further analysis of the main weakness of the package: the current lack of comprehensiveness of the EU data protection framework has not been remedied.

I.2. Main weakness of the package: lack of comprehensiveness is not remedied

22. The comprehensiveness of a revised EU data protection framework was announced by the Commission in its Communication of November 2010, entitled: 'A comprehensive approach on personal data protection in the European Union',

23. It has been welcomed and endorsed by the European Parliament and the Council. In its Resolution of 6 July 2011, the European Parliament expressed its full engagement with a comprehensive approach.[13] Also the Council, in its conclusions of 24 and 25 February

[12] See EDPS Opinion of 14 January 2011, pt. 64.
[13] See European Parliament Resolution of 6 July 2011, 2011/2025(INI).

2011, referred to a new legal framework based on the comprehensive approach.[14] In its Opinion of 14 January 2011, the EDPS called comprehensiveness a *conditio sine qua non* for effective data protection in the future.[15]

24. Now that the reform package has been adopted, it must be noted that the proposals – in their present form - will unfortunately not contribute to the comprehensiveness of the EU legal framework on data protection.

25. Although it is true that a Regulation as the proposed main instrument for EU rules on data protection, and the application of the proposed Directive to domestic processing, will considerably contribute to the comprehensiveness of the rules on data protection applying at the national level in both areas, these developments alone do not lead to a comprehensive system, as will be explained below.

I.2.a. The data protection framework is only partly covered

26. The data protection rules for EU institutions, bodies and agencies as laid down in Regulation (EC) No 45/2001 have been left untouched as well as all specific acts in the area of police and judicial cooperation in criminal matters, such as the rules for Europol and Eurojust, or the rules on data protection under the Prüm-decision.[16] Also there are at present no rules foreseen for the Common Foreign and Security Policy, based on Article 39 TEU.

27. In its Communication of November 2010, the Commission already announced that it would assess the need to adapt other legal instruments on data protection as a second step. In his opinion of January 2011, the EDPS expressed his dissatisfaction that certain areas would still be excluded from the general legal instruments.[17]

28. The EDPS regrets that in the present Communication the Commission has not used the opportunity to, at least, better explain and commit itself, with use of concrete timetables presenting strict deadlines, to the procedure and future steps regarding the entire reform of the EU data protection framework. There is no mention at all in the Communication of the second step of the reform process. The EDPS encourages the Commission to publicly announce the time schedule on the second stage of the reform process as soon as possible.

(i) Review of Regulation (EC) No 45/2001

29. The EDPS recommends, for the sake of legal certainty and uniformity, incorporating the substantive rules for EU institutions and bodies in the proposed Regulation. In his opinion of January 2011 the EDPS already expressed his preference for this option. A single legal text avoids the risk of discrepancies between provisions and would be the most suitable vehicle for data exchanges between the EU level and the public and private entities in the Member States.[18]

[14] See the Council conclusions of the 3071st Justice and Home Affairs Council meeting of 24 and 25 February 2011.
[15] See EDPS Opinion of 14 January 2011, pt. 34.
[16] See Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), OJ L121, 15.05.2009, p. 37; Council Decision 2009/426/JHA of 16 December 2008, OJ L138, 4.6.2009, p. 14 and Council Decision 2008/615/JHA of 23 June 2008 (the 'Prüm-Decision'), OJ L210, 6.8.2008, p. 12.
[17] See EDPS Opinion of 14 January 2011, pt. 169.
[18] See EDPS Opinion of 14 January 2011, pt. 45. The positive experience with data protection officers in the context of Regulation (EC) No 45/2001 could also contribute to the ongoing debate.

30. Another - although not preferred - option would be that the Commission commits itself to ensure that the rules for EU institutions and bodies are aligned with the new general data protection Regulation and enter into force at the latest when the latter applies. An even earlier moment could be preferable to allow the institutions to gain experience with the new system before it is used in all Member States. It would in any event be clearly unacceptable if the Commission and the other EU institutions and bodies were not bound by the same new rules which apply at Member State level.

31. Moreover, it would be highly undesirable for the EDPS to supervise compliance of EU institutions and bodies with substantive rules which would be inferior to the rules supervised by his counterparts at national level. This would become particularly apparent in the context of the European Data Protection Board, in which the EDPS is supposed to have an active role. Furthermore, it should be noted that Regulation (EC) No 45/2001 is already out of date with regard to electronic communications, being limited to telecoms provisions based on the predecessor of the ePrivacy Directive.[19]

(ii) Specific acts in the area of police and judicial cooperation in criminal matters

32. As regards the specific acts in the area of police and judicial cooperation in criminal matters, it is stated in Article 61(2) of the proposed Directive that the Commission shall review these acts within three year after the entry into force of the Directive. The EDPS believes that such a deadline would lead to an unacceptably long period during which the current, widely criticised patchwork remains in force.

33. As a clarification of the entire framework should be provided as soon as possible, the EDPS strongly recommends the legislator to set a much stricter deadline which ensures that the specific rules are amended at the latest at the moment the Directive enters into force.

(iii) Common Foreign and Security Policy

34. The EDPS recommends that the Commission presents as soon as possible common rules for this area, based on Article 39 TEU, and in principle identical to the common rules in other areas.

I.2.b. The two proposed instruments taken together do not create a comprehensive data protection framework

35. As the EDPS has stated before, consistency and comprehensiveness militate in favour of an approach whereby a Regulation sets out the general rules on data protection, complemented by additional sectoral rules.[20] Such a Regulation would indicate the general conditions for restricting certain rights and obligations for the purpose of prevention, detection, investigation and prosecution of criminal offences. Additional specific rules would harmonise national rules adopted in this area as contemplated in Declaration 21 to the Lisbon Treaty.

36. Unfortunately, the Commission has chosen differently. The proposed Directive constitutes a self-standing instrument which contains its own, often different version of the definitions, principles, rights and obligations for the law enforcement sector. This in

[19] Directive 97/66/EC of 15 December 1997, OJ L24, 30.1.1998, p. 1.
[20] See EDPS Opinion of 14 January 2011, pt. 48.

itself complicates the legislative procedure and there is also a great risk that these provisions might be even further amended in ways different from those in the Regulation.

37. The EDPS urges the legislator to ensure that both instruments contain the same essential provisions, and enter into force at the same date. Divergence between equivalent provisions of both instruments should only be allowed if it is duly justified. We encourage the Commission, the Council and the Parliament to come to a commitment that they will do their utmost to ensure consistency of both instruments, in terms of substance as well as on timing.

38. The choice for a self-standing instrument is regrettable and constitutes a missed opportunity to clarify and ensure the consistent application of rules applicable to situations in which activities of the private sector and of the law enforcement sector interact with each other and borderlines are becoming increasingly blurred. Examples of these situations are the transfer of PNR data and data on financial transfers to law enforcement authorities. The Commission itself has acknowledged this shortcoming in the current legal framework. In Annex III of the Impact Assessment of both proposed instruments, Framework Decision 2008/977/JHA is strongly criticised for failing to address the legal uncertainty for situations in which data collected for commercial purposes are used for law enforcement purposes.[21]

39. This also applies to other situations, for instance when information is transferred between a law enforcement authority and a private entity or when a law enforcement authority would transfer data to another public authority not responsible for law enforcement. It becomes even more complex if public information systems are partly established in the area of police and judicial cooperation in criminal matters, and partly in other areas. The clearest example on EU level is the Schengen Information System, which in addition also has national and European parts.[22]

40. As will be discussed in the more detailed comments in Chapter II and III of the present opinion, the provisions which touch on the relation between both instruments do not address the matter in a clear manner.[23] On the contrary, the proposals only seem to add to the confusion in the area. The current proposals might in this respect still lead to diverging national law and inconsistent national practice, and might still raise issues of applicable law. They also do not clarify how the competence between Member States and the EU is divided as regards the negotiations with third countries on the possible transfer of such data.

CHAPTER II - COMMENTS ON THE PROPOSED REGULATION

II.1. Introduction

41. The proposed Regulation is a huge step forward for data protection in the EU. The EDPS supports the proposal because it is based on the correct choice of legal

[21] See Annex III, p. 4.
[22] See Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System, OJ L381, 28.12.2006, p. 4 and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System, OJ L 205, 7.08.2007, p. 63.
[23] See in particular part II.3.a.(iv), II.5.f and III.2.c.

instrument, a regulation, and because of the very welcome substance of many of the proposed changes to the current rules.

42. Nevertheless the proposal gives rise to a number of horizontal issues, such as the relationship between EU and national law, which will be discussed in part II.2 below. In the same part, several other horizontal issues are addressed, namely the possible delegated or implementing acts in relation to many provisions of the proposed Regulation, the special arrangements for micro, small and medium enterprises throughout the Proposal, and the use of the notion of 'public interest'.

43. From part II.3 onwards, the content of the proposed Regulation will be commented upon in greater detail chapter by chapter. The EDPS will underline many positive elements of the proposal, amongst which are:
- the clarification of the scope of application of the proposed Regulation (see part II.3);
- the enhanced transparency requirements towards the data subject and the reinforcement of the right to object (see part II.5);
- the general obligation for controllers to ensure and be able to demonstrate compliance with the provisions of the Regulation (see part II.6);
- the reinforcement of the position and role of national supervisory authorities (see part II.8);
- the main lines of the consistency mechanism (see part II.9).

44. The EDPS will devote most attention to the provisions of the proposal which raise concerns or require further improvement, amongst which are in particular:
- the new ground for exceptions to the purpose limitation principle (see part II.4.a);
- the possibilities for restricting basic principles and rights (see part II.2.a.(iii) and II.5.f);
- the obligation for controllers to maintain documentation of all processing operations (see part II.6.e);
- the transfer of data to third countries by way of derogation (see part II.7.d);
- the role of the Commission in the consistency mechanism (see part II.9.b.(ii));
- the mandatory nature of imposing administrative sanctions (see part II.10.c).

II.2. Horizontal issues

45. A Regulation is the most far reaching instrument of secondary EU law, as it applies directly in all Member States, and will thus create one single applicable law in the whole EU, with priority over any national law that is not compatible with it.[24] It is therefore important to take a closer look at how the proposed Regulation deals with the relationship between EU law and national law in this area.

46. In particular, the issue arises on which points the Regulation should allow some margin for Member States to have national laws which either incorporate provisions of the proposed Regulation to have them fit into their particular national legal order, or lay down specific rules that might be justified for certain areas where there are apparent cultural differences between the Member States.

47. When establishing the proper equilibrium, the EU legislator should consider whether each and every proposed margin for manoeuvre for Member States would perhaps lead

[24] See Article 288 TFEU.

unnecessarily to diverging national laws which would maintain the difficulties under the current Directive 95/46/EC relating to diversity and complexity of applicable law and competence of supervisory authorities.

48. A second issue of general importance arises from the numerous provisions which empower the Commission to adopt delegated or implementing acts. The EDPS welcomes this approach in as far as it contributes to the consistent application of the Regulation, but has reservations insofar as it might at some points build unduly on such acts.

49. Other general issues involving the right balance between diversity and consistency arise in relation to the special arrangements for micro, small and medium enterprises throughout the Proposal, and the extensive use of the notion of 'public interest'. These issues will be further discussed below.

II.2.a. Relationship between EU law and national law

(i) The general approach of the Regulation

50. Although the proposed Regulation goes a long way towards creating a single applicable law for data protection in the EU, a closer analysis of its provisions shows that more space remains for coexistence and interaction between EU law and national law than one might be inclined to think. In fact, there are quite a few examples of provisions where the Regulation clearly *builds* on national law, or conversely allows or mandates national law to build on and thus give *effect* to its provisions. There are also different examples of provisions where the Regulation allows or requires national law to *specify* or further develop its rules in certain areas or even to *depart* from its provisions under certain conditions.

51. Clear examples of the first category - *building* on *national law* - can be found in Article 6 of the proposed Regulation on the grounds of lawful processing. According to Article 6(1), processing of personal data shall be lawful if and to the extent that such processing is (c) necessary for compliance with a legal obligation to which the controller is subject, or (e) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In both cases, the proposed Regulation builds on grounds for processing essentially provided under national law, subject only to further conditions as to the quality of the law in Article 6(3).[25]

52. Examples of the second category - national law *building* on the *Regulation* – relate to the organisation and functioning of supervisory authorities (Articles 46 to 49). Those provisions are needed to respect the institutional and constitutional systems of the Member States, and only oblige them to establish and organise supervisory authorities that are able to execute the tasks entrusted to them in the Regulation.[26]

[25] Since 'processing' as defined in Article 4(3) has a wide scope, this example is relevant for many provisions in national law imposing obligations to collect, store, retain or exchange personal data either in the public or in the private sector, and for a range of other public tasks. Further examples are visible in Article 4(5) on the definition of controller, Article 6(1)(b) on performance of contracts and Article 8(2) with a reference to national contract law.

[26] Other examples are visible in Article 78 on the establishment of penal sanctions, and more implicitly in Articles 73 to 76 on remedies which are likely to require at least some integration in national law, or will be subject to procedural requirements laid down in national law.

53. Examples of the third category – *specifying* or further developing the Regulation – and of the fourth category – *departing* from the Regulation – will be discussed below in more detail, as they are more problematic from the point of view of consistency and diversity.

54. In all these cases, the question may arise as to the scope of the national law. Where the proposed Regulation *builds* on national law (first category), the scope of national law is clearly determined by its own terms and the constitutional system of the relevant Member State. The same will apply in the second category (national law *building* on the Regulation), although the Regulation may in some instances provide additional scope to reach across national borders.

55. In the third and fourth category, the territorial scope of national law may be more problematic in the absence of an explicit provision in the Regulation itself.[27] The EDPS therefore recommends that an explicit provision is included in the Regulation that clarifies the issue of territorial scope of these national laws (see on this point also part II.3.b).

(ii) Specific data processing situations

56. Chapter IX of the proposed Regulation leaves additional room for specific national rules for certain data processing situations mentioned in Articles 80, 81, 82, 84 and 85. These relate to freedom of expression, health, employment, professional secrecy and churches and religious associations.

57. Whilst there is a need to reconcile uniform data protection rules with national specificities, the EDPS is not convinced that these exemptions and derogations are absolutely necessary for all sectors included in Chapter IX as currently proposed, although this may be part of a more general problem (see point (iv) below).

58. In particular with regard to the employment sector, the data protection principles already apply under existing law without prejudice to employment law obligations, as both legal frameworks should be considered as complementary. A legal obligation in employment law could thus, for example, constitute a legitimate basis for processing under Article 6 of the proposed Regulation.

59. Second, Articles 81, 82 and 84 of the proposed Regulation state that the specific national rules should be 'within the limits of this Regulation'. The EDPS assumes that this is intended to prevent derogations to the principles of the Regulation in the different sectors. He recommends replacing this formulation by clear wording stating that national law specifications should be 'without prejudice' to the Regulation.

60. The provisions of Chapter IX on specific data processing situations will be discussed in more detailed in part II.11 below.

[27] Article 4 of Directive 95/46/EC provides currently for some extra-territorial effect of the national law implementing it. See Opinion 8/2010 of the Article 29 Working Party of 16 December 2010 on applicable law (WP 179).

(iii) Other provisions allowing for specifying or derogating national rules

61. Other possibilities for specific national rules are foreseen in a number of other provisions of the proposed Regulation. The EDPS sees different types of provisions allowing for a national margin of discretion, as set out above.

62. The fourth type of provisions is of a different nature and empowers Member States to *depart* from the provisions of the Regulation.

63. The main provision in this respect is Article 21 which permits Union or Member State law to restrict the scope of certain provisions in the Regulation. This provision is presently located in Chapter III of the proposed Regulation on the rights of data subjects, but it has a broader scope than providing for restrictions on the rights of the data subjects, since it also extends to the main principles laid down in Article 5 of the Proposal, such as the principles of lawfulness, fairness, purpose limitation, accuracy and necessity (see also part II.4.a below).

64. Compared to the present Article 13 of Directive 95/46/EC, Article 21 of the proposed Regulation significantly extends the grounds for restrictions beyond the specific interests linked to criminal offences, regulated professions and important economic or financial interests, by including 'other' undefined public interests. However there is no justification for extending the scope of restrictions to such interests and the EDPS considers this provision to be unnecessary and disproportionate. He therefore calls for restricting the use of the public interest exemption to clearly identified and limited circumstances including criminal offences or economic and financial interests.

65. Furthermore, the EDPS recommends that the legislator introduce in Article 21 more detailed guarantees as to the quality of the national law. This will be further discussed in part II.5.f below.

66. Other provisions of the proposed Regulation also allow for national law to restrict the scope of certain provisions. This is the case with Article 6(4) which allows for national law which derogates from the purpose limitation principle, and Article 17(3)(d) which allows national law to require the retention of data even though someone has invoked his or her right to be forgotten. In both cases, the derogations are unnecessary, and Article 21 could be relied upon to restrict the scope of the provisions, if required.

67. The EDPS takes the view that Article 21 should not be supplemented by such specific possibilities for restrictions. Therefore, he recommends deleting or restricting the scope of Article 6(4) and Article 17(3)(d) (see also part II.4.a and II.5.b).

(iv) Other specific national laws

68. In most Member States, there will be a large number of national laws that may not deal with data protection in a formal sense, but nonetheless contain a variety of provisions on the collection, retention, deletion, exchange or publication of personal data, or on the way in which the rights of data subjects should be exercised or respected in a specific field.

69. Many of those laws may come within the scope of Directive 95/46/EC and may have represented part of the implementation of that Directive into national law. In most Member States, such laws will be consistent with the national data protection law, but

may further specify its provisions for a certain area. Such laws will be more frequent in the public sector, but may also be relevant in a range of other areas.

70. It is clear that such laws must be amended if they are not compatible with the proposed Regulation, to the extent to which their provisions would not provide a basis for lawful processing of personal data (see part II.2.a.(i) above) and are not provided for in the Regulation. This would require that such national laws be aligned with the provisions of the Regulation, including the general principle of free movement of personal data within the Union as now expressed in Article 1(3) thereof. It is not always clear what room the Regulation leaves for national law. For instance, to what extent are the provisions of Chapters II and III exhaustive and to what extent are provisions for specific sectors allowed? The EDPS recommends that this issue be examined more carefully, in order to decide whether there is a need for a further provision specifying the extent to which specific national laws are allowed, 'without prejudice to the Regulation', as mentioned above.

II.2.b. Delegated and implementing acts

71. In many provisions of the proposed Regulation the Commission is empowered to adopt delegated or implementing acts. Although such further acts might contribute to the uniform application of the Regulation and allow for further alignment of national practice based on experience gained after the Regulation applies, the EDPS, as said, has reservations as to an approach that builds so heavily on these acts. Furthermore, the EDPS doubts whether all issues are addressed at the correct legislative level.

72. First, if delegated or implementing acts are not yet adopted when the Regulation applies, which seems realistic with a view to the large number of envisaged acts, namely 45, the effective and consistent application of the Regulation may be at risk. For example, this could be the case with the threshold for the personal data breach notification. If no delegated act is in place, every single data breach will have to be notified to the national supervisory authority.

73. The absence of delegated and implementing acts would also have adverse consequences for the enforcement of the rules through the imposition of administrative sanctions, as foreseen in Article 79. A uniform sanction regime in the EU depends heavily on the existence of sufficient clarity about the precise meaning of the relevant rules, where necessary provided by delegated or implementing acts. For example, a failure to comply with the obligation to notify a data protection breach can by fined up to 1 000 000 Euro (see Article 79(6)(h)). Without a clear threshold, national practice might be highly inconsistent with negative consequences for the internal market.

74. Second, it is questionable whether the delegated acts foreseen in the proposed Regulation are all restricted to non-essential elements as required by Article 290(1) TFEU. For instance, the threshold for the personal data breach notification in Articles 31 and 32 constitutes an essential element which should be addressed in the Regulation. Also the elaboration of what constitutes 'a high degree of specific risks' (Article 34(2)(a) and (8)) or 'important grounds of public interest' (Article 44(1)(d) and (7)) should in the EDPS' view not be left completely to delegated acts. The use of vague notions cannot be justified by granting the Commission the competence to adopt delegated acts at some time in the future. Legal certainty requires these notions to be sufficiently defined in the legislative act.

75. Third, the choice between a delegated and an implementing act is not always justified. It should be underlined that the European Parliament has a more limited role in the procedure leading to the adoption of an implementing act. In this respect, the EDPS has particular concerns with regard to the implementing acts foreseen in relation to the security breach notification (Article 31(6)) and the Data Protection Impact Assessment ('DPIA', Article 33(7)).[28]

76. In this light, the EDPS recommends that the legislator reconsider at least the delegation of power in Articles 31(5) and (6), 32(5) and (6), 33(6) and (7), 34(2)(a) and 44(1)(d) and (7). The power to adopt implementing acts on the basis of Article 62 will be discussed separately in part II.9.b.(ii).

II.2.c. The special arrangements for micro, small and medium-size enterprises

77. There are several provisions in Chapter IV of the proposed Regulation on controller and processor which create exceptions for micro, small and medium-size enterprises ('MSMEs'). This is the case with regard to the obligation for controllers outside the EU to appoint a representative (Article 25), documentation (Article 28) and the duty to appoint a data protection officer (Article 35).

78. Furthermore, when the Commission is empowered to adopt delegated or implementing acts, it is stated several times that the Commission shall take the appropriate or specific measures for MSMEs. This is done in relation to processing of personal data of a child (Article 8(3)), procedure and mechanisms for exercising the rights of the data subject (Article 12(6)), obligation to inform the data subject (Article 14(7)), responsibility of the controller (Article 22(4)) and obligation to carry out a DPIA (Article 33(6)).

79. The EDPS acknowledges that the difference in size of an enterprise may have an effect on the weight of the additional administrative burden stemming from the data protection rules. However, data protection is a fundamental right, and individuals are entitled to the same level of protection of their data regardless of whether their data is being processed by a MSME or a large undertaking. This explains that there are no special facilities for MSME in the context of the general principles for data protection applying to all controllers. At the same time, it must be noted that these principles should always be applied in ways that take account of the relevant context. Additional administrative burdens may be lightened so long as the full protection of the data subject is ensured.

80. As will be discussed in part II.6 below on controller and processor, it should also be clear that the exceptions to the provisions of Chapter IV should only relate to *specific* obligations elaborated in Chapter IV and not to the general obligations contained in Article 22(1) and (3). This should be clarified in a recital. That being said, the EDPS considers that some of the exemptions for MSMEs are too broad and suggests to reconsider the specific obligations and the need for a threshold, as will be discussed in part II.6.

81. As to delegated and implementing acts, the EDPS has particular concerns as to the specific measures for MSMEs which the Commission might envisage when it adopts a delegated act for specifying criteria and requirements for the methods of verifiable consent given or authorised by a child's parent or custodian (see Article 8(3)). Furthermore, it is unclear what the Commission will do with regard to the data

[28] For comments on Article 41(3) see part II.7.f and on Article 62 see part II.9.b.(ii).

protection impact assessment, which, according to the EDPS is a crucial new obligation to ensure the accountability of all controllers, be they small, medium-size or large enterprises.

82. The EDPS recommends that the legislator limits appropriate and specific measures for MSMEs to selected implementing acts only, and not to delegated acts, focusing on administrative specifications rather than on substantial measures. He suggests an amendment of Articles 8(3), 14(7), 22(4) and 33(6) in this sense.

II.2.d. The notion of 'public interest'

83. The notion of 'public interest' is used throughout the proposed Regulation, generally to allow for exemptions to the main principles. To give a few examples, as already discussed, Article 21 provides for possible restrictions to the main principles of the proposed Regulation on the basis of legislative measures taken by Member States for undefined public interests. The wording of recital 87 of the proposed Regulation, which refers to *important* grounds of public interest in the context of data flows, shows that the notion of 'public interest' is envisaged broadly, in a criminal, but also an economic perspective, extending to health and social security issues as well.

84. The EDPS objects to the broad use of the notion of 'public interest' in the context of the Proposal. In view of the impact it would have on effective compliance with its main provisions he considers that the notion of 'public interest' should be further refined in each provision of the Proposal where it is mentioned. This is done for instance in the context of the processing of health data, where public interests are listed in relation to the area of public health (including e.g. high standards of quality and safety for medicinal products). The EDPS recommends that specific public interests are explicitly identified in relation to the context of the intended processing in each relevant provision of the proposal.[29] Furthermore, the EDPS recommends considering additional requirements for invoking a public interest. Such additional requirements could be, for instance, that the ground can only be invoked in specifically pressing circumstances or on imperative grounds laid down in law.

85. Concrete suggestions on this point will be made when discussing the different chapters of the proposed Regulation.

II.3. General provisions (Chapter I)

86. The EDPS strongly supports the objective of the proposed Regulation to harmonise and simplify the application of data protection principles across the EU. In a technological environment where data processing is rarely limited to territorial boundaries, this will enhance legal certainty both for individuals and data controllers. The EDPS welcomes the clarification provided by the Proposal on its scope of application and the development of the list of definitions. Some aspects of the text could be clarified or strengthened.

II.3.a. Material scope of application (Article 2)

87. Article 2 of the proposed Regulation refers to the processing of personal data by automated means or as part of a filing system in a way similar to Directive 95/46/EC.

[29] See in particular recital 87, Articles 17(5), 44(1)(d) and 81(1)(b) and (c) of the proposed Regulation.

Paradoxically, considering the horizontal approach to data protection provided by the Lisbon Treaty, the list of exemptions of the Proposal is more developed than in Directive 95/46/EC.

(i) National security

88. As far as the exception for 'activities falling outside the scope of Union law' is concerned, the EDPS wishes to express a more general comment. While 'national security' falls outside the scope of Union law, it is not always fully clear what this notion covers, as it depends on Member States national policy. At national level, the use of the wording 'national security' or 'state security', depending on Member States, with a different scope of application, can also be confusing.[30] Obviously, the EDPS does not contest the exception, but he considers that it should be avoided that it is unduly used to legitimise the processing of personal data outside the scope of the Regulation and the Directive, for instance in the context of the fight against terrorism.

(ii) EU institutions and bodies

89. The specific case of Union institutions, bodies, offices and agencies mentioned in Article 2(2)(b) is presently addressed by Regulation (EC) No 45/2001. As has been discussed in part I.2.a, the EDPS would have preferred the inclusion of the processing of personal data at Union level in the proposed Regulation. As a minimum, Regulation (EC) No 45/2001 should be amended in a way consistent with the present Proposals, and allowing its entering into force when the Regulation starts to apply.

(iii) Personal and household activities

90. With regard to personal or household activities mentioned in Article 2(2)(d), the EDPS regrets that the scope of this exception is not further clarified. Recital 15 indicates that the exception applies in the absence of gainful interest, but it does not address the common issue of processing of data for personal purposes on a wider scale, such as the publication of personal information within a social network.

91. In line with the rulings of the Court of Justice in *Lindquist* and *Satamedia*, the EDPS suggests that a criterion be inserted to differentiate public and domestic activities based on the *indefinite* number of individuals who can access the information.[31] This criterion should be understood as an indication that an indefinite number of contacts shall in principle mean that the household exemption does no longer apply. It is without prejudice to a stricter requirement for a genuine personal and private link, to prevent that individuals making data available to several hundreds or even thousands of individuals would automatically fall under the exemption. The EDPS would also advise adding to recital 15 a clarification as to the activities which may fall within a grey area, such as the website of a local community or a trade union, which may involve a limited number of individuals but should nevertheless be subject to the Regulation.

92. Finally, the EDPS welcomes the precision at the end of recital 15 according to which the exception for personal or household activities does not apply to controllers or processors which provide the means for processing of personal data for such activities. He

[30] This confusion is compounded by references to 'economic well being' of a country. It also leads to problems with security clearances which are conceived differently in the various Member States.

[31] See CJEU 6 November 2003, *Lindqvist*, C-101/01, [2003] ECR I-12971 and CJEU 16 December 2008, *Satamedia*, C-73/07, [2008] ECR I-9831.

understands that this precision implies that information service providers must comply with the Regulation even if their customers use the service in a personal context. This is justified by the fact that providers of services such as social networks or applications in the clouds follow a specific business model independent of the objectives of their customers.

93. The EDPS notes however that the wording of recital 15 is not absolutely clear as it mentions that the household exemption should *also* not apply in that case. Read in the context of the whole recital, it could lead to think that the word 'Regulation' was mistakenly replaced by 'exemption', which would completely change the sense of the recital. The EDPS therefore recommends the deletion of the word 'also' from recital 15.

(iv) Competent authorities for law enforcement purposes

94. According to Article 2(2)(e), the proposed Regulation does not apply to processing of personal data 'by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'. According to recital 16, such processing is subject to the provisions of a specific legal instrument, namely the proposed Directive.

95. The EDPS understands from the proposals that 'competent authorities' subject to the proposed Directive are law enforcement authorities, meaning that their main tasks are related to criminal offences and penalties. The proposed Regulation would apply to all other public authorities.

96. However, the last sentence of recital 16 is not consistent with Article 2(2)(e). It presents as a specific issue (using the wording 'however') the processing of data by public authorities 'under this Regulation' but for law enforcement purposes, stating that this processing will be subject to the principles of a more specific instrument (the proposed Directive). The EDPS suggests making recital 16 consistent with Article 2(2)(e) to avoid any misunderstanding about whether 'non law enforcement' public authorities would fall under the scope of the proposed Regulation.

97. Furthermore, the two Proposals make reference to 'competent authorities' respectively in Article 2(2)(e) of the Regulation and Article 1(1) of the Directive, while the definition of Article 3(14) of the Directive adds the criterion of a 'public' authority. The EDPS suggests aligning the two Proposals by adding in Article 2(2)(e) of the Regulation that the exception applies to competent *public* authorities. A comparable change could also be made in Article 1(1) of the Directive.

98. Finally, the EDPS welcomes the fact that it is clear from both Proposals that private actors processing data in connection with the exercise of official authority are subject to the Regulation and not to the Directive, under possible national restrictions pursuant to Article 21. This is a clear improvement over the current situation where some activities of private actors for law enforcement purposes fall outside of the scope of Directive 95/46/EC, on the basis of the *PNR* ruling of the Court of Justice.[32] However, the EDPS deplores the fact that the conditions under which this kind of processing can take place are not further regulated (see part II.5.f).

[32] CJEU 30 May 2006, *European Parliament/Council and Commission*, C-317/04 and C-318/04, [2006] ECR I-4721.

II.3.b. Territorial scope of application (Article 3)

99. Article 3 of the proposed Regulation deals with the territorial scope of the Regulation. In comparison with the current rules contained in Directive 95/46/EC, Article 3 contains some substantive changes. While the Proposal retains the existing criterion of the processing of data in the context of the activities of an *establishment* of the controller within the EU (Article 3(1)), it is complemented by Article 3(2) which abandons the present criterion of 'equipment' in favour of new criteria consisting of 'offering of goods or services' and 'monitoring behaviour' of data subjects in the Union.

100. The EDPS supports the new criteria aiming at defining when EU law will be applicable to controllers established outside the EU and he welcomes the explanations given in recital 21 on the notion of 'monitoring the behaviour' of the data subject. This new provision is in line with the recommendations made in the Article 29 Working Party opinion on applicable law and in the previous opinion of the EDPS on the review of the data protection framework.[33] He considers that the offering of goods and services or the monitoring of the behaviour of data subjects in the Union makes much more sense and is more in line with the reality of global exchanges of information than the existing criterion of the use of equipment in the EU, under Article 4(1)(c) of Directive 95/46/EC.

101. With regard to controllers established within the EU, the Regulation will apply directly in all Member States and the application of Article 3(1) will be considerably simplified under the new framework. The EDPS fully supports this move towards greater simplification and legal certainty. He would however recommend further clarifying or specifying the criterion of (main) establishment as defined in Article 4(13), as this is an essential element impacting on the role of supervisory authorities. This will be developed further in part II.3.c below.

102. The EDPS notes furthermore that Article 3 of the Proposal only provides for determination of the application of *EU* law. The Proposal does not foresee any criteria for *national* applicable law issues. In principle, a regulation would make a provision on national applicable law useless. However, as highlighted in part II.2.a.(i), Member States keep the possibility to adopt specific legislation on data protection, in the field of employment or health for instance. It is not clear if and on what basis a national and sectoral data protection law or another national law relevant in that context could be applicable beyond the borders of that Member State.

103. The question could arise for example in the case of a multinational company with a main establishment in Ireland, applying specific Irish data protection rules in the field of employment: would these rules apply to its subsidiaries elsewhere? In the context of Directive 95/46/EC, the criterion of the 'context of the activities of the establishment of the controller' of Article 4 could lead to apply Irish rules beyond Irish borders to the other subsidiaries (provided they only execute decisions of the Irish establishment). However in the Proposal there is no criterion to address *national* applicable law issues: the 'main establishment' criteria of the Proposal only allows for determination of the way in which supervisory authorities will be involved. In the interests of legal certainty, the EDPS calls for an additional provision clarifying the status of these cases (see also the comments in part II.2.a.(i)).

[33] See Opinion 8/2010 of the Article 29 Working Party of 16 December 2010 on applicable law (WP179) and the EDPS Opinion of 14 January 2011, pt. 122 and further.

II.3.c. Definitions (Article 4)

104. The definitions of ‘data subject’ and ‘personal data’ are closely related. In comparison with Directive 95/46/EC, all essential elements which define 'personal data' in the present framework have been taken over under the 'data subject' definition in the new Proposal. The main elements of the definitions remain the same, complemented by details on location data and online identifiers, which the EDPS welcomes. He would only suggest on this point to better distinguish in the definition between identifiers (such as an ID number, an on-line identifier) and factors or attributes such as physical, genetic, economic information.

105. In relation to this, the EDPS has strong doubts about the last sentence of recital 24 which mentions that specific 'factors' such as identification numbers or online identifiers 'need not be considered as personal data in all circumstances'. Although, obviously, a unique number such as a bar code taken on its own may not be considered personal data, as soon as this information relates to an individual who can be identified by the controller *or by any other person*, it is personal data. This will in practice most often be the case for identification numbers of personal devices, such as mobile telephones and laptops. The EDPS is concerned that the present wording of the recital could misguide the general understanding of the notion of personal data. He calls for a clearer explanation in the recital along the lines explained above, insisting on the fact that as soon as there is a close relation between an identifier and a person this will usually trigger the application of the data protection principles.

106. The notion of 'main establishment' is developed in Article 4(13). While the EDPS welcomes the precisions of recital 27 referring to the place where main *decisions* as to the purposes, conditions and means of processing are taken, he regrets that the proposal does not address the situation of groups of undertakings, where several legal entities and their establishments in different countries may have a role in determining purposes, conditions and means of a processing activity, independently of the location of the central administration. This situation is addressed in the context of binding corporate rules ('BCRs') but not with regard to the definition of the main establishment, which focuses on the controller and not on the group of undertakings to which the controller and other legal entities in the group belong.

107. The EDPS suggests that criteria to identify the main establishment of the relevant controller are refined in the definition and in the recitals, taking into account the 'dominant influence' of one establishment over others in close connection to the power to implement personal data protection rules or rules relevant for data protection.[34] Alternatively, the definition could focus on the main establishment of the group as a whole. These different options may lead to different outcomes, with different pros and cons for supervisory authorities and companies involved. However, it should be noted that relevant obligations would in all cases continue to be addressed to the controllers, so that the rights of data subjects would not be affected.

108. Finally, the EDPS calls for a definition of the notion of a ‘transfer’ of personal data. He recalls that this has proved to be a problematic issue which has been specifically left by the Court of Justice to the legislator to resolve.[35] Defining what a transfer is and what it is not should be clearly addressed in the Proposal, especially with regard to the network environment, where the difference between actively transferring and making data

[34] Such as for instance rules on whistle blowing.
[35] See the *Lindqvist* ruling of the CJEU cited in footnote 31.

available is becoming theoretic while the consequences in terms of applicable law are huge for data controllers and individuals.

109. In the *Lindqvist* ruling, the Court of Justice made clear that a publication on the Internet did not represent a data transfer.[36] However, how far this reasoning also applies to other types of exchanges on networks, like servers of companies, remains unclear. The EDPS wishes to put forward possible elements which could contribute to identify what a transfer is. The fact that it is aimed at communicating data to identified recipients (rather than making data openly available), could be taken into account, as it justifies the assessment of the level of protection guaranteed by the (country of the) recipient, as well as possible measures to be taken in order to ensure the protection of the data. Other elements to take into consideration are whether the data has been made freely available with the aim of giving access to it and whether the transfer is likely to have actually reached one or more recipients abroad.

110. Finally, the EDPS notes that in Article 3(4) of the proposed Directive a definition is provided on the notion of 'restriction of processing'. In the proposed Regulation this notion is used in Article 17(4) in relation to the right to be forgotten. For the sake of consistency and clarity of the concept of restriction of processing in both Proposals, the EDPS recommends to insert a definition of the notion of 'restriction of processing' also in Article 4 of the proposed Regulation and to further develop this definition (in both Proposals) in line with Article 17(5) of the proposed Regulation (see also part III.5.e).

II.4. Principles (Chapter II)

111. Chapter II of the proposed Regulation provides for the principles to be respected for any processing of personal data (Article 5) and the conditions under which a processing is lawful (Article 6). It also deals with certain specific situations, in particular the processing of special categories of data ('sensitive data') and data processing which does not allow a natural person to be identified.

112. The public consultations launched by the Commission as of 2009 have confirmed that the basic principles enshrined in the Union data protection legislation still remain valid.[37] However they have also shown that these principles should be reconsidered to take into account the rapid pace of technological change and increased globalisation.

113. The EDPS welcomes the fact that Chapter II of the proposed Regulation builds on these well-established data protection principles and provides for significant improvements. In particular the clarification of the notion of 'consent' is very welcome.

II.4.a. Principles relating to personal data processing, including purpose limitation (Article 5)

114. Article 5 of the Proposal introduces several improvements to Article 6 of the current Directive 95/46/EC:
    - According to Article 5(a) personal data must not only be processed lawfully and fairly but also in a transparent manner in relation to the data subject. This useful addition reflects the introduction of stricter obligations on the controller to inform data subjects (see in particular Article 14);

[36] *Ibidem*.
[37] See the Explanatory Memorandum to the proposed Regulation, p. 4.

- The principle of 'data minimisation' is explicitly mentioned in Article 5(c). According to this provision personal data should be limited to the minimum necessary and should only be processed if the purpose of the processing could not be fulfilled by other means. Although, in terms of substance, this obligation already exists under the current rules, the EDPS welcomes the visibility given to it by the addition in Article 5(c);
- According to Article 5(f) the controller has not only to ensure but also to demonstrate compliance with the Regulation. This provision establishes the principle of accountability of the controller which is further specified in Chapter IV.

115. According to the purpose limitation principle, personal data must be processed for a specific purpose and must not be further processed in a way incompatible with the purposes for which they have been collected. This core principle from Directive 95/46/EC is retained in Article 5(b).

116. However, the effectiveness of the purpose limitation principle depends on (1) the interpretation of the notion of 'compatible use' and (2) the possible derogations to the purpose limitation principle, in other words, the possibilities and conditions for *incompatible* use.

117. The EDPS is aware of the fact that the notion of 'compatible use' is interpreted differently in various Member States. Still, the EDPS calls for additional precision in the proposed Regulation.

118. The proposed Regulation constitutes the right instrument to flesh out this principle, possibly inspired by best practices in the way 'compatibility' has been interpreted at national level. The EDPS supports the fact that the issue of compatibility is mentioned as one of the key topics to be addressed by the Article 29 Working Party in its Work programme for 2012-2013.[38] This is likely to provide precious input for a common understanding of the notion of 'compatibility'.

119. As to the possibilities and conditions for incompatible use, the logic of Directive 95/46/EC is that such incompatible use is only allowed subject to the conditions of Article 13 for certain reasons of public interest. In the proposed Regulation this would be Article 21 (see for further comments on this provision part II.5.f below).

120. However, the EDPS notes that a new paragraph 4 is added to Article 6 on lawfulness of processing which opens possibilities to process data for incompatible purposes other than the ones listed in Article 21, and is not drafted as a derogation from the purpose limitation principle. Processing is allowed as long as it has a legal basis in Article 6(1)(a) to (e). Only the ground contained in Article 6(1)(f), the balance of interests, cannot be relied upon for further use for an incompatible purpose under Article 6(4).

121. The EDPS has strong reservations with regard to this new provision, which has broad practical consequences and changes the spirit of the purpose limitation principle as we currently know is. It gives broad possibilities for re-use of personal data in particular in the public sector, in cases based on Article 5(c) and (e) where the controller is subject to a legal obligation, or in case of public interest or exercise of officially authority vested in the controller, without any assurance that the infringement of the purpose limitation principle has been considered separately and adequately.

[38] See Work Programme 2012-2013 of the Article 29 Working Party of 1 February 2012 (WP 190).

122. Also in the case of processing of data for an incompatible purpose in the context of a contract with the data subject, this provision is unwelcome. Although at first sight it could be argued that in this situation the data subject regains control on the situation, in practice the influence of the parties to a contract is not always balanced, and there are strong doubts that an individual would really be in a position to react to an incompatible use of his or her personal data in a contractual relationship.

123. The EDPS recalls that the requirement of compatible use and the requirement of lawfulness are two cumulative locks which aim at ensuring a compliant processing of personal data. The requirement of compatibility cannot be lifted simply by referring to a condition of lawfulness of the processing. This would also be contrary to Article 5 of Council of Europe Convention 108. It is rather Article 21 which should ensure that a change of purpose is done only under strict conditions.

124. Therefore, the EDPS recommends maintaining the logic of Directive 95/46/EC, and not weakening the purpose limitation principle, by deleting Article 6(4), or at the very least restricting its scope to further processing of data for incompatible purposes to the grounds contained in Article 6(1)(a), consent, and 6(1)(d), vital interest of the data subject. This would also require an amendment of recital 40.

II.4.b. Lawfulness of processing (Articles 6, 7 and 8)

(i) Consent

125. The data subject's consent constitutes the first legal ground in Article 6(1) for the processing of personal data provided that certain conditions are met.

126. The EDPS is pleased to see that, building on the recent opinion of Article 29 Working Party[39], the proposal addresses the notion of 'consent' in a comprehensive and suitable manner in order to further specify and reinforce these conditions.

127. Article 7 introduces new and positive elements in particular by imposing the burden of the proof on the controller, by introducing safeguards in the context of a written declaration and by excluding the validity of the consent where there is a significant imbalance between the position of the data subject and the controller. Recital 34 gives some examples of situations where there is a clear imbalance such as the employment context or when the controller is a public authority.

128. Article 8 addresses separately the issue of consent given by a child in the online environment. The requirement of authorisation by a parent or custodian only for children below the age of 13 years is a reasonable approach.

129. Recital 25, which deals in a more general way with the issue of consent in the online environment, has been further elaborated with helpful additions. The EDPS considers that this recital should further specify that when visiting an Internet website there is a need to actively tick a box to ensure valid consent, as pre-ticked boxes do not meet the consent requirements. He also recalls that the burden of proof lies on the controller, and that the reliability of consent can greatly vary depending on the means used, from boxes to tick to electronic signatures. The controller should therefore be attentive to the level

[39] Opinion 15/2011 of the Article 29 Working Party of 13 July 2011 on the definition of consent (WP 187).

of reliability of the means used to obtain consent, in particular by taking into account the sensitivity of the processing. This should all be specified in the recitals. As the controller bears the burden of proof for a valid consent, it is in his own interest to provide for reliable means to obtain consent.

130. Against this background, the EDPS notes that the proposed Regulation does not deal with the issue of the (legal) representation of the data subject in a more general manner. The EDPS recommends including a provision on this matter, covering the representation of all individuals lacking sufficient (legal) capacity or otherwise unable to act. This provision should not only deal with the conditions for consent, but should also address the way in which a representative may exercise the rights of these individuals on their behalf. Due account should thereby be given to the possible conflict of interests between the individual and his or her representative.

(ii) Other legal bases for lawful processing

131. Article 6(1) establishes five grounds under which a processing operation is lawful without consent. This provision is to a great extent similar to Article 7 of Directive 95/46/EC.

132. The main difference is that the legitimate interest of the controller referred to in Article 6(1)(f) would be excluded as a valid ground for processing carried out by public authorities in the performance of their tasks.[40] As explained in recital 38 this is connected to the fact that under Article 6(3) the basis of their processing must be provided only by law.

133. The EDPS recommends adding in a recital further indication of what exactly can be covered by the legal obligation or the tasks carried out 'in the public interest or in the exercise of public authority' as referred to in Article 6(1)(e) of the proposed Regulation. The recital could mention, in the same spirit as recital 27 of Regulation (EC) No 45/2001, that tasks carried out in the public interest include the processing of personal data necessary for the management and functioning of those authorities.

II.4.c. Processing of special categories of data (Article 9)

134. Data relating to criminal convictions and related security measures are part of those personal data which by their nature are particularly sensitive and deserve specific protection. Article 9(2)(j) of the proposal introduces some additional flexibility to the present legal regime under Article 8(5) of Directive 95/46/EC for the processing of such data by others than official authority e.g. by a controller subject to a legal or regulatory obligation.

135. However, it is unclear how Article 9(2)(j) relates to the other grounds for exception in Article 9(2). Especially the reference to the performance of a task carried out for important public interest reasons should be clarified in relation to the ground laid down in Article 9(2)(g). If the intention is to put a higher threshold in Article 9(2)(j) this should be made explicit. Furthermore, the EDPS sees no reason why the requirement of control of official authority should not be extended to all grounds indicated in Article 9(2)(j), including when a task is carried out for important public interest reasons.

[40] Another (unexplained) difference, with practical consequences, is that Article 6(1)(e) and (f) now only refer to the controller and no longer to 'third parties to whom the data are disclosed'.

136. The EDPS also notes that the proposed Regulation no longer includes the processing of data related to offences in the special categories of data. On this point, the scope of this provision is now limited to criminal convictions or related security measures. The EDPS is not convinced that the deletion of this category of data is justified. Furthermore, processing of data relating to matters which have not led to convictions (such as suspicions) should also be included, as it can lead to unfair decisions vis-à-vis the data subject. They deserve in his view the adoption of specific safeguards at least equal to those applying to convictions.

137. The specific rules for processing of data concerning health (see Article 81) will be addressed in Chapter III.11 below.

II.4.d. Processing not allowing identification (Article 10)

138. Article 10 of the proposed Regulation is a new provision establishing that a controller is not obliged to acquire personal information to identify the data subject for the sole purpose of complying with the Regulation. The EDPS understands that this provision does not modify the notion of personal data, nor the scope of the Regulation, but has been added to address practical issues raised especially by data controllers who cannot identify directly the individual behind the data, in particular in the online environment as described in recital 24.

139. However, the EDPS considers that Article 10 should in no way hamper the rights of the data subjects in particular concerning access to their information. Recital 45 already addresses this issue, but it should be made more explicit by explaining that the data controller should not be able to invoke a possible lack of information to refuse a request of access, when this information can be provided by the data subject to enable such access.

II.5. Rights of the data subject (Chapter III)

140. The EDPS welcomes the strengthening of data subjects' rights through, on the one hand, measures reinforcing the obligations incumbent on controllers for ensuring the effective exercise of such rights (e.g. the obligation to adopt procedures and mechanisms, to respond to access requests within set deadlines, to give reasons for their refusal to take action, or to inform recipients of any rectification or erasure) and, on the other hand, the reinforcement of the scope of current rights (such as the right to erasure, which has been strengthened into a right to be forgotten) as well as the creation of a new right to data portability.

141. However, the extent to which the right to be forgotten may be enforceable in practice remains unclear. Furthermore, the scope of the limitations that can be applied to the exercise of data subjects' rights has been extended without being well defined, which would call for the implementation of additional safeguards to ensure that such rights are not unduly restricted.

II.5.a. Transparency and information to data subjects (Articles 11 and 14)

142. The provisions on transparent information and communication constitute a significant improvement of the existing provisions set forth in Articles 10 and 11 of Directive 95/46/EC. The EDPS welcomes the explicit, general obligation on controllers to communicate with the data subject about data protection using clear and plain language (see Article 11 of the proposed Regulation). Furthermore, the EDPS welcomes the specification of the type of information that must be provided by the controller to the data subject when his or her personal data is collected.

143. In this respect, Article 14 provides a list of all the information that must be provided by the controller to the data subject on a mandatory basis. This may include 'any further information necessary to guarantee fair processing' (see Article 14(1)(h)).

144. The EDPS recommends clarifying in Article 14 that such additional information should in particular cover information on the existence of certain processing operations which have a particular impact on individuals, such as those for which a personal data impact assessment indicates that there is a high risk (see Article 33) and measures based on profiling (Article 20), as well as the consequences of such processing on individuals. This modification would also make Article 14 consistent with other provisions of the proposed Regulation where such a right to information about profiling is clearly mentioned, namely Article 15(1)(h) on the right of access and Article 20(4) on measures based on profiling.

145. It should be noted, at the same time, that Article 14 does not stand in the way of best practices using 'multi-layered notices', which allow different layers of information, offering individuals all the information needed to understand their position and make decisions, in a more understandable form.[41] Nor does it require providing information where the data subject has already received it before, thus enabling the controllers to organise information activities in the most efficient and effective way.

II.5.b. Right to be forgotten and to erasure (Article 17)

146. The right to erasure has been strengthened into a right to be forgotten to allow for a more effective enforcement of this right in the digital environment. The controller will be held liable in cases where he has made personal data public or has authorised a third party publication of the data.[42] However, the obligations are limited to taking 'all reasonable steps' to inform third parties which are processing the data that a data subject requests them to erase any links to, or copy or replication of that personal data. These 'reasonable steps' may consist in implementing technical measures.

147. Therefore, Article 17 contains an obligation of *endeavour* upon the controller which is more realistic from a practical point of view than an obligation of *result*. It also reflects Article 13 (on rights in relation to recipients) which provides that the controller should be exempted from the obligation to inform all recipients of any rectification or erasure when this 'proves impossible or involves a disproportionate effort'.

148. The EDPS welcomes this provision, but emphasises that the right to be forgotten must be effective in reality. It may in some cases be a huge effort to inform all third parties

[41] See on multi-layered notices: Opinion 10/2004 of the Article 29 Working Party of 25 November 2004 on more harmonised information provisions (WP 100).
[42] The notion of 'authorisation' of a third party publication is not defined and needs further clarification.

who may be processing such data, as there will not always be clear understanding of where the data may have been disseminated. To have an effective right to be forgotten implies that the scope of the right should be clear from the moment the Regulation applies. Article 17 might need to be further developed in that respect.

149. Article 17(3) provides grounds for an exception to erase the data without delay. This paragraph duplicates, and hence has no added value for, the system of exemptions, restrictions and specific rules already foreseen in the proposed Regulation (see also the comments in part II.2.a.(iii)). In particular Article 17(3)(d) will only create confusion. A restriction of the purpose limitation principle and of the rights of the data subject (including Article 17) should be based on Article 21, subject to the comments made in part II.5.f below. Therefore, the EDPS recommends deleting Article 17(3).

II.5.c. Right to data portability (Article 18)

150. Article 18 creates a new right allowing data subjects to obtain a copy of their personal data undergoing processing in an electronic format and to transmit it from one electronic service provider to another. According to the EDPS, the relationship of the right for data subjects to obtain a 'copy' of their data under this provision with their right to obtain 'communication of the personal data undergoing processing' under the exercise of their right of access should be further clarified.

151. Furthermore, the text of Article 18(2) seems to limit the scope of the right to data portability to personal data that has been provided by the data subject on the basis of consent or a contract. This raises the question whether the right should not extend to data which has been collected on other grounds as well.

152. As to the substance of the right, it is unclear from the current text how the right to data portability relates to the right of erasure and whether data should be deleted by the controller once the right has been invoked. The use of the word 'copy' in Article 18(1) seems to imply otherwise. However, the data controller is always subject to the obligation to delete data when they are no longer necessary for the purpose for which they were processed (Article 5(e)), except in cases where the controller would still have a valid legal basis for continuing to process some of the data (e.g. to comply with a legal obligation, such as for tax purposes). The EDPS recommends that it is clarified in Article 18 that the exercise of the right to data portability is without prejudice to the obligation to delete data when they are no longer necessary, according to Article 5(e).

II.5.d. Right to object (Article 19)

153. The EDPS welcomes the intention of the Commission to strengthen the right to object. The modifications to the right to object are meant to improve the right currently provided in Article 14 of Directive 95/46/EC. In particular because the threshold of demonstrating 'compelling legitimate grounds' in relation to the specific situation of an individual (see Article 14(a) of Directive 95/46/EC) would no longer be required from the data subject. The burden of proof would shift to the controller whenever he would refuse to enforce the objection received from a data subject.

154. However, it should be further clarified what the practical consequences are if the right is invoked. In Article 19(3) it is stated that if an objection is 'upheld', the controller shall *no longer use or otherwise process* the personal data concerned. This raises the question when and how an objection is 'upheld'. Furthermore, it is not made explicit what the

controller is supposed to do with the data if there is disagreement with the data subject and no decision by, for instance, a supervisory authority has yet been taken.

155. From Article 17(1)(c) it seems to follow that the data should in principle be erased: the data subject shall have the right to obtain from the controller the *erasure* of his or her personal data and the abstention from further dissemination if the data subject objects to the processing pursuant to Article 19. It is not clear whether the exceptions provided in Article 17(4)(b), which allow the restriction instead of erasure of data, can be invoked if there is disagreement about whether the right to object should be upheld. The EDPS recommends that the legislator clarify the relation between Article 17 and Article 19 and addresses clearly what the controller should do in case of disagreement with the data subject.

156. Furthermore, the EDPS recommends that it is explained in a recital what may qualify as 'compelling legitimate grounds' justifying the refusal of the exercise of the right to object.

II.5.e. Measures based on profiling (Article 20)

157. Article 20 builds upon the existing Article 15 of Directive 95/46/EC on automated individual decisions, and extends its scope to all types of measures which produce legal effects on a natural person, not only to decisions. It would apply not only to processing intended to evaluate certain personal aspects but also to those activities carried out to analyse or predict these aspects, therefore encompassing a broader category of processing. It also introduces a number of categories of personal aspects which would fall under the scope of this provision, such as processing concerning an individual's economic situation, location, health and personal preferences.

158. Article 20(2) sets forth the conditions under which this type of processing may take place by way of derogation. Article 20(2)(a) provides data subjects with the right to have human intervention but not with the right to submit their point of view, as is currently provided for in Article 15 of Directive 95/46/EC. The EDPS recommends that the latter right be restored to Article 20(2)(a). Such a right would notably allow individuals to be heard before a measure which significantly affects them is taken. This would reinforce the fairness of such a processing.

II.5.f. Restrictions (Article 21 and recital 59)

159. In Article 21, the proposed Regulation introduces a number of possible restrictions to the rights and obligations set forth in the Regulation. The provision has already been briefly discussed in part II.2.a.(iii) above. As said there, the provision is placed in the wrong chapter of the proposed Regulation since it does not only relate to data subjects' rights. Furthermore, the EDPS calls for restricting the use of the public interest exemption in this provision to clearly identified and limited circumstances including criminal offences or economic and financial interests (see also part II.2.d above).

160. The scope of possible restrictions has been considerably expanded in comparison to what is currently provided for in Article 13 of Directive 95/46/EC. All the rights of the data subject can now be restricted on the basis of Article 21 (including the right to object, and measures based on profiling). Furthermore, restrictions are possible as regards the basic data protection principles contained in Article 5(a) to (e) and the obligation to notify a personal data breach to the data subject (Article 32).

161. The restrictions must be laid down in Union or Member State law. The EDPS considers that a law based on Article 21 must meet the criteria of any law derogating from a fundamental right, as recalled in recital 59, and in particular the criteria of necessity and proportionality. It is not sufficient for such a law only to specify the objectives and the controller of the processing, as foreseen in Article 21(2).

162. The EDPS therefore recommends introducing detailed guarantees in the text of Article 21, namely that such law should specify the objectives pursued by the processing, the categories of personal data to be processed, the specific purposes and means of processing, the controller, the categories of persons authorised to process the data, the procedure to be followed for the processing, and the safeguards against any arbitrary interferences by public authorities. There is a need to define with sufficient clarity and certainty the specific areas for which the law should provide detailed guarantees in order to preserve the data subjects' legitimate interests in cases where such a restriction is applied. To avoid diverging interpretations, these restrictions should be further harmonised at EU level.

163. Furthermore, additional safeguards should also be included in Article 21 along the lines of those provided in Article 20(2) to (5) of Regulation (EC) No 45/2001, such as the information of data subjects of a restriction and of their right to refer the matter to the supervisory authority to obtain indirect access through the supervisory authority in each case where their right to direct access is restricted pursuant to Article 21.

164. This leads to another, more specific issue, namely the application of the restrictions under Article 21 to data collected by private controllers for law enforcement purposes, which could lead to their further processing without having to respect any of the basic guarantees listed in Article 5. It should be made clear in Article 21 that the possibility of applying restrictions to the processing performed by private controllers for law enforcement purposes should not force them to retain data in addition to those strictly necessary for the original purpose pursued nor to change their IT architecture for the purpose of responding to any possible request from a law enforcement authority.

165. The EDPS suggests deleting the ground contained in Article 21(1)(e) which allows restrictions in case of 'monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority' in case of public security, criminal offence or other public interests. Although this wording is not new (see Article 13(1)(f) of Directive 95/46/EC), the EDPS takes the view that the wording is too vague with regard to the nature of the connection with the exercise of official authority, especially if and to the extent private actors would be processing personal data in connection with the exercise of public authority. In any event, the other grounds of Article 21(1) already provide for sufficient flexibility.

II.6. Controller and processor (Chapter IV)

166. The EDPS welcomes the major improvements set forth in Chapter IV. This chapter introduces the increasingly well-known ‘principle of accountability’, which lays down a greater emphasis on the responsibility of the controller.[43] As a general rule the controller must adopt policies and implement appropriate measures to ensure and be able *to demonstrate* compliance with the data protection rules, and to ensure that the

[43] Opinion 3/2010 of the Article 29 Working Party of 13 July 2010 on the principle of accountability (WP 173).

effectiveness of the measures is verified (see Article 22(1) and (3)). Notwithstanding the difficulty of translating this concept, the EDPS recommends making an explicit reference to the principle of accountability, in any event in recital 60.

167. In this context, the proposed Regulation introduces the principles of data protection by design and by default and the obligations to keep documentation of all processing operations, to notify security breaches, to perform a data protection impact assessment before starting certain processing operations which might lead to a prior consultation of the supervisory authority, and to designate a data protection officer.

168. Throughout this Chapter, exceptions are provided for MSMEs as well as for public authorities. In this respect, the EDPS wishes to repeat the comment made in part II.2.c that these exceptions should only relate to the specific obligations set forth in Chapter IV and not to the general obligations contained in Article 22(1) and (3). This is reflected in the current text of the proposed Regulation, which the EDPS fully supports.

169. This being said, although there is a need to take account of the size of a specific enterprise when implementing the specific obligation, the EDPS considers that some of the exemptions for MSMEs are too broad and some of the specific obligations too detailed. Moreover, the exceptions for public authorities are not always justified. These points will be elaborated below.

II.6.a. Responsibility of the controller (Article 22)

170. Article 22(1) develops the general principle contained in Article 5(f) of the proposed Regulation, namely that the controller should ensure and demonstrate compliance with the Regulation. This leads to the general obligation to actively adopt policies and implement 'appropriate measures' which enable it to comply with this principle. As said, the EDPS welcomes this general obligation as it underlines the new approach based on the accountability of the controller.

171. Article 22(2) lists what measures in particular are intended by the first paragraph of Article 22. The EDPS welcomes this specification, subject to some further comments, and also supports the fact that the list is not presented as exhaustive. The general principle of accountability should not be interpreted as limited to the specific obligations referred to in Article 22(2).

172. Article 22(3) contains an important additional element for the controller, namely that it should also implement mechanisms to ensure the verification of the 'effectiveness' of the measures referred to above. This obligation applies without exception, although the way in which the verification should be carried out – e.g. by an independent internal or external auditor – depends on the specific circumstances (proportionality).

173. At the core of the general obligations are therefore the requirements that the measures should be *appropriate* and *effective*. This second element follows only indirectly from the language of Article 22(3). The EDPS takes the view that it would be better to express both elements in Article 22(1) and recommends amending the provision accordingly.

174. The term 'appropriate' implies that the measures should take account of the context and the specific circumstances of the case. This is an important element that ensures the

'scalability' of the general obligation in practice, i.e. that effective measures can be required under *all* circumstances in a way appropriate for the relevant case.

175. Which measures may be required – other than those specifically referred to in Article 22(2) – remains unclear, although Article 22(4) provides for delegated acts to specify them. However, it follows from Article 37 on the tasks of the data protection officer, that assignment of responsibilities, training of staff, and adequate instructions are among them. It is also reasonable to expect that the controller should at least have an overview and a general inventory of the processing operations within the scope of its responsibility. The EDPS recommends including such elements in a general provision preceding the specific obligations in Article 22(2) and further developing the concept of 'management control'.

176. To increase the public accountability of controllers, the EDPS also recommends inserting a new paragraph in Article 22 providing that the controller – either voluntarily or under a legal obligation - publishes a regular report of its activities. This report should also contain information on the policies and measures referred to in Article 22(1) and the verification of their effectiveness under Article 22(3).

II.6.b. Data protection by design and by default (Article 23)

177. The EDPS is pleased that the principles of data protection by design and data protection by default have been included explicitly in the proposed Regulation.

178. According to the principle of 'data protection by design', the controller should take data protection requirements into account from the outset when defining a processing operation. The EDPS welcomes the fact that the principle has been further substantiated in Article 23(1). In particular, the EDPS supports the introduction of references to 'the state of art and the cost of implementation' on the one hand and of 'appropriate technical and organisational measures and procedures' on the other hand.

179. Article 23 does not address the way a processor can be bound by the principle of data protection by design. However, the EDPS sees a link between this provision and Article 26 which deals with the processor in general. According to Article 26(1), the controller has to choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the Regulation. Nonetheless, the EDPS would recommend that the legislator also underline the obligation of the processor itself to take account of the principle of data protection by design while processing personal data on behalf of the controller. This obligation could be added to the list of specifications contained in Article 26(2).

180. Article 23(2) contains the principle of data protection by default, but it is not given a clear substance. The first sentence does not add much to the general principles of data processing in Article 5, and the data minimisation principle in Article 5(c) in particular, except from the confirmation that such principles should also be embedded in the design of relevant systems.

181. The principle of data protection by default aims at protecting the data subject in situations in which there might be a lack of understanding or control on the processing of their data, especially in a technological context. The idea behind the principle is that privacy intrusive features of a certain product or service are initially limited to what is

necessary for the simple use of it. The data subject should in principle be left the choice to allow use of his or her personal data in a broader way. The EDPS recommends including in Article 23(2) a reference to this position of the data subject and providing the necessary clarification in recital 61.

182. The principles of data protection by design and by default are not presently addressed to advisers, developers and producers of hardware or software. However, they will be relevant for them from the start, as controllers are bound by them and accountable for compliance. In other words, obligations for controllers (and for processors, as mentioned above) are likely to create some incentives for the market of relevant goods and services.

II.6.c. Joint controllers (Article 24)

183. Article 24 deals with the situation where a controller defines a processing of personal data jointly with others ('joint controllers'). The EDPS supports the idea of making compulsory an arrangement between them. However the responsibility in situations where there is no determination of the respective responsibilities in the arrangement or no arrangement at all needs to be clarified. A solution might be to make joint controllers jointly responsible and to provide that the data subjects may exercise their rights with each of them.

II.6.d. Representatives of controllers not established in the Union (Article 25)

184. According to Article 3(2) and Article 25(1), a controller not established in the Union which processes personal data of data subjects residing in the Union has to designate a representative in the Union. Such a representative has an important role to play under the Regulation in particular as a contact point for data subjects (Article 14 (1)(a)) or for the supervisory authority (Article 28(3) and Article 29) and in case of infringements of the provisions of the Regulation (see Article 78).

185. Article 25(2) provides significant exceptions to this obligation in particular for enterprises employing less than 250 persons, public authorities, and controllers located in a country recognised as providing an adequate level of protection or in the case of occasional offers of goods and services.

186. The EDPS does not understand why there should be an exemption from the obligation to have a representative for controllers located in third countries with an adequate level of data protection. The fact that the third country ensures an adequate level of protection in that third country does not have any bearing on the fact that the EU should have a point of contact for enforcing compliance with the data protection rules *on the EU territory*. Therefore, the EDPS recommends the legislator to delete Article 25(2)(a).

II.6.e. Documentation (Article 28)

187. Article 28 of the proposed Regulation introduces an obligation for controllers and processors to maintain documentation of the processing operations for which they are responsible. This obligation replaces the general obligation to notify individual processing operations to the supervisory authority under Articles 18(1) and 19 of Directive 95/46/EC. The documentation should be available on request to the supervisory authority. The intention of this change is to reduce the administrative burden on controllers. Article 28(4) provides an exemption for a natural person without

a commercial interest or for an enterprise or organisation employing fewer than 250 persons where the processing operations do not relate to its main activities.

188. The EDPS welcomes this change of approach, which must be seen in the light of the general principle of accountability, but has serious reservations about the way it has been implemented, which raises doubts whether it would indeed lower the administrative burden generated by the data protection rules as much as expected.

189. It should be noted that Directive 95/46/EC presently allows exemptions and simplifications of the general duty to notify processing operations to the supervisory authority, which have been used extensively in a number of Member States. The introduction of a duty to maintain detailed documentation of all processing operations is therefore likely to create a considerable burden for many controllers. It is also questionable whether the maintenance of detailed documentation of all processing operations is an 'appropriate and effective measure' to ensure and demonstrate compliance with data protection rules in an increasingly dynamic environment, both for small, medium-size and large organisations, and this even more so in the foreseeable future.

190. The EDPS would therefore prefer a different approach for the obligation to maintain adequate documentation, so as to make it appropriate and effective for in principle all controllers. This could be accomplished by combining the most general elements of the present text in Article 28(2)(a), (b) and (h) with a duty to keep an inventory[44] of all processing operations for which the controller is responsible as well as a description of the way in which the controller has ensured that these processing operations comply with data protection rules. This would support the general obligation of accountability and focus more on the desired results. The present obligation in Article 28(3) to make the documentation available to the supervisory authority could then be supplemented by an additional obligation to inform the supervisory authority upon request about the subjects now mentioned in Article 28(2)(c) to (g).

191. In the light of the foregoing, the EDPS recommends that the present exemptions in Article 28(4) be reconsidered. It may well be that these exemptions could be deleted altogether.

II.6.f. Security of processing (Article 30)

192. In Article 30 on security of processing, reference is made to the controller and the processor. The EDPS welcomes that both actors are mentioned, but recommends the legislator to clarify the provision in such a way that there is no doubt about the overall responsibility of the controller. From the text as it currently stands, both the processor and the controller seem to be equally responsible. This is not in line with the preceding provisions, in particular Articles 22 and 26 of the proposed Regulation.

193. Article 30 is quite general as regards substantive requirements. The EDPS welcomes that the risks represented by the processing and the nature of the personal data to be protected are mentioned as elements to determine the appropriate level of security. However, for the provision to be effective, more detailed rules are required. A further description in a recital could be built on the three basic principles of security, namely confidentiality, integrity and availability. According to the EDPS, the Regulation should

[44] A management tool to ensure overview and support implementation of data protection requirements, which is much less detailed than a register of notifications, as currently required under Directive 95/46/EC.

oblige the controller to adopt an information security management approach within the organisation, including the implementation of an information security policy specific to the data processing performed, where appropriate.

194. As already alluded to in part II.2.b, the administrative sanctions foreseen for not complying with appropriate measures relating to security (see Article 79(6)(e)) cannot be imposed, as long as no further specification is given in the delegated and implementing acts announced in Article 30(3) and (4). These acts should therefore be adopted at the moment the Regulation applies.

195. The EDPS notes a link between Article 30(2) and the DPIA as laid down in Article 33 and suggest clarifying this link, by including an explicit reference to the DPIA in Article 30. It should be noted however that the evaluation of risks in the latter case is a wider concept than the DPIA in Article 33.

II.6.g. Personal data breach (Articles 31 and 32)

196. Building on the personal data breach notification in Article 4(3) of the e-privacy Directive 2002/58/EC, the Commission proposes to introduce in Article 31 a general obligation for the controller to notify personal data breaches to the supervisory authority. In addition, under Article 32, the controller is obliged to communicate to the data subject a personal data breach which is likely to affect his protection except where the controller has demonstrated to the supervisory authority that it has implemented appropriate technological protection measures and applied them to the data concerned.

197. The EDPS is pleased to see the introduction of these provisions which can help enhancing both the security of processing and the accountability of the controller.

198. However, as has already been said in part II.2.b, the proposed Regulation fails to specify the criteria and requirements for establishing a data breach and the circumstances in which it should be notified. Both provisions empower the Commission to adopt delegated acts to this end. As stated, the EDPS takes the view that in the absence of such delegated acts, the new obligations cannot effectively be implemented. These acts should therefore be adopted at the moment the Regulation applies.

199. In addition, the EDPS recommends that the Regulation provides in Article 31 for a more realistic time limit than 24 hours after becoming aware to notify the data breach to the supervisory authority (for example no later than 72 hours). Setting a too strict deadline might undermine the effectiveness of the two provisions.

II.6.h. Data protection impact assessment (Article 33)

200. Article 33(1) of the Proposal obliges the controller or the processor to carry out an assessment of the impact on the protection of personal data of the envisaged processing operations where they present specific risks. Article 33(2) provides a non-exhaustive list of such processing operations. Some of these operations must or might require the prior consultation of the supervisory authority (see Article 34(2) and (4) and part II.6.i below). Article 33(3) sets out what a DPIA should entail in greater detail.

201. The EDPS welcomes the insertion of this new provision as it constitutes an important mechanism for ensuring the accountability of the controller. Moreover, it contributes to the practical implementation of the principles of 'privacy by design' and 'privacy by

default'. However, the EDPS is not completely satisfied with the list of processing operations contained in Article 33(2). In particular the limitation of the processing operations in subparagraph (b), (c) and (d) to processing on a large scale basis is not justified. The EDPS takes the view that even on a small scale the operations indicated in these three subparagraphs would require a data protection impact assessment. Moreover, it is not at all clear what could qualify as 'on a large scale'.

202. Article 33(5) provides derogations to this obligation for public authorities or bodies where the processing results from a legal obligation pursuant to Article 6(1)(c) except if decided otherwise by Member States. In recital 73 it is stated that public authorities or bodies should carry out a DPIA if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the task of the public authority or body is based and which regulates the specific processing operation in question. This seems to refer also to processing based on Article 6(1)(e) of the proposed Regulation.

203. Article 33(5) should be aligned with recital 73 in order to prevent any misunderstanding. It should be made clear that for both grounds the exception for carrying out a DPIA only applies if a specific assessment, equal to a DPIA, has already been made in the legislative context.

204. Article 33(6) empowers the Commission to adopt delegated acts which specify the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 33(1) and (2). Also the requirements for the assessment in paragraph 3 can be further specified in a delegated act. In doing so, the Commission must consider specific measures for MSMEs.

205. The EDPS calls upon the legislator to reconsider this provision (see also part II.2.b and c). In its current state it is too vague about what exactly can be specified in the delegated act by the Commission. It should be ensured that the essential elements are sufficiently defined in the legislative act. It should also be clear that the size of a company should never lift the obligation of performing a DPIA with regard to the processing operations which present specific risks.

II.6.i. Prior authorisation and prior consultation (Article 34)

206. Article 34 deals with both prior authorisation and prior consultation. However, only the first paragraph deals with prior authorisation which only applies to one specific issue, namely the transfer of personal data to a third country or to an international organisation. The EDPS recommends moving the first paragraph to Chapter V, on third country transfer, and to limit Article 34 to prior consultation only.[45] This would do more justice to the fact that the cases for prior authorisation have been limited in the proposed Regulation and the fact that the DPIA is linked to prior consultation and not to prior authorisation.

207. In general, the EDPS welcomes Article 34 which builds on the prior checking procedure set out in Article 20 of Directive 95/46/EC and which provides for an appropriate involvement of the supervisory authority prior to processing operations likely to present specific risks, with the possibility of a further intervention, where that is justified.

[45] This would also imply a change of the title of Section 3 of Chapter IV of the Regulation, which is currently somewhat misleading.

II.6.j. Data Protection Officer (Article 35)

208. The proposed Regulation introduces in Article 35 an obligation for the controller or processor to designate a data protection officer ('DPO') to monitor internally compliance with the proposed Regulation where the processing is carried out in the public sector or in the private sector by a large enterprise, or where the core activities of the controller require regular and systematic monitoring of data subjects.

209. The EDPS notes that the function of a DPO is not a complete novelty since it is already an option open to Member States under Directive 95/46/EC and an obligation of the Union institutions and bodies under Regulation (EC) No 45/2001. The EDPS welcomes that building on the positive experience gained, the proposed Regulation dedicates a full section (Section 4 of Chapter 4) to the DPO and makes his mandatory designation of more general application.[46] Indeed, the EDPS considers that the DPO, performing his duties and tasks independently, is a key element of the proposed new legal framework since he would not only have to inform and advise the controller or the processor of their obligations but also to monitor internally the application of the Regulation and finally to act as the contact point of the supervisory authority.

210. It should be emphasized, however, that the DPO should not be seen as the *only* person involved in ensuring compliance with data protection requirements. While it is the main responsibility of the controller and the staff involved in the relevant processing operations to ensure compliance, the DPO has a special role in advising the controller and monitoring the implementation and application of the policies and appropriate measures adopted by the controller. This also explains why the DPO should perform his duties and tasks independently and should not receive any instructions as regards the exercise of his function, as explicitly mentioned in Article 36(2).

211. Given in particular that following Article 35(2) and Article 35(3) a group of undertakings or several public entities may appoint a single DPO, the EDPS recommends that the Regulation should set out a lower threshold than 250 employees for requiring the designation of a DPO in an enterprise. Although this may not be in line with the definition of (M)SMEs, there is no convincing reason not to lower the threshold in the specific area of data protection. In addition, the proposed Regulation should further clarify the scope of Article 35(1)(c) which provides for a mandatory appointment of a DPO where the core activities of the controller consist of processing requiring regular and systematic monitoring of data subjects.

212. According to Article 36(1) the DPO must be involved by the controller in all issues relating to the protection of personal data, and as mentioned, following Article 36(2) the controller must ensure that the DPO can act in an independent manner. In order to further strengthen these provisions, the EDPS recommends that the Regulation should provide additional guarantees, in particular:
    - stronger conditions for the DPO's dismissal, for example by establishing in Article 35(7) an obligation for the controller to inform the supervisory authority;
    - specification of the obligation for the controller or processor set out in Article 36(1), by providing that the DPO should be given access in particular to all information

[46] See also the EDPS Position Paper of 28 November 2005 on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) No 45/2001, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf.

relevant to data protection policies, documentation, personal data breaches, impact assessments and all relevant contacts with the supervisory authority;
- giving the DPO access at all times to data and premises necessary to perform his duties, as done in point 4 of the Annex to Regulation (EC) No 45/2001.

213. In addition, building on the experience gained within the EU institutions and bodies, the EDPS is of the opinion that the DPO has an important role to play in providing information on and raising awareness of data protection within the organisation that has appointed him or her. Therefore, the EDPS recommends that Article 37(1)(a) should be expanded to this extent.

II.7. Transfer to third countries (Chapter V)

214. The provisions on third country transfers have been considerably developed and specified. The current prohibition of any transfers to countries that are not deemed adequate is replaced by a general principle in Article 40 that transfers can take place only if the conditions for transfers set forth in the proposal Regulation are met. The Proposal clarifies that the rules on transfers apply not only to controllers but also to processors as well as to additional recipients in the case of onward transfers.

215. The Proposal maintains the Commission's power to adopt decisions recognising the adequacy or the non-adequacy of a third country, now also involving international organisations. It introduces new criteria for the assessment which no longer take into account the specific modalities of the processing surrounding a data transfer operation or a set of data transfer operations. Instead, Article 41(2)) focuses more clearly on the rule of law and the existence of effective redress mechanisms and of an independent supervisory authority in the third country in question, although a certain role for self-regulation continues to be an option.

216. The proposed Regulation introduces some flexibility by setting forth new mechanisms that may be used to provide adequate safeguards for data transfers to third countries which do not benefit from an adequacy decision (such as a detailed mechanism for the use of BCRs, and the conditions for the use of various types of contractual clauses). The EDPS welcomes these mechanisms which are already used in practice and which will definitely benefit from a clear legal basis in the Regulation.

II.7.a. Applicability of the Proposed Regulation to existing international agreements

217. Recital 79 provides that the Regulation should not affect international agreements concluded between the European Union and third countries regulating the transfer of personal data. The EDPS recommends that the non-applicability of the Regulation to international agreements should be restricted in time to apply only to already existing international agreements. Furthermore, a transitional clause should be inserted in the Proposal providing for the review of these international agreements within a set time in order to align them with the Regulation (e.g. as provided in recital 72 of the proposed Directive). This clause should be included in the substantive provisions of the proposal, and contain a deadline of no longer than two years after the entry into force of the Regulation.

II.7.b. Transfers to third countries that have been declared inadequate (Article 41)

218. It is unclear whether transfers to third countries for which the Commission has adopted a non-adequacy decision would be totally prohibited or would still be possible under certain conditions. This uncertainty stems from a contradiction between the text of recital 82, which is totally opposed to a transfer in such cases and Article 41(6), which states that such prohibition is 'without prejudice to Articles 42 and 44'.

219. Article 42 provides that transfers by way of appropriate safeguards can be done 'where the Commission has taken *no decision* pursuant to Article 41' (emphasis supplied). This would imply that transfers by way of appropriate safeguards would no longer be an option where the Commission has adopted a non-adequacy decision. This outcome would be unjustified as such a decision would only confirm the need for appropriate safeguards in specific cases, and certainly in case of repeated or systematic data transfers, as now applies under Directive 95/46/EC.

220. The EDPS therefore recommends that Article 42 (and recital 82) be modified to clarify that, in the case of a non-adequacy decision, transfers to that country would only be permitted subject to appropriate safeguards or under the derogations set forth in Article 44.[47]

II.7.c. Transfers by way of appropriate safeguards (Article 42)

221. Article 42(1) sets forth the principle that transfers to a third country in the absence of any decision[48] from the Commission on the level of adequacy of that country can only take place if the controller or the processor has adduced appropriate safeguards 'in a legally binding instrument'. However, Article 42(5) allows for such transfers even if the safeguards are not provided for in a legally binding instrument, provided that prior authorisation is obtained from the supervisory authority. In these cases, appropriate safeguards may consist in 'other suitable and proportionate measures justified in the light of all the circumstances' surrounding the transfer (according to recital 83), such as 'provisions to be inserted into administrative arrangements providing for the basis for such transfer' (according to Article 42(5)).

222. In the EDPS' view, the possibility of using non-legally binding instruments to provide appropriate safeguards should be clearly justified and limited only to cases where the necessity to rely on this type of non-binding measure has been demonstrated. In principle, especially as concerns controllers and processors from the private sector, the EDPS sees no reason why there should be any derogation to the obligation to have guarantees clearly defined in a legally binding instrument. Article 42 should be modified accordingly.

223. The necessity to have recourse to non-legally binding safeguards in the public sector should be carefully assessed, in view of the purpose of the processing and the nature of the data. If such recourse is clearly justified, Article 42 should specify the conditions for the use of this possibility.

[47] In line with comments made under II.7.d, transfers between public authorities could also be allowed if there is a legally binding international agreement allowing for the transfer under specific conditions guaranteeing an adequate protection.

[48] See also the comments under part II.7.b on the meaning of these terms.

II.7.d. Derogations (Article 44)

224. It should be made clear in Article 44 that the use of *any* derogation as a justification for a transfer should be interpreted restrictively and be valid only for occasional transfers that cannot be qualified as frequent, massive or structural. This reasoning is in line with the interpretation given by the Article 29 Working Party to the current Article 26(1) of Directive 95/46 on derogations.[49] There is a risk that the protection afforded to individuals under the Regulation would be significantly weakened if any set of transfers, including those that are repeated or massive, could always be justified by one of the derogations and would thus escape from the requirement to enter into appropriate safeguards. The proposed Article 44(1)(h) is insufficient to address this risk.

225. The derogation in Article 44(1)(d), in cases where a transfer is necessary for 'important grounds of public interest', read in conjunction with recital 87 is too broad and would allow data transfers when they are 'required and necessary' for a wide range of important grounds of public interests such as social security, taxation, customs as well as for the prevention, investigation, detection and prosecution of criminal offences without any specific data protection guarantee.

226. The wide character of the public interest grounds which can be used according to this provision as well as in other parts of the Proposal has been criticised earlier (see part II.2.d). If not carefully drafted, these provisions could allow for a number of transfers between public authorities and/or from private entities to law enforcement authorities without any further safeguard. This would be contrary to the spirit of the Regulation and the respect of individuals' fundamental right to data protection.

227. It is not enough that Article 41(5) requires that the public interest is recognised in Union law or in national law to legitimise all transfers under such legal ground. It should be carefully assessed, on a case by case basis, whether the derogation for an important ground of public interest would be applicable to a particular transfer. The EDPS emphasizes that if the transfers are repeated, massive or structural, they should only take place on the basis of an international agreement which provides for appropriate safeguards. The EDPS therefore recommends that Article 44 (and recital 87) is modified to clarify that the possibility to transfer data under such ground should only concern occasional transfers and be based on a careful assessment of all the circumstances of the transfer on a case by case basis.

228. The reference to 'appropriate safeguards' in Article 44(1)(h) and in Article 44(3) should be clarified or preferably replaced by a different notion, as in principle appropriate safeguards for transfers are those listed in Article 42, and possibly further detailed in delegated acts pursuant to Article 44(7). Derogations apply precisely when there are no safeguards according to Article 42.

II.7.e. Disclosures to third countries by virtue of extra-territorial laws, regulations and other legislative instruments (recital 90)

229. The EDPS recommends that the principles articulated in recital 90 should be set forth in a substantive provision in the Regulation. This provision should clarify the conditions under which such requests could be fulfilled.

[49] See Working document of the Article 29 Working Party of 26 November 2005 on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP114).

230. Recital 90 implies that the conditions for such transfers would be met 'where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject'. However, as stated in section II.5.f above, the fact that an EU or national law recognises an important ground of public interest does not in itself provide justification for a transfer to a third country.

231. Furthermore, appropriate guarantees should be in place in such cases, involving judicial guarantees as well as data protection safeguards (including the existence of international or bilateral cooperation agreements on specific issues). It should be further assessed how supervisory authorities could intervene in such cases, whether by giving an opinion or an authorisation on the transfer.

232. Article 44(7) read together with Recital 90 provides that the Commission will specify further in a delegated act the conditions under which an important ground of public interest exists. However, the EDPS considers that the specific grounds of public interest should not be left to delegated acts but should be mentioned explicitly in the text of the Proposal itself as they constitute an essential element of the Proposal.

II.7.f. The use of the examination procedure in the context of third country transfers (Article 41(3))

233. The procedure for adoption of implementing acts to assess adequacy is laid down in Article 41(3) which refers to the examination procedure. The EDPS considers that these decisions should not be taken solely under the examination procedure but addressed through a thorough assessment mechanism with the full involvement of the supervisory authorities, as is currently the case concerning the assessment of adequacy under Article 30(1)(b) of Directive 95/46/EC. The EDPS suggests adding explicitly in Article 66 that the European Data Protection Board ('the Board') shall be consulted in this context.

II.8. Competences and powers of supervisory authorities (Chapter VI)

234. The EDPS welcomes the provisions of Chapter VI of the proposed Regulation which strengthen the independence of supervisory authorities. These provisions recognise that supervision by an independent authority is an essential element of the EU data protection rules. This follows from Article 16 TFEU and Article 8 of the Charter and has been underlined by the Court of Justice in the *Commission/Germany* ruling of March 2010.[50]

235. It is essential that this independence is ensured both from a functional and an institutional perspective. In this respect, the EDPS considers that the provisions which clarify the powers of authorities and the need for adequate resources and infrastructure are crucial.[51] The provisions of the Proposal developed in Article 48(1) concerning the members of the authority are also of particular importance.

236. With regard to the conditions of appointment of members (Article 48), the EDPS considers that further assessment is needed with regard to the present wording of the Proposal. The provision allows appointments either by parliament or by government, which means they can be decided by the government without substantial involvement of the parliament. The EDPS suggests reinforcing the democratic guarantees of

[50] CJEU 9 March 2010, *Commission/Germany*, C-518/07, [2010] ECR I-1885, paras 23 and 50.
[51] Article 47(5) of the proposed Regulation.

appointments by requiring a more systematic role for the national parliaments in the procedure for appointment of members of supervisory authorities.[52]

237. Article 51(2) provides for a 'lead authority' determined by the main establishment of the controller or processor. The EDPS would first refer to the comments made in part II.3.c on the current definition of main establishment. However, regardless of the outcome of that analysis, he takes the view that the role of a lead authority should not be seen as an exclusive competence, but rather as a structured way of cooperation with other competent supervisory authorities, as the 'lead authority' will depend heavily on the input and support of other supervisory authorities at different points in the process.

238. The EDPS welcomes the explicit list of powers for supervisory authorities set out in Article 53. This list contains a number of examples of ordering powers, including the possibility to impose a temporary or definite ban on processing or the suspension of data flows. Non-compliance with such a decision will be subject to the highest category of administrative sanction under Article 79(6)(m).

239. One of the powers mentioned is the power to 'where appropriate, order the controller or the processor to remedy a breach, in a specific manner, in order to improve the protection of the data subject' (Article 53(1)(a)). This power enables the supervisory authority to impose specific conduct where a controller or processor has not acted in compliance with an obligation, and could be used in a wide variety of situations. This underlines the need for flexibility and a broad margin of manoeuvre for supervisory authorities, as also expressed in the term 'where appropriate'.

240. The EDPS emphasizes that this *remedial* power may well be exercised together with and in addition to the *punitive* power to impose an administrative sanction as provided for in Article 79. However, it requires a broader discretion than currently expressed in that provision. Non-compliance with a specific order should in any case normally qualify for a higher administrative sanction than a single breach of the same general provision (see also the comments in part II.10.c). This is also generally in the interest of data subjects. The EDPS recommends modifying the proposed Regulation accordingly.

II.9. Cooperation and consistency (Chapter VII)

241. The EDPS expresses strong support for the cooperation and consistency mechanisms developed in Chapters VII of the proposed Regulation, subject to the comments below on certain details. He considers that these mechanisms will bring simplification to the benefit of data subjects as well as data controllers. They will also ensure stronger enforcement in a consistent way across the EU, which is also important in cases where data controllers operate from outside the EU.

242. The reinforced role of the European Data Protection Board as successor of the Working Party 29 is an essential aspect of the new harmonised framework. The EDPS supports this reinforced role but calls at the same time for a better balance between on the one hand the role of the Board and the supervisory authorities represented in the Board, and on the other hand the wide powers given to the Commission. The powers of the Commission in the context of the consistency mechanism are now unacceptably strong.

[52] See more generally on the involvement of parliaments in the functioning of supervisory authorities, the ruling of the CJEU in *Commission/Germany*, cited in footnote 50.

II.9.a. Cooperation (Chapter VII, section 1)

243. The EDPS welcomes the intention of organising cooperation in a more structured way, and he supports obligations to exchange information or organise joint investigations. His understanding is that these provisions relate to procedures and should not impede on national sovereignty (see also part II.8).

244. The EDPS has no further specific comments with regard to the co-operation procedure as developed in Articles 55 and 56.

II.9.b. Consistency (Chapter VII, section 2)

(i) Further refinement of the consistency mechanism

245. With regard to circumstances which can trigger the consistency mechanism, the EDPS notes that, although Article 58(2) defines in an exhaustive way the measures to be communicated to the European Data Protection Board, the scope of the mechanism is considerably extended in paragraph 3: any authority can request that any matter shall be dealt with by the Board. This means that a much greater number of cases may trigger the first phase of the consistency mechanism, in comparison with what is foreseen by the Commission in the legislative financial statement attached to the proposed Regulation. Together with the need for translations in all relevant cases, this is also bound to have important consequences in terms of administrative support from the secretariat of the Board. See for more detailed comments and recommendations on the allocation of budget relating to the secretariat of the Board the Annex to the present Opinion.[53]

246. In the second stage developed in Article 58(7), the Board will decide whether it will issue an opinion by a simple majority rule *or* on request of any supervisory authority or of the Commission. The EDPS questions the sense of a vote if any authority can always request that an opinion is adopted. He recommends refining the scope of Article 58(7) and giving more weight to the majority rule, to avoid that the Board is bound to issue an opinion any time there is a request by one single authority. He suggests that a request by one authority could be submitted to vote in case the issue at stake does not relate to one of the main measures described in Article 58(2).

247. The EDPS also calls for more flexible deadlines with regard to the role of the Board when it is seised in the context of the consistency mechanism. He refers in particular to the deadlines of Article 58(6) and (7) requiring 'immediate' information of members of the Board, also in connection with the provision of translation of documents, and to the deadline of one month for the adoption of the opinion of the Board. The EDPS suggests to replace the word 'immediately' in Article 58(6) by 'without delay' and to extend the deadline of one month in Article 58(7) to at least two months/eight weeks.

(ii) The role of the Commission in the consistency mechanism (Articles 59 and 60)

248. The Commission can intervene at different occasions in the context of the consistency mechanism. In addition to triggering the consistency mechanism by seizing the Board, the Commission may adopt an opinion and a suspending decision according to the conditions of Articles 58 and 59. Moreover, the Commission may overrule a decision of a national supervisory authority *in a specific matter* by way of adopting an

[53] The Annex is available in English on the EDPS website (www.edps.europa.eu).

implementing act (see Article 60(1) and 62(1)(a)). The EDPS fundamentally disagrees with this approach as far as this relates to draft measures of a supervisory authority in specific matters.

249. As to the possibility of issuing an opinion, the EDPS notes that the Commission can adopt an opinion independently (1) of the evolution of the procedure before the Board, (2) of the substance of the opinion of the Board, and (3) of the reaction of the supervisory authority to the opinion of the Board. The EDPS regrets that any opinion of the Commission is not linked more closely to the procedure before the Board and to the outcome of this procedure. In his view the Commission should intervene by way of an opinion only if the procedure has not permitted to reconcile the position of the authority with the opinion of the Board, or if the outcome of the procedure would possibly be in breach of EU law. The EDPS recommends complementing Article 59 in that sense.

250. As far as suspension measures are concerned, as foreseen in Article 60, the EDPS considers that 'serious doubts' in the correct application of the proposed Regulation do not justify a decision of suspension of a measure taken by a national supervisory authority. He advises to limit any suspension to a clear breach of EU law with risks of irreparable effects, subject to scrutiny of the Court of Justice.

251. The possibility for the Commission to overrule a decision of a national supervisory authority *in a specific matter* by way of adopting an implementing act[54] raises the same concerns. The power of the Commission goes as far as allowing for the adoption of implementing acts with immediate effect (so without any prior opinion or reasoned decision) on grounds of urgency relating to the interests of the data subjects.[55]

252. The EDPS is strongly opposed to this power of the Commission. It prejudices the independence of national supervisory authorities guaranteed under Chapter VI and cannot be regarded as necessary for the Commission to perform its tasks as guardian of the treaties.

253. The Court of Justice has clearly stated that supervisory authorities should be free from 'any external influence'.[56] According to the EDPS, supervisory authorities are not free of any influence if the Commission is given the power to intervene in individual cases. The fact that the Commission itself has independent status, does not mean it is in all cases independent from the actors the national supervisory authorities are supervising. It should be kept in mind that the Commission performs a number of different functions. It is not excluded that national supervisory authorities have to assess the conduct of public or private actors in which the Commission has a specific interest (for instance in competition law issues, or cases of financial support from EU funds).

254. The power to overrule decisions of a national supervisory authority is not necessary for the Commission to perform its tasks as guardian of the treaties. The proposed power superficially resembles the competences of the Commission in the area of competition law in which it cooperates with national competent authorities. This competence is, however, explicitly provided in Article 105 of the TFEU. There is no similar legal basis as regards data protection. The EDPS considers that the main tools for the Commission to perform its role of guardian of the treaties in this subject area are the normal infringement procedure as laid down in Articles 258 to 260 (directed at Member States)

[54] Article 60(1) and 62(1)(a) of the proposed Regulation.
[55] Article 62(2) of the proposed Regulation.
[56] See the *Commission/Germany* ruling of the CJEU cited in footnote 50.

and its consultative role in the consistency mechanism. The EDPS suggests that these competences could be complemented by a power for the Commission to request interim measures before the Court of Justice, which could include a request for a suspension order.

255. In conclusion, the EDPS recommends that the role of the Commission in the consistency mechanism should consist in an initial phase of the power to seise the Board, as foreseen in Article 58(4), and in a subsequent phase of the power to adopt opinions. Article 59 should be developed in this perspective, in line with suggestions made above. This provision should in particular make a clear connection between the role of the Board and any possible position of the Commission. Subsequent procedures initiated by the Commission should consist of actions before the Court of Justice, in the context of an infringement procedure or to request interim measures.

II.9.c. The European Data Protection Board (Chapter VII, section 3)

256. The EDPS welcomes the provisions of the proposed Regulation aiming at more consistency and effectiveness in the role of the European Data Protection Board, acting as the successor of the Article 29 Working Party. The Proposal also ensures the independence of the Board by providing for a secretariat independent from the Commission, and via an explicit reference to this independence in the text of the Proposal.[57]

II.10. Remedies, liability and sanctions (Chapter VIII)

257. The Proposal provides for detailed possibilities of remedies and sanctions, and it clarifies the liability of controllers in relation to damages suffered by data subjects. These measures are in line with the general objective of the proposed Regulation to reinforce the concrete application of data protection principles.

258. While the EDPS supports these efforts to make the law more effective, he will in the following chapters also point at some complexities inherent to the new scheme of remedies, and at undue rigidities in the way sanctions should be applied. Suggestions will be made with a view to make the system more accessible and flexible.

II.10.a. Remedies

259. The EDPS welcomes that the proposed Regulation foresees several redress mechanisms with a view to facilitate enforcement by the data subject. However, he notes that while one of the red lines of the Proposal is to bring simplification to the present framework, the remedies foreseen in the Proposal do not always support this objective.[58] The following comments will identify the need for clarification or improvement in this respect.

260. The EDPS welcomes the (new) right for organisations or associations defending data subjects' rights and interests to lodge a complaint before a supervisory authority or to bring an action to Court (see Articles 73 and 76). The EDPS notes that in both cases the organisation or association is to act 'on behalf of one or more data subjects'. The EDPS

[57] Article 65 of the proposed Regulation.

[58] Many different procedures can be initiated at the level of supervisory authorities, within or outside the consistency mechanisms (for instance in the context of preliminary contacts or investigations), and at the level of courts, in different countries and in relation to various measures.

suggests clarifying the nature of the mandate that the organisation must obtain from data subjects, and the degree of formality required.

261. The EDPS regrets that no wider collective action is introduced in the Proposal in parallel with the possibility for organisations and associations to defend data subjects' rights. As already stated in his opinion on the Communication of the Commission on a new data protection framework, 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.[59] These actions would be useful especially in cases with smaller impact, where it is unlikely that the victims of a breach of data protection rules would bring individual actions against a controller, given the costs, delays, uncertainties, risks and burdens they would be exposed to. He suggests including a wider provision on collective actions in the proposed Regulation.

262. The EDPS notes that Article 75(2) allows data subjects to have a judicial remedy in the country where they reside. Although this right is welcomed, it might lead to complex situations involving a court from one Member State, and a supervisory authority of another Member State on the basis of the main establishment of the controller or its representative. It also means that courts could be seized in all Member States where individuals reside, independently of the Member State of the competent supervisory authority.

263. The EDPS notes that Article 76(3) and (4) partly address this issue, as it foresees possibilities to suspend a proceeding before a court when parallel proceedings are being conducted in another Member State. He suggests developing this further, taking into account the need for further harmonisation and more systematic information procedures at the level of courts.

264. The EDPS also raises the question of the compatibility of the criteria triggering the competence of courts according to the Proposal with the criteria of the Brussels I Regulation, with regard to tort actions.[60] In this context, the place where the harmful event occurred or may *occur* as well as the place of the harmful event or the place where the damage was *suffered* could be invoked by the individual. Even if in both cases the aim is to ensure the most direct access to court, to the benefit of the victim, in practice this may lead to cumulating the number of courts possibly competent. The EDPS calls for a clarification in the Proposal on its interaction with the Brussels I Regulation.

265. According to Article 75(2), the right of the data subject to bring proceedings before the court of his place of residence will not apply if the controller is a public authority. The EDPS calls on the legislator to ensure that the derogation will not apply to a public authority of a third country, since in that case, the derogation would deprive data subjects of an essential means of redress.

266. The EDPS also notes the insertion in the Proposal of a new right for individuals to request the supervisory authority of their country to bring proceedings against the

[59] See the EDPS Opinion of 14 January 2011, pt. 95 and further. 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 C255, 27.10.2007, p. 10.

[60] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L12, 16.01.2001, p. 1. See also the Proposal for a regulation of the European Parliament and the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, COM(2010)748 final.

competent authority in another Member State if he is concerned about the decision of that authority[61]. Such a provision may be justified by the need to ensure that data subjects will not be deprived of a possibility to be protected even if the 'lead' authority in a specific case is in another Member State. It may however have counterproductive consequences in terms of enhancing trust and cooperation between supervisory authorities.

267. The EDPS would consider it highly undesirable if two independent supervisory authorities would be opposite parties in a national court case: he wonders whether such a procedure would effectively enhance the rights of the data subjects. He would very much favour a reinforcement of the role of the Board in case of conflict between two authorities rather than the settling through legal proceedings.

268. In any case, he advises to specify the type of 'concern' of a data subject which could trigger the proceedings and to restrict it to a more precise risk of impact on the data subject's rights. In addition, the supervisory authority which is seized by the data subject should have a right of appreciation with regard to this request and should be able to assess whether there are sufficient reasons to start proceedings against another supervisory authority. In practice, there may well be other options available to reach a satisfactory outcome.

II.10.b. Liability (Article 77)

269. Article 77 builds on the liability of controllers for damages suffered by data subjects, as laid down in Article 23 of Directive 95/46/EC. It confirms that the controller bears the risk of such damages, except where he can prove that he is not responsible for the event giving rise to the damage. This approach is now extended to the processor and to other controllers or processors involved in the processing, who shall be jointly and severally liable for the entire amount of the damage, subject to the same exception.

270. This approach is reasonable and fair from the point of view of the data subject. He or she will usually not be able to do much more than alleging a breach and damage sustained from that breach. In contrast, controllers and processors have more access to the relevant facts of the event once they have been established.

271. However, in view of the responsibility of the controller, a data subject should not have to choose between the controller and the processor. It should be possible always to address the controller, regardless of where and how the damage arose. The Regulation should provide for a subsequent settlement of the damages between the controller and the processor, once the distribution of liability among them has been clarified. The same applies to the case of multiple controllers and processors.

272. The EDPS recommends that Article 77 be amended along these lines. It would also be appropriate to provide for the compensation of immaterial damage or distress, as this may be particularly relevant in this field.

273. Finally, he recalls the issues arising in the context of groups of undertakings. It might be useful to also introduce a provision using the concept of a single economic entity or

[61] Article 74(4) of the proposed Regulation.

single undertaking.[62] This would allow making a group liable for breaches committed by a subsidiary.

II.10.c. Sanctions (Article 79)

274. The EDPS welcomes the right of supervisory authorities to engage in legal proceedings and to impose remedial and administrative sanctions. These sanctions are essential elements ensuring effective enforcement powers to supervisory authorities. However, in order to ensure complete clarity and legal certainty, the EDPS calls for additional specifications of the circumstances in which administrative sanctions shall be imposed.

275. The EDPS notes that the Proposal seems to afford very little margin of appreciation to an authority with regard to the circumstances in which it would have to impose a sanction. Only in some limited cases of first and non-intentional non-compliance may a warning replace the sanction. It is therefore all the more important that the obligations under the proposed Regulation are clear, especially for data controllers. The EDPS calls for some further flexibility of the system. A margin of appreciation for supervisory authorities with regard to administrative sanctions is an indispensible element of a consistent and scalable enforcement scheme. This is all the more true in view of the different options that are available to supervisory authorities once a particular breach has been established (see also the comments made in part II.8 on remedial sanctions).

276. In this respect, it is not clear whether and how a sanction shall be applied to a data controller who has complied only partially with an obligation, for instance by taking general organisational measures with regard to his responsibility as a data controller pursuant to Article 22, but without implementing all the detailed measures listed therein. The EDPS considers that this should be clarified in the text.

277. Furthermore, although it should be clear that a breach has occurred, sanctions should not be systematically imposed and a margin of manoeuvre should be left to the supervisory authority, especially in cases where the obligations of the proposed Regulation need to be clarified in a delegated or an implementing act (see also part II.2.b above) and such act has not (yet) been adopted. This is the case for instance with regard to the notification of security breaches, where the threshold to be defined by the Commission appears as an essential element of the obligation (Article 79(6)(h)), or in the case of 'privacy by design' obligations, which can be specified through delegated acts and technical standards (see Article 79(6)(e)).

278. It is also unclear from the text the extent to which cumulative sanctions in relation to connected infringements can be imposed on the same controller, and whether several supervisory authorities can impose the same administrative sanction on the same controller. In any event, the relation and possible coexistence between decisions taken by supervisory authorities pursuant to Article 53 (for instance the imposition of a ban on a processing, or an order to remedy a breach in a specific manner) and sanctions or penalties according to Article 78 and 79 should be clarified, possibly in the recitals, taking into account the principle of *ne bis in idem* as interpreted by the Court of Justice.[63]

[62] This concept is commonly used in EU competition law vis-à-vis multinational corporations, see f.i. the ruling of the CJEU of 10 September 2009, *Akzo Nobel/Commission*, C-97/08 P, [2009] ECR I-08237.

[63] See e.g. CJEU 11 February 2003, *Gözütok and Brügge*, C-187/01 and C-385/01, [2003] ECR I-1345.

279. Guidelines on the use of the different enforcement powers should be developed by the supervisory authorities in practice. This may call for a carefully developed and consistent enforcement strategy, where necessary coordinated at EU level in the Board, and made public at a large scale for an optimal effect. The EDPS suggests making a reference to these guidelines in Article 52(1) on the duties of the authorities, and possibly also in Article 66 (on the tasks of the Board).

280. The relationship between the powers of supervisory authorities and the imposition of administrative sanctions or penalties also raises more general procedural questions. The EDPS wonders to what extent information collected from a data controller on the basis of Article 53(1)(c) may be used to impose a sanction on that controller without contradicting the general right against self-incrimination.

II.11. Specific data processing situations (Chapter IX)

281. In part II.2.a, the EDPS has already made some general comments about the provisions on the specific data processing situations contained in Chapter IX of the proposed Regulation. The EDPS questions the need for the additional rules made possible under Article 82. Furthermore, the EDPS recommends the legislator to change the wording 'Within the limits of this Regulation' to 'Without prejudice to this Regulation' in Articles 81, 82 and 84.

282. In this part some further comments will be made on Article 80, Freedom of expression, Article 81 on processing of personal data concerning health and Article 83 on the processing of data for historical, statistical and scientific research purposes.

II.11.a. Freedom of expression and public access to documents (Article 80)

(i) Freedom of expression

283. The reconciliation of freedom of expression with the right to privacy and data protection is a complicated matter. What is considered as representing a fair balance between both fundamental rights is to a great extent determined by national cultural traditions. For that reason, under the European Convention of Human Rights ('ECHR'), the member States of the Council of Europe are left a margin of discretion, as follows from the numerous cases before the European Court of Human Rights ('the ECtHR') on this matter.[64] The EDPS fully supports the flexibility given to Member States under Article 80 to put in place exemptions or derogations from the provisions of the Regulation.

284. However, the EDPS takes the view that the revision of the existing rules on data protection should improve the way in which the EU rules allow for such flexibility, but should not reduce their impact. The proposed Article 80 is almost completely based on Article 9 of Directive 95/46/EC, with one significant difference which will be discussed below.

285. According to the EDPS, there is reason for a more substantive amendment because of the fact that since the adoption of Directive 95/46/EC, the Internet has developed worldwide as the main medium for the expression of information, opinions and ideas. Although freedom of the press has always been considered at the core of the freedom of expression because of the role the press plays as public watchdog, it is clear that in

[64] See f.i. ECtHR 24 June 2004, *Von Hannover/Germany*, 59320/00, *RJD* 2004-VI.

contemporary society this role is no longer exclusively performed by the traditional press. For instance, through a blog every citizen can also act as a public watchdog.

286. This development has been acknowledged by the Court of Justice in the *Satamedia* ruling referred to in recital 121 of the proposed Regulation.[65] The potentially restrictive wording in the current Article 9 of Directive 95/45/EC ('solely for journalistic purposes') has been interpreted in such a broad way by the Court of Justice that this wording has no real substantive value. Therefore, the EDPS recommends deleting this wording from Article 80 and simplifying the provision by referring only to the general notion of freedom of expression. In addition, the reference to the purpose of artistic and literary expression can be deleted as this is also covered by the notion of freedom of expression.

287. The EDPS suggests that Article 80 state that Member States shall provide for exemptions or derogations from provisions included in the Regulation (as already indicated in the current text) if such is necessary for reconciling the right to data protection with the right to freedom of expression. Furthermore, it could be added, in the provision or in a recital, that when reconciling the two fundamental rights the essence of both rights should not be impaired.[66]

288. The EDPS also strongly recommends maintaining the word 'necessary' as in the current Article 9 of Directive 95/46/EC, and not introducing the weaker wording 'in order to' as proposed in Article 80. Of course, exceptions to both fundamental rights should be necessary which could be seen as neutralising the notion. However, the proposed regulation elaborates the rules for only one of the two fundamental rights involved, namely the right to data protection. There is every reason to underline in this instrument that these rules may only be derogated from to the extent actually necessary for reconciling the right to data protection with the right to freedom of expression.

289. The necessity requirement underlines that Member States should carefully consider for which data processing activities of controllers invoking their right to freedom of expression it is actually necessary to derogate from the general data protection rules.

(ii) Public access to documents

290. As with freedom of expression, the reconciliation of data protection and public access rules is a sensitive matter. Member States have widely diverging laws and practises in this area, and EU competence to harmonise the matter is, unlike the right to data protection, limited by the Lisbon Treaty to access to documents of the EU institutions (Article 15 TFEU).

291. Recital 18 of the proposed Regulation is broadly similar to recital 72 of the current Directive 95/46/EC. It states that the Regulation allows the principle of public access to official documents to be taken into account when applying the provisions of the Regulation. However, with the instrument of a regulation it is even less obvious how this can actually be done. The EDPS takes the view that a substantive provision should be included in the proposed Regulation.

292. The EDPS recommends that the legislator add a provision in the proposed Regulation stating that personal data in documents held by public authorities and bodies may be

[65] See the *Satamedia* ruling cited in footnote 31.
[66] See CJEU 12 June 2003, *Schmidberger*, C-112/00, [2003] ECR I-5659, para 80.

publicly disclosed if such is (1) provided for by EU or national law, (2) necessary for reconciling the right to data protection with the right of public access to official documents and (3) constitutes a fair balance of the various interests involved.

II.11.b. Processing of personal data concerning health (Article 81)

293. There are several changes proposed as regards the processing of data concerning health. On the one hand these changes clarify and harmonise certain issues, Article 4(12) and recital 26 of the proposed Regulation define the notion of 'data concerning health' and Article 81 exemplifies the list of grounds for which data concerning health may be processed if necessary without the consent of the data subject. Also the reference to 'within the limits of this Regulation', as discussed in part II.2.a.(ii), should rather be changed to 'without prejudice to the Regulation', should ensure that data protection rules are equally applicable in the health care sector. The EDPS welcomes these changes.

294. On the other hand, the proposed changes also raise new issues which need clarification. In particular, the relation between Article 9 and Article 81 is confusing. Furthermore, taken as a whole, the changes do not address all the obstacles which have arisen under Article 8 of Directive 95/46/EC.

295. The link between Article 9 and Article 81 is made in Article 9(2)(h) this states that the prohibition of processing data concerning health is lifted if the processing is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81. However, processing of health data is also possible on other grounds listed in Article 9(2), without any reference to Article 81. It is confusing that several of these other grounds overlap the grounds listed in Article 81(1) and (2).

296. In Article 81(1)(b) and (c) reference is made to 'reasons of public interest', which resembles the wording of Article 9(2)(g), which lifts the prohibition for processing of special categories of data if necessary for a task carried out 'in the public interest'. Processing of data concerning health for historical, statistical and or scientific purposes is dealt with in Article 81(2), but is also allowed under Article 9(2)(i), in both cases subject to the conditions and safeguards referred to in Article 83. It should be emphasised that Article 81 does not distinguish between public or private entities. Furthermore, the Commission is empowered twice (in Article 9(3) and in Article 81(3)) to adopt delegated acts on the area of data concerning health; however, the provisions are formulated slightly differently.

297. In light of these comments, the EDPS recommends the legislator to align these two provisions and clarify the scope and nature of Article 81.

298. This leads to another concern. Several complications have occurred in the national and cross-border context relating to the protection of data concerning health. To give some examples, the different requirements of consent in this area have been noted as forming obstacles to the cross border exchange of health data. Furthermore, determining responsibility can be very complicated in the healthcare sector as there can be long chains of practitioners involved. This is even further complicated with the development of eHealth applications as actors outside the healthcare sector (producers of technical devices, communication service providers etc.) are involved as well. Moreover, security requirements are insufficiently harmonised and, currently, further processing of data concerning health for research purposes lacks a clear legal basis in the current Directive 95/46/EC. Only this last issue has been solved in the current proposal.

299. The EDPS is aware of the national sensitivities of the healthcare area, and the limited competence of the EU in this area. However, he recommends that the legislator further harmonise national legislation by giving further direction on the requirement of consent, the determination of responsibilities and security requirements. There seems to be an imbalance in the current Proposal between the detailed grounds for processing data concerning health, on the one hand, and the lack of corresponding assurance of the protection of data subjects in this area on the other.

II.11.c. Processing for historical, statistical and scientific research purposes (Article 83)

300. The EDPS welcomes the specific provision on data processing for historical, statistical and scientific research purposes. However, he regrets that no distinction is made therein between processing for such purposes of special categories of data and of other personal data. It should be made clear that additional safeguards should be put in place if special categories of data (such as health data) are processed.

301. Furthermore, the EDPS recommends the legislator furthermore to replace the wording 'Within the limits of this Regulation' by 'Without prejudice to this Regulation'.[67] Contrary to Articles 81, 82 and 84, the provision of Article 83 does not allow for specific national rules. The provision contains additional conditions and is referred to throughout the Regulation. It should be clearly stated that this provision is without prejudice to other provisions in the Regulation. For instance, the purposes of the research as such should be legitimate and in line with the Regulation.

302. The point of departure for data processing for historical, statistical and scientific research purposes should be that such processing is done by using anonymised data. This should be more explicitly mentioned in the first paragraph of Article 83. Only if it proves impossible for carrying out the research may this be different. The controller should be able to justify and demonstrate the necessity of processing data of data subjects. The EDPS welcomes the explicit safeguard mentioned in Article 83(1)(b), but would encourage the legislator to clarify what is meant by the word 'separately' and ensure that this separate storage actually protects the data subjects.

303. Article 83(1)(b) refers to 'data enabling the attribution of information to an identified or identifiable data subject'. The EDPS strongly recommends aligning this sentence with the definitions proposed in Article 4(1) and (2). It would be more appropriate to refer to 'data which enables certain information to be related to a data subject'.

304. A final remark relates to the power granted to the Commission under Article 83(3) to adopt delegated acts. The EDPS has concerns about the delegation to the Commission of the power to lay down 'any necessary limitations on the right of information to and access by the data subject' and to detail the conditions and safeguards for the rights of the data subject under these circumstances. The EDPS takes the view that a limitation of the rights of data subjects should not be done through a delegated act. If there are any necessary limitations they should be included in the provision itself.

[67] The same recommendation was made vis-à-vis Articles 81, 82 and 84 of the proposed Regulation.

CHAPTER III - COMMENTS ON THE PROPOSED DIRECTIVE

III.1. Introduction

305. The processing of personal data in the area of police and judicial cooperation in criminal matters, which by its very nature poses specific risks for the citizen, requires a level of data protection at least as high as under the proposed Regulation, if not higher due to its intrusive nature and the major impact such processing may have on the individual's life.

306. Whilst the law enforcement area requires some specific rules, every departure from the general data protection rules should be duly justified based on a proper balance between the public interest in law enforcement and citizens' fundamental rights.

307. In a democratic society, major discrepancies between data protection in the law enforcement area and in other areas would not only undermine the fundamental right to protection of personal data, but would also have an adverse effect on the efficiency of law enforcement, the mutual trust between Member States, and the trust of the citizen that the State will behave in a law-abiding and responsible way.

308. In recital 7 of the proposed Directive it is stated that the level of protection of the rights of individuals with regard to the processing of personal data by competent authorities must be equivalent in all Member States. The EDPS welcomes this statement. One of the main arguments for this review package is that under the Lisbon Treaty a robust system of data protection is needed which gives equal protection for all data subjects independently of where they reside. This argument fully applies to the area of police ad judicial cooperation in criminal matters.

309. The EDPS welcomes the fact that the proposed Directive, unlike Framework Decision 2008/977/JHA, also covers the domestic processing of personal data. However, as already stated in Chapter I of the present Opinion, this safeguard will only have added value if the Directive substantially increases the level of data protection in the area, which is not the case.

310. The EDPS takes the view that the proposed Directive, in many aspects, does not meet the requirement of a consistent and high level of data protection, described by the Commission itself as 'crucial' (see recital 7). In many instances there is no justification whatsoever for departing from the provisions of the general rules in the proposed Regulation. The EDPS is concerned in particular with regard to:
- the lack of clarity in the drafting of the principle of purpose limitation (see part III.4.a);
- the absence of any obligation on competent authorities to be able to demonstrate compliance with the Directive (see part III.6);
- the weak conditions for transfers to third countries (see part III.7);
- the unduly limited powers of supervisory authorities (see part II.8.a).

III.2. Horizontal issues

311. This part will briefly discuss the lack of any general obligation to evaluate existing data processing operations, the lack of clarity about the rules applicable to transfers of data between competent law enforcement authorities and other authorities or private entities, and the processing of data relating to children.

III.2.a. Specific acts in the area of police and judicial cooperation in criminal matters

312. As said in part I.2.a, the EDPS regrets that the proposed Directive leaves all specific acts in the area of police and judicial cooperation in criminal matters unaffected (see Article 59 of the proposed Directive).[68]

313. It is stated in Article 61(2) of the proposed Directive that the Commission shall review these acts within three years after the entry into force of the Directive. As stated, the EDPS believes that such a deadline would lead to an unacceptably long period during which the current, widely criticised patchwork remains in force.

314. As a clarification of the entire framework should be provided as soon as possible, the EDPS strongly recommends the legislator to set a much stricter deadline which ensures that the specific rules are amended at the latest at the moment the Directive enters into force.

III.2.b. Evaluation mechanisms

315. The EDPS would welcome a provision which obliges Member States to introduce evaluation mechanisms for regular evidence based assessments of whether data processing activities of a certain scale do actually constitute a necessary and proportionate measure for the purposes of preventing, detecting, investigation and prosecuting criminal offences. Such mechanisms are normal and good practice in modern public administrations. Such a mechanism would constitute an effective safeguard against unnecessary data processing activities and an unjustified expansion of such activities.

III.2.c. Transfers to other public authorities or private parties

316. The EDPS wishes to repeat the comments made in part I.2.b that the two proposed instruments do not offer a clear legal framework for situations in which there is a mix of actors and purposes covered by the two different instruments.

317. This does not relate solely to the use by law enforcement authorities of data collected by private entities for commercial purposes. It also concerns the situation in which a law enforcement authority transfers the data it has collected to a private party for a law enforcement purpose or to another public authority for an unrelated purpose.[69] The proposed Directive should clarify the conditions under which such processing is allowed.

318. The current Article 7(b) seems to provide a general legal basis for such a transfer of data (see on this provision also part III.4.a.(i) below). However, the proposed Directive does not lay down any specific guarantees for transfers of personal data to private parties or non law enforcement authorities. In this respect, Principle 5 of Council of Europe Recommendation No R(87)15 states that communication of personal data from law enforcement authorities to other public bodies or to private parties should only be permissible under specific and strict conditions.

[68] See for instance Council Decision 2008/615/JHA cited in footnote 16.

[69] For instance, police services could be required under national law to disclose information to immigration services, taxation authorities or civil courts (or these recipients could be allowed under national law to receive law enforcement information from competent authorities).

319. The EDPS therefore recommends that the legislator insert a provision imposing these specific and strict conditions.

III.2.d. Processing of data relating to children

320. The EDPS notes that, unlike the proposed Regulation, no specific attention is given to the position of children under the proposed Directive. However, in the area covered by the Proposal, children deserve specific treatment.

321. Specific attention should be given in particular to the issue of accuracy of children's identification data and their reliability in time: for instance, the level of accuracy of biometric data, such as finger prints or facial image, is different from those of adults, and they may change much more rapidly in time. As some decisions in relation to a child are also based on age verification, specific safeguards should be taken so that only necessary data are collected and kept. Furthermore, children's data may be subject to different retention periods, in relation to reliability and the purpose for their retention, and due to special rules of criminal procedure for minors.

322. The EDPS therefore recommends that the need for specific safeguards in relation to the processing of data of children be stated specifically in the proposed Directive, in a substantive provision.

III.3. General provisions (Chapter I)

323. According to Article 1(1), the proposed Directive lays down rules to ensure the protection of personal data in the course of activities of police and judicial co-operation in criminal matters. Article 1(1) should be read in conjunction with Article 2(1) stating that the proposal shall apply to the processing of personal data by a competent authority for the purpose of the prevention, investigation, detection and prosecution of criminal offences (referred to throughout this Opinion as 'law enforcement purposes').

324. Article 2(3) excludes from the scope of application of the Proposal the processing of personal data in the course of an activity which falls outside the scope of Union law, in particular concerning national security. As with the equivalent provision in the proposed Regulation (Article 2(2)(a), see part II.3.a.(i)) the EDPS would like to make a general comment that while 'national security' falls outside the scope of Union law, it is not always fully clear what this notion covers, as it depends on Member States national policy. At national level, the use of the wording 'national security' or 'state security', depending on Member States, with a different scope of application, can also be confusing. Obviously, the EDPS does not contest the exception, but he considers that it should be avoided that the exception is unduly used to legitimise the processing of personal data outside the scope of the Regulation and the Directive, for instance in the context of the fight against terrorism.

325. A competent authority is defined in Article 3(14) as meaning any public authority competent for the prevention, investigation, detection and prosecution of criminal offences. The EDPS has stated above that the notion of competent authority should be applied consistently in both proposed instruments (see part II.3.a.(iv)).

III.4. Principles (Chapter II)

326. There are considerable differences between the provisions contained in Chapter II of the proposed Directive and those in Chapter II of the proposed Regulation.

327. Article 4 of the proposed Directive contains the principles relating to data processing and constitutes the equivalent of Article 5 of the proposed Regulation. However, compared to the proposed Regulation, some principles are missing or need further clarification in the context of the proposed Directive. In particular the purpose limitation principle contained in Article 4(b), read in conjunction with Article 7 of the proposed Directive, needs clarification.

328. The provisions different from the proposed Regulation are the distinction between different categories of data subjects and the different degrees of accuracy and reliability of personal data. The EDPS welcomes these provisions but would advise the legislator to strengthen them.

329. In the proposed Directive, specific attention is also given to the processing of special categories of data. However, the current provision (Article 8) does not provide sufficient guidance on how these data should be treated differently.

III.4.a. Principles relating to personal data processing (Article 4) and lawfulness of processing (Article 7)

(i) Purpose limitation (Article 4(b)) and lawfulness of processing (Article 7)

330. Article 4(b) contains the purpose limitation principle in a wording which is similar to the current Article 6(1)(b) of Directive 95/46/EC and Article 5(b) of the proposed Regulation: 'personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'.

331. The EDPS welcomes this consistent approach. However, the true value of the purpose limitation principle depends on (1) the interpretation of the notion of compatible use and (2) the possible derogations to the purpose limitation principle, in other words, the possibilities and conditions for *incompatible* use.

332. It goes without saying that there should be legal certainty about the further use of personal data by law enforcement authorities. Unfortunately, this clarity is not provided by the proposed Directive.

333. As to the notion of compatible use, the EDPS has made some comments above on Article 5(b) of the proposed Regulation (see part II.4.a). Whilst the recitals of the proposed Regulation at least attempt to provide some guidance on what constitutes a compatible purpose, there is no such clarification in the proposed Directive.

334. The EDPS therefore recommends introducing such a clarification in the recitals of the proposed Directive. In particular, the proposed Directive should clarify that the notion of compatible use is to be interpreted restrictively. It must also be made clear that a purpose for further use is not necessarily compatible with the initial purpose simply because this further purpose is also a law enforcement purpose. To put it differently, it should be clear that within the law enforcement context different purposes can be

incompatible. Any other interpretation would render the requirement contained in Article 4(b) (specified, explicit and legitimate) meaningless.

335. As regards further use for an *incompatible* purpose, whether a purpose within or outside the law enforcement context, strictly speaking the proposed Directive does not provide any legal ground for such processing. According to the logic of the current Directive 95/46/EC, such processing should be dealt with in a separate provision which, for a limited number of grounds and subject to strict conditions, allows for a derogation from the purpose limitation principle (see Article 13 of Directive 95/46/EC). Such a provision is missing in the proposed Directive.

336. However, the possibility of departing from the purpose limitation principle seems to be implicitly accepted in the provision on the lawfulness of processing, namely Article 7 of the proposed Directive. Although no reference is made to a possible derogation from the purpose limitation principle, the grounds listed in Article 7(b), (c) and (d) may refer to situations which entail processing of data for incompatible purposes, including purposes outside the law enforcement context. This is contrary to the logic of Directive 95/46/EC, in which the provision on the lawfulness of processing (Article 7) relates to the legitimate grounds for the *initial* purpose for data processing (and compatible further use).

337. The EDPS sees no reason to depart from the logic of Directive 95/46/EC and to weaken existing requirements (see in that respect also the criticism on the change brought about in the proposed Regulation in part II.4.a above). The EDPS therefore recommends making a clear distinction between the lawfulness of processing of personal data for an initial, specified, explicit and legitimate purpose and the derogations according to which personal data may be further used for a purpose incompatible with the initial purpose.

338. This would require Article 7(a) to be changed into a self standing provision ensuring in a general manner that all data processing operations are provided for by law, thereby fulfilling the requirements of the Charter of Fundamental Rights and ECHR, in particular as to the accessibility and foreseeability of the law as developed by the ECtHR under Article 8(2) ECHR.

339. Article 7(b) to (d) should be replaced by an additional, separate provision which exhaustively lists the grounds of public interest for which a derogation to the purpose limitation principle can be allowed. This provision should set out the conditions under which the derogation can be invoked. Any change of purpose should fulfil the requirements of proportionality and necessity. A change of purpose should also, as noted above, be provided for by law, in compliance with the Charter and the ECHR. Incidental use may only occur when necessary in a specific case, for instance for the immediate protection of the vital interest of the data subject or another individual, or to prevent an immediate and serious threat to public security.

340. As in Article 6(2) of the proposed Regulation, the proposed Directive should also include a provision on the processing of personal data for historical, statistical and scientific purposes containing similar safeguards as the ones referred to in Article 83 of the proposed Regulation.

(ii) Data quality (Article 4(c) to (e))

341. Article 4(c) to (e) set forth principles on data quality which are to a great extent similar to those embodied in Article 6(1)(d) of Directive 95/46 and Article 5 of the proposed Regulation.

342. In the law enforcement context in particular, the EDPS recommends providing in the proposed Directive for an obligation for the competent authority to put mechanisms in place to ensure that time limits are established for the erasure of personal data and for a periodic review of the need for the storage of the data.

343. This obligation for a periodic review is typical for the area of police and judicial cooperation. It is present in existing instruments such as Article 20 of the Europol Decision and Article 112 of the Schengen Convention.[70]

344. Moreover, according to Council of Europe Recommendation 87/15, rules aimed at fixing storage periods for the different categories of personal data (see below) as well as regular checks on their quality should be established to ensure that police files are kept up to date and purged of superfluous or inaccurate data.[71]

345. As the EDPS stressed in his third opinion on Framework Decision 2008/977/JHA, distinctions between different categories of personal data are necessary not only for the protection of the personal data of the individual but also for the efficient operation of police services.[72] Old and out of date information is at best useless and at worst misleading, diverting resources from current priorities to matters which are not, and should not, be the focus of investigation necessary for the ability of the recipients.

(iii) Demonstrating compliance with the proposed Directive (Article 4(f))

346. Article 5(f) of the proposed Regulation lays down the general principle that controllers should *ensure and demonstrate* for each processing operation their compliance with the provisions of the Regulation. However, the equivalent provision of the proposed Directive (Article 4(f)) only refers to a general obligation on the controller to *ensure* compliance with the provisions adopted pursuant to the Directive.

347. There is no justification for not requiring the controller to *demonstrate* compliance as well. The obligation to keep documentation under Article 23 of the proposed Directive should be linked to the general obligation to demonstrate compliance, as under Article 5(f), Article 22 and Article 28 of the proposed Regulation. Moreover, the controller should be required to ensure and demonstrate compliance *for each processing operation*.

[70] See Council Decision 2009/371/JHA cited in footnote 16 and Regulation (EC) No 1987/2006 of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) OJ L381, 28.12.2006, p. 4.

[71] See principle 7 of the Recommendation (Length of storage and updating of data) and points 96 to 98 of the explanatory memorandum. Special attention should be devoted here to temporary files, 'dead' files and intelligence files.

[72] See Third Opinion of the EDPS of 27 April 2007 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, OJ C139, 23.06.2007, p.1, point 32.

348. The EDPS therefore recommends aligning the wording of Article 4(f) of the proposed Directive with Article 5(f) of the proposed Regulation and amending Articles 18 and 23 of the proposed Directive accordingly.

III.4.b. Distinction between categories of data subjects (Article 5)

349. Article 5 lays down the obligation for the controller to make a clear distinction between personal data of different categories of persons (suspected, convicted, victims, informers, contacts, others).

350. The EDPS fully supports the introduction of this obligation as a specific data protection rule for law enforcement. It is essential, not only from the perspective of the data subject, but also for law enforcement authorities, that the data related to the different categories of persons are distinguished according to the different degree of involvement in a crime and are treated differently. Comparable distinctions are also foreseen in EU legislation for police cooperation, such as Article 14(1) of the Europol Decision.[73]

351. The EDPS recommends adding the category of non-suspected person to Article 5 Specific conditions and safeguards are necessary to ensure proportionate use of data about such persons and to avoid prejudice to persons that are not actively involved in a crime.

352. Furthermore, the EDPS considers that Article 5 should be reinforced by deleting the wording 'as far as possible' and by specifying the consequences of the categorisation for the different data subject.

353. The wording 'as far as possible' is not needed, since, when collecting data, law enforcement authorities must have a specified purpose and should therefore, at the time of the collection, have a *prima facie* opinion on which category the data are related to. If law enforcement authorities still have doubts how to categorize the data collected during the first stage of the investigation, (e.g. personal data contained in an address book), they may use the category 'others'. Of course, this first categorisation will be adjusted when needed as the investigation progresses further.

354. The EDPS further recommends including in the provision the obligation for Member States to lay down the consequences of the categorisation, reflecting the particularities of the different categories of data processed and the different purposes for which these data are collected by law enforcement and judicial authorities. These consequences should concern the conditions for collecting data, the time limits, limitations to data subject's rights of access and information, modalities of access to data by competent authorities.

III.4.c. Different degrees of accuracy and reliability of personal data (Article 6)

355. Article 6 of the proposed Directive provides that the different categories of data will be distinguished according to their degree of accuracy and reliability and that personal data based on facts will be distinguished from those based on personal assessments. This is an important provision since law enforcement authorities also use soft data based on presumptions rather than on facts.

[73] Council Decision 2009/371/JHA, cited in footnote 69.

356. The EDPS welcomes this provision and underlines its importance both for data subjects and for law enforcement authorities. This can be seen in particular in the exchange of data between law enforcement authorities, when data may be processed far from their source and completely out of the context in which they were originally collected and used. The failure to designate their degree of accuracy and reliability could actually undermine the effectiveness of data exchanges, as police authorities would not be able to ascertain whether the data should be construed as ‘evidence’, ‘fact’, ‘hard intelligence’ or ‘soft intelligence’. The data subject might also be disproportionately affected by the possible lack of accuracy in data relating to suspicions about him or her.

357. However, in light of the foregoing observations, the EDPS considers that this provision should be strengthened and made mandatory by deleting the wording 'as far as possible'. As already explained above, (see part III.4.b on categories of data subjects), law enforcement authorities should have a *prima facie* opinion on the degrees of reliability of data and this assessment of reliability is an indispensible element of their processing.

358. The EDPS therefore recommends deleting the wording 'as far as possible' in paragraphs 1 and 2 of Article 6 of the proposed Directive.

III.4.d. Processing of special categories of data (Article 8)

359. The EDPS welcomes the specific provisions in the proposed Directive on the processing of special categories of data. However, in its current form, Article 8 does not give any direction on how these data should be treated with particular care under the exceptions. Article 8(2)(a) states only very broadly that the prohibition on the processing of such data does not apply if the processing 'is authorised by a law providing appropriate safeguards'. Recital 26 explains that the processing is only allowed if it is 'specifically authorised by a law which provides suitable measures to safeguard the data subject's legitimate interests'.

360. The EDPS recommends that the legislator includes the more restrictive wording of the recital in Article 8 itself and further clarifies in Article 8 and the recitals what is envisaged by suitable measures going beyond the regular safeguards applying to any kind of data processing.

III.5. Rights of data subjects (Chapter III)

361. Chapter III of the proposed Directive deals with the data subject's rights of information, access, rectification and erasure in a way which is generally consistent with current data protection legislation and Article 8 of the Charter. The EDPS welcomes these provisions since they provide for a harmonised set of rights for data subjects while taking into account the particular nature of processing by law enforcement and judicial authorities. However, the EDPS considers that some improvements are still necessary.

III.5.a. Transparency and information to the data subject (Articles 10 and 11)

362. In part II.5.a, the EDPS already underlined that transparency is a crucial part of data protection, not only because of its inherent value but also because it enables other data protection principles to be exercised. Individuals are only able to exercise their rights if they know about the processing of their data. This is even more important in the law enforcement area, where the use of personal data inevitably has an enormous impact on the lives and freedoms of private individuals.

363. The EDPS therefore welcomes the general obligation on controllers to have transparent and easily accessible policies on data protection issues and to communicate with the data subject on this matters using clear and plain language (see Article 10(1) and (2) of the proposed Directive). Furthermore, the EDPS welcomes the specification in greater detail of what type of information must be provided by the controller to the data subject when his or her personal data is collected (see Article 11).

364. However, the EDPS regrets that this obligation is greatly weakened by the addition in Article 10(1) of the limitation that the 'controller shall take all reasonable steps'. Whilst the specificities of the law enforcement sector may require to a certain extent a less liberal approach to transparency, the proposed Directive already takes this into account by providing specific exemptions to the right of information in Article 13 of the proposed Directive. When these exemptions are not applicable, there is no justification for further reducing the obligation in Article 10.

365. The EDPS therefore recommends deleting the reference to 'all reasonable steps' in paragraph 1 as well as in paragraph 3 of Article 10.

III.5.b. Modalities for exercising the data subject's rights (Article 10)

366. Unlike Article 12(2) of the proposed Regulation, Article 10(4) of the proposed Directive does not impose a time-limit on the controller to inform the data subject about his or her request. The substitute notion of 'undue delay' in Article 10(4) would be ineffective in practice, as there is no deadline. Because data subjects' private life may be particularly affected due to the intrusive nature of law enforcement and the level of sensitivity of the data processed, there is a particular need to give them legal certainty when exercising these rights and certainly not to weaken their rights in practice.

367. The EDPS therefore recommends that the proposed Directive should include an explicit time limit in Article 10(4) and that such information should be given at the latest within one month of receipt of the request, in line with the proposed Regulation.

368. Moreover, while Article 12(4) of the proposed Regulation refers to requests which are 'manifestly excessive', Article 10(5) of the proposed Directive uses the word 'vexatious'. For the sake of clarity, the EDPS would prefer the use of the wording 'manifestly excessive'. Furthermore, the EDPS recommends giving further guidance on this notion in a recital.

369. Finally the EDPS recommends including in the proposed Directive a provision similar to Article 13 of the proposed Regulation but with a widened scope. The controller should be required to communicate to each recipient to whom the data have been disclosed, any rectification, erasure or change of the data, either or not carried out in accordance with Article 15 or 16 of the proposed Directive, unless this proves impossible or involves a disproportionate effort. Comparable obligations can already be found in existing EU instruments in the law enforcement area.[74]

[74] See f.i. Article 16 of the Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information, OJ L325, 11.12.2009, p. 6. See also Principle 5(5)ii of Council of Europe Recommendation No R(87)15 on the use of personal data in the police sector.

III.5.c. Limitations to the data subject's rights (Articles 11, 13, 15 and 16)

370. There is no doubt that certain limitations to the data subject's rights may be necessary in the law enforcement area since information on criminal investigations could prejudice the investigation itself. However, since these limitations are exceptions to a fundamental right, they should only be applied so far as necessary and proportionate in each case. Furthermore, exceptions should be limited and well defined and, where possible, partial and limited in time. In addition, any limitation of the data subject's rights should be accompanied with appropriate safeguards.

371. Articles 11(4) and 13 lay down the exemptions allowing partial or complete restriction of the transparency obligation and the right of access when such exemptions constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned. The EDPS welcomes that the proposed Directive harmonises the grounds and conditions for the possible derogations.[75]

372. However, unlike the provisions on transparency and the right of access, the grounds and conditions for restricting the right to rectification (Article 15) and the right to erasure (Article 16) are not mentioned in the proposed Directive. In both provisions it is only stated that the controller should inform the data subject about the reasons for a refusal and the possibilities to go to a supervisory authority or to a court. The EDPS recommends that the grounds and conditions for restricting these two rights are mentioned as well.

373. With regard to national provisions, Article 11(5) and Article 13(2) provide that with a view to the specific nature of certain categories of data processing, Member States may determine by law categories of data processing which may wholly or partly fall under the exemptions. However, this should only be allowed for limited situations in which such a categorical exemption is duly justified.[76] This implies that it should be obvious that the legitimate grounds for an exemption apply to all relevant data under all circumstances. In principle, any partial or complete restriction to the right of information and/or access should be carefully assessed by the controller on a case by case basis in relation to the ground invoked for such limitation.

374. The EDPS recommends, in order to ensure the exceptional character of this exemption, adding a sentence in Article 11(4) and Article 13(1) stating that the controller should be required to assess in each specific case by way of a concrete and individual examination whether partial or complete restrictions for one of the grounds applies.

375. Furthermore, a limited interpretation of the scope of Article 11(5) and Article 13(2) should be ensured through an amendment of the provisions itself.

376. Finally, the EDPS recommends deleting the word 'omitting' in Article 11(4) and Recital 33 as far as it has no added value.

[75] Restrictions to data subject's rights are allowed by identical provisions laid down with regard to both right to information and right to access.

[76] Article 109 of the Schengen Convention might serve as an illustration. According to this provision alerts for discrete surveillance shall in any event not be communicated to the data subject concerned.

III.5.d. Additional safeguards (Articles 14 and 45(1)(c))

377. The proposed Directive contains several additional obligations and safeguards which accompany the restriction of the rights laid down in Articles 13, 15 and 16 providing, in particular, for intervention by a supervisory authority.

378. For example, when refusing or restricting access, rectification or erasure, the controller is required to inform the data subject about the possibility of lodging a complaint to the supervisory authority and seeking a judicial remedy (see Articles 13(3), 15(2) and 16(4)). Moreover, according to Article 14, the data subject has the right to request the supervisory authority to check the lawfulness of the processing.

379. The EDPS welcomes these additional safeguards relating to the supervisory authority. However their effectiveness is limited because these authorities have no power under the proposed Directive to order the controller or the processor to comply with requests relating to data subjects' rights.

380. The EDPS therefore recommends adding this power, as will be further discussed in part III.8.a of this opinion.

III.5.e. Right of erasure (Article 16)

381. The EDPS notes that the controller can in specific cases mark the data instead of deleting them. The spirit of this provision is the same as that of Article 17(4) and (5) of the proposed Regulation. However, the proposed Regulation foresees a possibility to 'restrict' the processing when data are not deleted, whereas the proposed Directive simply foresees the 'marking' of data.

382. For the sake of consistency and clarity of the concept of restriction of processing in both Proposals, the EDPS recommends using in Article 16(3) the wording 'shall restrict processing' instead of 'shall mark'. He also recommends developing the definition in Article 3(4) of the proposed Directive further in line with Article 17(5) of the proposed Regulation. As already stated in part II.3.c, we recommend the legislator to include the definition of 'restriction of processing' in the Regulation as well.

383. In addition, he recommends adding in Article 16 of the proposed Directive the obligation for the controller to inform the data subject before lifting any restriction on processing. There is no reason why the proposed Directive should depart from the standards of Article 17(6) of the proposed Regulation in this respect.

III.6. Controller and processor (Chapter IV)

384. In part II.6 of this opinion, the EDPS has expressed satisfaction with the major improvements proposed with regard to the rules for controllers and processors as provided for by Chapter IV of the Regulation. However, the EDPS is less positive about how the rules for controllers and processors have been developed in Chapter IV of the proposed Directive.

385. The EDPS understands that some of the provisions of the proposed Regulation have to be adapted in order to take account of the specific nature of the legal instrument (a Directive) and the specific nature of the processing in the area of police and judicial co-operation in criminal matters. However, the deviations from the general rules in the

current Proposal go much too far. For example, there is absolutely no justification for deleting the data protection impact assessment and for simplifying drastically other provisions such as those concerning the Data Protection Officer.

386. Such differences significantly undermine the aim of a strong, consistent and comprehensive data protection framework stated by the Commission in its Communication. As will be developed in greater detail below, the EDPS therefore recommends aligning the proposed Directive with the relevant provisions in the proposed Regulation.

III.6.a. Data protection by design and by default (Article 19)

387. The EDPS notes that Article 19 is a very simplified version of the provision on data protection by design and by default provided for in Article 23 of the proposed Regulation.

388. In particular Article 19(1) does not refer to the moment the measures and procedures implementing both principles have to be put into effect. Likewise, Article 19(2) merely states that 'the controller shall implement mechanisms for ensuring that, by default, only those personal data which are necessary for the purposes of the processing are processed'.

389. The EDPS recommends that the above recommendations on Article 23 of the proposed Regulation, to further substantiate the notion of data protection 'by default' (see part II.6.b), should equally be taken into account for the proposed Directive.

III.6.b. Documentation and keeping of records (Article 23)

390. According to Article 23(1) the controllers and processors should be required to maintain documentation of the processing operations under their responsibility. The list of information is provided in Article 23(2) whereas Article 23(3) establishes that the documentation should be made available on request to the supervisory authority.

391. As already stated, the documentation requirement stems from the general obligation to be able to *demonstrate* compliance with the Directive. In line with the proposed Regulation, this should be explicitly stated in Article 4(f) and Article 18 of the proposed Directive.

392. In addition, given the specific nature of the processing covered by the Directive, Article 24 establishes that records of the main processing operations carried out are to be kept for the purposes of verification of the lawfulness, self-monitoring and data security.

393. It should be noted that the list in Article 23(2) is less detailed than the comparable list in Article 28(2) of the proposed Regulation. The comments made above in part II.6.e therefore do not fully apply here. Nevertheless, it would be advisable to better align both provisions in the light of those comments before they are finally adopted. This concerns in particular the name and contact details of the data protection officer, and the mechanisms implemented to verify the effectiveness of the measures in place to ensuring compliance.

394. Moreover, the obligation to make the documentation available to the supervisory authority should also be supplemented by an additional obligation to inform the

supervisory authority on other relevant points, such as the categories of data subjects and the categories of personal data, and a general indication of time limits for erasure.

395. In addition, the information to be kept on transfers to third countries is too limited (see Article 23(2)(d)). With regard to transfers to third countries the EDPS further recommends including the requirement to keep information on the legal ground on which the data is transferred, with a substantive explanation especially if a transfer is based on Article 35 or 36.

396. Article 24 deals with the keeping of records. The EDPS welcomes this provision and recommends to specifically include the identity of the recipients of the data. Furthermore, the EDPS recommends providing in Article 24, as in Article 23, that the supervisory authority shall have access to this information on request.

III.6.c. Data security (Articles 27 to 29)

397. The EDPS is pleased to see that the obligation to notify a personal data breach to the supervisory authority and the data subject is also proposed in the Directive.

III.6.d. Data protection impact assessment

398. In his comments on the proposed Regulation, the EDPS welcomes the introduction of the principle of a data protection impact assessment in Article 33 of the proposed Regulation as it constitutes an important mechanism for ensuring the accountability of the controller (see part II.6.h). Moreover, it contributes to the practical implementation of the principles of 'privacy by design' and 'privacy by default'.

399. The DPIA does not appear in the proposed Directive at all. Nor is there any provision for a preliminary impact assessment when biometric data are processed, as suggested by the Council.[77] If this omission is based on the idea that public authorities are exempted from the mandatory DPIA under the Regulation, the EDPS would recall the comment made in part II.6.h above that the exemption should only apply if a specific assessment, equal to a DPIA, has already been made during the legislative process.

400. The EDPS sees no justification why the DPIA should not also be included in the proposed Directive accompanied by the exception clause discussed above. The specific nature of the processing operations carried out by law enforcement authorities makes it even more necessary to carry out such impact assessments.

401. The EDPS therefore invites the legislator to insert in the proposed Directive a provision requiring the competent authorities to carry out a DPIA, unless a specific assessment, equal to a DPIA, has already been made during the legislative process.

III.6.e. Prior consultation (Article 26)

402. Under Article 26(1), Member States should provide that the controller or the processor must consult the supervisory authority prior to processing operations which will form part of a new filing system to be created where special categories of data are to be processed and where the technology, mechanisms or procedures to be used are likely to present specific risks. According to Article 26(2), Member States may provide that the

[77] See the Council conclusions of the 3071st Justice and Home Affairs Council meeting of 24 and 25 February 2011, pt. 9.

supervisory authority establishes a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

403. The EDPS considers that the scope of the consultation procedure is too limited and recommends to align the provision more closely with the procedures developed in Article 34(2) of the proposed Regulation. These procedures are based on the existence of the data protection impact assessment. If the proposed Directive remains as it is now, the absence of any DPIA would make it very difficult to identify potential risks for the fundamental rights and freedom of data subjects.

404. In such circumstances, there should be an obligation for the controller or the processor to consult systematically the supervisory authority where a new processing operation is introduced in an existing filing system. Only if the obligation of a data protection impact assessment is introduced in the proposed Directive could the scope of the consultation procedure be limited to cases presenting specific risks, as there would be a real guarantee then that such risks would be prior identified.

III.6.f. Data protection officer

405. The EDPS has emphasised in the context of the proposal for a Regulation the importance of the data protection officer ('DPO') function for ensuring internal compliance with data protection rules. Therefore, he strongly supports the introduction in Article 30(1) of the proposed Directive of a provision providing for the obligation for the controller or processor to appoint a DPO.

406. The EDPS regrets that the Proposal fails to establish some basic requirements for the designation and for the position of the DPO. The EDPS therefore recommends that the Proposal should be aligned to the proposed Regulation and should provide additional guarantees: first, Article 30 should deal with the issue of conflict of interest and lay down a minimum term of office of two years and, second, Article 31 should provide for an appropriate administrative attachment with due regard to the independent role of the DPO and with a view in particular to avoiding possible uneven relations or influence by high rank controllers.

III.7. Transfer to third countries (Chapter V)

407. In an increasingly connected world, effective police and judicial cooperation within EU borders depends more and more on cooperation with third countries and international organisations. Because the development of this international cooperation is likely to rely heavily on exchanges of personal data, it is all the more important for the EU to develop these exchanges in full respect for human rights, including data protection.

III.7.a. General principles for transfers (Article 33)

408. According to Article 33, transfers of personal data to a third country or an international organisation including further onward transfer to another third country or international organisation may take place when the transfer is necessary for law enforcement purposes under the conditions laid down in Chapter V of the proposed Directive.

409. The existing legal instruments in the area of police and judicial cooperation require the controller in the third country or international organisation to be an authority competent

for law enforcement purposes.[78] Article 33 of the proposed Directive does not include this requirement, which is only mentioned in recital 45 thereof. This is clearly not sufficient. The EDPS strongly opposes any possibility of transfer and further processing of personal data by third countries beyond the framework set up by the Directive.

410. Therefore, the EDPS strongly recommends completing Article 33 of the proposed Directive by the requirement that the transfer may only take place if the controller in the third country or the international organisation is a competent authority within the meaning of the proposed Directive.

III.7.b. Transfer where there is a positive adequacy decision (Article 34)

411. As a general rule, a transfer may take place where the Commission, on the basis of Article 41 of the proposed Regulation or Article 34 of the proposed Directive, has decided that the third country or international organisation ensures an adequate level of protection. The principle of 'adequate level of protection' is enshrined in the Additional Protocol to Convention 108.[79] This principle has also been implemented and specified in several legal instruments of the European Union, not only in Directive 95/46/EC, but also in legal instruments within the area of police and judicial cooperation, such as the legal instruments establishing Europol and Eurojust. The EDPS welcomes this reference to adequacy decisions in Article 34 of the proposed Directive and related mechanism.

III.7.c. Transfer where there is no decision on adequacy (Articles 35 and 36)

412. Where there is no Commission decision on adequacy, transfers may take place where (i) appropriate safeguards have been provided for in a legally binding instrument or (ii) the controller has concluded, after having assessed all the circumstances surrounding the transfer of personal data that appropriate safeguards exist (Article 35).

413. However, an assessment by the controller alone cannot be considered as an appropriate and sufficient safeguard to allow transfers to a third country or an international organisation on a systematic or structural basis, as it clearly does not provide sufficient protection for the data subjects.

414. The EDPS also notes that, except for the requirement of specific documentation - which is an additional safeguard but not sufficient in itself, the proposed Directive does not provide any guarantee for such transfers. In contrast, Article 42(5) of the proposed Regulation provides in such cases for prior authorisation of the supervisory authority.

415. The EDPS therefore strongly recommends deleting Article 35(1)(b) or as a minimum adding the requirement of a prior authorisation of the supervisory authority.

416. Where there is neither a decision on adequacy, nor appropriate safeguards under Article 35, a transfer may still take place under Article 36 where it is necessary (i) to protect vital interests of the data subject or another person, (ii) to safeguard legitimate interests of the data subject, (iii) for the prevention of an immediate and serious threat to public security, (iv) in individual cases for law enforcement proposes and (v) in individual

[78] See Article 17(1) of the Council Decision 2009/934/JHA cited in footnote 73 and Article 13(1)(b) on the Council Framework Decision 2008/977/JHA.

[79] The Additional protocol regarding supervisory authorities and transborder data flows lays down the general principle - subject to certain derogations - that transfer of personal data to third party is permitted only if that party 'ensures an adequate level of protection for the intended data transfer'.

cases for the establishment, exercise or defence of legal claims relating to law enforcement purposes.

417. The EDPS emphasizes that any derogation used to justify a transfer needs to be interpreted restrictively and should not allow the frequent, massive and structural transfer of personal data. Whilst Article 36 paragraphs (d) and (e) foresee that the derogation applies in individual cases, it should be clear that even an individual case should not allow wholesale transfers of data and should be limited to data strictly necessary. This applies equally to any transfer justified by a serious threat to public security, as mentioned in Article 36(c). The EDPS recommends that this be clarified in a recital.

418. Moreover, the EDPS recommends that additional safeguards such as the obligation to specifically document these transfers (e.g. data transferred, time of transfer, data about the recipient, reason for the transfer and recipient etc.) are added to Article 36.

III.7.d. Transfer where there is a negative decision on adequacy

419. The conditions permitting a transfer to a third country or an international organisation which does not offer an adequate level of protection are unclear. Indeed, whilst Article 34(6) and recital 48 of the proposed Directive allow transfers to such countries or organisations when based on appropriate safeguards (Article 35) or derogations (Article 36), Article 35(1) which deals with the appropriate safeguards refers to situations where the Commission has taken no decision.

420. A similar comment was made in part II.7.b with regard to the Regulation. The EDPS therefore suggests that Article 35(1) be modified to ensure consistency among these provisions. Nevertheless, when there is a decision of non-adequacy, possibilities to continue to transfer personal data should be very limited in this particular field. The EDPS recommends that any transfer in this situation should therefore only be based on:
    - Article 35(1)(a) if there is a legally binding international agreement allowing for the transfer under specific conditions guaranteeing an adequate protection,
    - Article 36(a) or (c), i.e. to protect the vital interest of the data subject or in case of an immediate and serious threat to public security.

III.8. Oversight mechanisms (Chapter VI, VII and VIII)

421. The EDPS notes that the provisions on oversight mechanisms by independent supervisory authorities, as well as the cooperation mechanisms between those authorities differ in some respects from the corresponding provisions in the proposed Regulation.

422. In this part the EDPS will analyse these differences, their justification, as well as the possible consequences for the organisation of the supervisory authorities. In most Member States, the same authorities will presumably be assigned to supervise the Regulation as well as the national laws implementing the directive.

III.8.a. Powers of supervisory authorities

423. According to the EDPS, under a comprehensive approach, there is no need for differentiating the powers of the supervisory authorities between the Regulation and the

Directive. Indeed, the proposed Regulation also foresees the oversight of public authorities by supervisory authorities.

424. As to the scope, the competent authorities to which the proposed Directive is supposed to apply under its Article 1(1) are on the one hand police authorities within the meaning of Article 87(1) TFEU, and on the other hand judicial authorities. According to the EDPS, a distinction could be justified to some extent between supervision by supervisory authorities of the police and supervision by supervisory authorities of the judiciary. In the case of the police, there is no need for specificities; to the contrary, in view of the powers of the police, strong supervision is possibly even more important than in other branches of government.

425. Whilst data subjects need full protection in the judicial area as well, under the rule of law some activities of the judiciary may be (partly) exempted from supervision by other public bodies like supervisory authorities. This is recognised by Article 51(3) of the proposed Regulation and Article 44(2) of the proposed Directive with regard to courts acting in their judicial capacity.

426. The EDPS recommends giving more guidance in a recital on what is meant to be covered by 'judicial capacity'. He understands the exception as addressing more particularly the processing of personal data in judicial proceedings on individual cases. On the other hand, the data protection principles – including supervision - should remain applicable, for instance, to processing of personal data by the registry, publication of public reports of proceedings, and publication of judicial decisions.

427. If some limited exception[80] is justified with regard to courts acting in their judicial capacity, the EDPS does not see any reason to limit the powers of supervisory authorities outside this specific context. The EDPS therefore recommends that the powers of supervisory authorities vis-à-vis national police authorities should be fully aligned with the powers under the proposal for a Regulation.

428. However, the most obvious difference between the proposed Regulation and the proposed Directive do not relate to the scope, but to the substance of the powers of the supervisory authorities. Whilst Article 53 of the proposed Regulation enumerates a long list of powers, Article 46 of the proposed Directive is more limited. Several powers of the supervisory authorities have been deleted without justification compared to the proposed Regulation. The EDPS refers in particular to the power of supervisory authorities to order the controller or the processor to comply with requests relating to data subjects' rights and the power to suspend data flows to a recipient in a third country or to an international organisation.[81] Moreover, the power to obtain from the controller or the processor access to all personal data or to any of its premises has been substantially reduced and replaced by the power to 'collect all the information necessary'.[82]

429. The EDPS recommends aligning the wording of Article 46(a) with the wording of Article 53 of the proposed Regulation.

[80] The scope and purpose of this exception remain problematic. There is a range of practices among the Member States, although most declarations of Contracting Parties to Convention 108 do not mention the exception. To the extent in which national data protection authorities are involved, they seem to find satisfactory solutions in practice. Further reflection on the subject is therefore needed.

[81] See Article 53(1)(b) and (h) of the proposed Regulation.

[82] Compare Article 53(2) of the proposed Regulation with Article 46(a) of the proposed Directive.

430. As said, the EDPS does not see any justification for a differentiation between the Regulation and the Directive as far as the powers of the supervisory authorities are concerned. However, he recognises that the effective powers under Article 46(b) of the proposed Directive are potentially strong, provided that it is ensured that all Member States *shall* provide supervisory authorities on their territories with *all* enumerated powers. As a minimum option he therefore advises changing the wording 'such as' in Article 46(a) and (b) into 'including'.

431. The EDPS also notes a significant difference concerning the annual activities report of the supervisory authorities. According to Article 54 of the proposed Regulation this report must not only be made available to the Commission and the European Data Protection Board, but must also be presented to the national parliament and must be made public. Article 47 of the proposed Directive only mentions the availability of the report to the Commission and the Board. The EDPS sees no justification for this difference, at least with regard to the national parliament. In this respect, the Court of Justice in the *Commission/Germany* ruling explicitly mentions reporting by the supervisory authority to the national parliament as a tool for complying with the principle of democracy.[83]

III.8.b. Co-operation and consistency

432. The proposal for a Regulation foresees an elaborate regime for mutual assistance between supervisory authorities and also encourages joint operations. The provisions of the Directive are much more limited. Of course, there are reasons for a more limited approach in the Directive, if only for reasons of national sovereignty. It would be difficult to imagine that members of staff of a supervisory authority in one Member State would conduct investigations in police premises in other Member States.

433. However, the proposed Directive recognises that close co-operation between supervisory authorities does make sense in the area of police and judicial cooperation. Recital 58 recalls that consistent application and enforcement should be ensured by a mechanism of (mutual) assistance of supervisory authorities. The exponential growth of exchange of information between national police and judicial authorities requires harmonised approaches, as well as guarantees that enforcement measures of supervisory authorities in one Member State will not be circumvented if no appropriate measures are taken in other Member States where the same data are available. Finally, close cooperation of supervisory authorities could facilitate the use of personal data in judicial proceedings with a cross border element.

434. More generally, the EDPS is not convinced that specific mutual assistance arrangements under the proposed Regulation could not be included in the proposed Directive. For instance, Article 55 of the proposed Regulation contains a number of detailed provisions aiming at ensuring a quick, efficient and compulsory cooperation between supervisory authorities.

[83] See the *Commission/Germany* ruling of the CJEU cited in footnote 50, para 55. See also the ruling of the CJEU of 20 May 2003, *Österreichischer Rundfunk*, C-465/00, C-138/01 and C-139/01, [2003] ECR I-4989, in which the Court laid down guidance on proportionality concerning the question whether the salary data concerned had to be disclosed to the public as well as to Parliament.

435. The EDPS therefore recommends including in any event the provisions of Article 55(2) to (7) in the proposed Directive.

436. He is also not convinced that a specific mechanism of enhanced cooperation inspired by the consistency mechanism of Articles 57 to 63 of the proposed Regulation could not be included in the Directive, possibly with more limited tasks. One of the reasons for setting up this mechanism is to ensure that EU data protection law is interpreted in a uniform way in the entire territory of the Union, in order to give all EU residents equal protection of their fundamental right, in cases with cross border elements. This reason fully applies to the area of police and judicial cooperation in criminal matters.

437. If, for instance, personal data of a specific individual are exchanged between competent authorities in different Member States, it would not be helpful if this individual could not benefit from the same level of protection in the sending and the receiving Member State.

438. The EDPS advises the legislator to reconsider the need for an enhanced cooperation mechanism, also in the scope of application of the proposed Directive.

CHAPTER IV - CONCLUSIONS AND RECOMMENDATIONS

439. The EDPS welcomes the proposed Regulation as it constitutes a huge step forward for data protection in Europe. The proposed rules will strengthen the rights of individuals and make controllers more accountable for how they handle personal data. Furthermore, the role and powers of national supervisory authorities (alone and together) are effectively reinforced.

440. The EDPS is particularly pleased to see that the instrument of a *regulation* is proposed for the general rules on data protection. The proposed Regulation would be directly applicable in the Member States and would do away with many complexities and inconsistencies stemming from the different implementing laws of the Member States currently in place.

441. The EDPS is, however, seriously disappointed with the proposed Directive for data protection in the law enforcement area. The EDPS regrets that the Commission has chosen to regulate this matter in a self-standing legal instrument which provides for an inadequate level of protection, by far inferior to the proposed Regulation.

442. A positive element of the proposed Directive is that it covers domestic processing, and thus has a wider scope than the current Framework Decision. However, this improvement only has added value if the Directive substantially increases the level of data protection in this area, which is not the case.

443. The main weakness of the package as a whole is that it does not remedy the lack of comprehensiveness of the EU data protection rules. It leaves many EU data protection instruments unaffected such as the data protection rules for the EU institutions and bodies, but also all specific instruments adopted in the area of police and judicial cooperation in criminal matters such as the Prüm Decision and the rules on Europol and Eurojust. Furthermore, the proposed instruments taken together do not fully address factual situations which fall under both policy areas, such as the use of PNR or telecommunication data for law enforcement purposes.

444. In the present Opinion the EDPS has provided detailed comments and recommendations on the two legislative proposals. All recommendations are listed below in concise way.

As regards the entire reform process (part I.2)

- Announce publicly the time schedule on the second stage of the reform process as soon as possible.
- Incorporate the rules for EU institutions and bodies in the proposed Regulation or at least have aligned rules in force when the proposed Regulation applies.
- Present as soon as possible a proposal for common rules for the Common Foreign and Security Policy, based on Article 39 TEU.

Recommendations on the proposed Regulation

Horizontal issues (part II.2)

- Add a provision clarifying the territorial scope of application of national law under the Regulation.
- Reconsider the delegation of power in Articles 31(5) and (6), 32(5) and (6), 33(6) and (7), 34(2)(a) and 44(1)(d) and (7).
- Provide appropriate and specific measures for MSMEs in selected implementing acts only, and not in delegated acts of Articles 8(3), 14(7), 22(4) and 33(6).
- Refine the notion of 'public interest' in each provision in which it is used. Specific public interests should be explicitly identified in relation to the context of the intended processing in each relevant provision of the proposal (see in particular, recital 87, Articles 17(5), 44(1)(d) and 81(1)(b) and (c)). Additional requirements could include that the ground can only be invoked in specifically pressing circumstances or on imperative grounds laid down in law.

Chapter I - General provisions (part II.3)

- Article 2(2)(d): insert a criterion to differentiate public and domestic activities based on the *indefinite* number of individuals who can access the information.
- Article 2(2)(e): provide that the exception applies to competent *public* authorities. Recital 16 should be made consistent with Article 2(2)(e).
- Article 4(1)(2): add a clearer explanation in a recital insisting on the fact that as soon as there is a close relation between an identifier and a person this will trigger the application of the data protection principles.
- Article 4(13): refine the criteria to identify the main establishment of the relevant controller, taking into account the 'dominant influence' of one establishment over others in close connection to the power to implement personal data protection rules or rules relevant for data protection. Alternatively, the definition could focus on the main establishment of the group as a whole.
- Add new definitions on ‘transfer’ and 'restriction of processing'.

Chapter II - Main principles (part II.4)

- Article 6: Add a recital to further clarify what falls under a task carried out 'in the public interest or in the exercise of public authority' in Article 6(1)(e).
- Article 6(4): delete the provision or at the very least restrict it to further processing of data for incompatible purposes on the grounds contained in Article 6(1)(a) and 6(1)(d). This would also require an amendment of recital 40.
- Add a new provision on the representation of all individuals lacking sufficient (legal) capacity or who are otherwise unable to act.

- Article 9: include offences and matters which have not led to convictions in the special categories of data. Extend the requirement of control of official authority to all grounds indicated in Article 9(2)(j).
- Article 10: make it more explicit in recital 45 that the data controller should not be able to invoke a possible lack of information to refuse a request of access, when this information can be provided by the data subject to enable such access.

Chapter III - Rights of the data subject (part II.5)

- Article 14: include information on the existence of certain processing operations which have a particular impact on individuals, as well as the consequences of such processing on individuals.
- Article 17: develop the provision further to ensure its effectiveness in reality. Delete Article 17(3)(d).
- Article 18: clarify that the exercise of the right is without prejudice to the obligation in Article 5(e) to delete data when they are no longer necessary. Ensure that Article 18(2) is not limited only to data that has been provided by the data subject on the basis of consent or a contract.
- Article 19: clarify what the controller should do in case of disagreement with the data subject and align with Article 17(1)(c). Explain in a recital what may qualify as 'compelling legitimate grounds'.
- Article 20: include the right of individuals to submit their point of view in Article 20(2)(a), as in the current Article 15 of Directive 95/46/EC.
- Article 21: introduce detailed guarantees that national law should specify the objectives pursued by the processing, the categories of personal data to be processed, the specific purposes and means of processing, the controller, the categories of persons authorised to process the data, the procedure to be followed for the processing, and the safeguards against any arbitrary interferences by public authorities. Include as additional safeguards informing of data subjects of a restriction and of their right to refer the matter to the supervisory authority to obtain indirect access. Add in Article 21 that the possibility of applying restrictions to the processing performed by private controllers for law enforcement purposes should not force them to retain data in addition to those strictly necessary for the original purpose pursued nor to change their IT architecture. Delete the ground contained in Article 21(1)(e).

Chapter IV - Controller and processor (part II.6)

- Article 22: refer explicitly to the principle of accountability, in any event in recital 60. Merge Article 22(1) and (3) and mention explicitly that measures should be *appropriate* and *effective*. Include a general provision preceding the specific obligations in Article 22(2) developing the concept of 'management control', including the assignment of responsibilities, training of staff, and adequate instructions and requiring that the controller should at least have an overview and a general inventory of the processing operations within the scope of his responsibility. Add a new paragraph to provide that when the controller decides or is obliged to publish a regular report of its activities this report should also contain a description of the policies and measures referred to in Article 22(1).
- Article 23: refer in Article 23(2) and recital 61 to the fact that data subjects should in principle be left the choice to allow use of their personal data in a broader way.
- Article 25(2)(a): delete the exception for adequate third countries.
- Article 26: add the obligation of the processor to take account of the principle of data protection by design to the list of specifications contained in Article 26(2).
- Article 28: reconsider or delete the exemptions of Article 28(4).

- Article 30: clarify Article 30 to ensure the overall responsibility of the controller and add the obligation on the controller to adopt an information security management approach within the organisation, including where appropriate the implementation of an information security policy specific to the data processing performed. Include an explicit reference to the DPIA in Article 30.
- Articles 31 and 32: specify the criteria and requirements for establishing a data breach and the circumstances in which it should be notified. Change the time limit of 24 hours in Article 31 to no later than 72 hours.
- Article 33: the list of processing operations contained in Article 33(2)(b), (c) and (d) should not be limited to processing on a large scale basis. Align Article 33(5) with recital 73. Limit Article 33(6) to non essential elements. Clarify that the size of a company should never lift the obligation of performing a DPIA with regard to the processing operations which present specific risks.
- Article 34: move Article 34(1) to Chapter V of the proposed Regulation.
- Articles 35 to 37: lower the threshold of 250 employees in Article 35(1) and clarify the scope of Article 35(1)(c). Add guarantees, in particular stronger conditions for the DPO's dismissal and ensure in Article 36(1) that the DPO is given access to all information relevant, and to premises necessary to perform his duties. Include in Article 37(1)(a) the role of the DPO in raising awareness.

Chapter V - Transfer to third countries (part II.7)

- State in recital 79 that the non-applicability of the Regulation to international agreements is restricted in time only to already existing international agreements.
- Insert a transitional clause providing for the review of these international agreements within a set time in order to align them with the Regulation.
- Article 41 (and recital 82): clarify that in the case of a non-adequacy decision, transfers should be allowed only under appropriate safeguards or if such transfer falls under the derogations set forth in Article 44.
- Article 42: Ensure that the possibility of using non-legally binding instruments to provide appropriate safeguards should be clearly justified and limited only to cases where the necessity to rely on such instruments has been demonstrated.
- Article 44 (and recital 87): Add that the possibility to transfer data should only concern occasional transfers and be based on a careful assessment of all the circumstances of the transfer on a case by case basis. Replace or clarify the reference to 'appropriate safeguards' in Article 44(1)(h) and in Article 44(3).
- Recital 90: change the recital into a substantive provision. Put in place appropriate guarantees for these cases, involving judicial guarantees as well as data protection safeguards.

Chapter VI and VII - Independent supervisory authorities, cooperation and consistency (part II.8 and II.9)

- Article 48: include a role for the national parliaments in the procedure of appointment of members of supervisory authorities.
- Article 52(1): include duty to develop guidelines on the use of the different enforcement powers, where necessary coordinated at EU level in the Board. This could possibly be included in Article 66 as well.
- Article 58: replace the word 'immediately' in Article 58(6) by 'without delay' and extend the deadline of one month in Article 58(7) to two months/eight weeks.
- Article 58: give more weight to the majority rule by ensuring that a request by one authority could be submitted to vote in case the issue at stake does not relate to one of the main measures described in Article 58(2).

- Articles 59 and 60: limit the power of the Commission by deleting the possibility to overrule a decision of a national supervisory authority in a specific matter through an implementing act. Ensure that the role of the Commission consists in an initial phase in triggering the seizure of the Board, as foreseen in Article 58(4), and in a subsequent phase in the power to adopt opinions. Insert a reference to a further procedure before the Court of Justice, in the context of an infringement procedure or of a request for interim measures such as a suspension order.
- Article 66: add that the Board shall be consulted in the context of adequacy assessments.
- Reconsider the current assessment of the impact of the secretariat of the European Data Protection Board in terms of financial and human resources (see the Annex to the present Opinion, available on the EDPS website).

Chapter VIII - Remedies, liability and sanctions (part II.10)
- Article 73 and 76: provide clarity about the mandate that the organisation must obtain from data subjects and the degree of formality required. Introduce a wider provision on collective actions.
- Article 74(4): limit the type of 'concern' of a data subject which could trigger the proceedings and restrict it to a more precise risk of impact on the data subject's rights.
- Article 75(2): specify that the derogation does not apply to a public authority of a third country.
- Article 76(3) and (4): insert a more systematic information procedure at the level of courts.
- Clarify the interaction with the Brussels I Regulation.
- Clarify the compatibility of the use of information obtained from a controller (on the basis of Article 53) with the general right against self-incrimination.
- Article 77: add that a data subject should always be able to address the controller, regardless of where and how the damage arose with regard to settlement of damage. Insert the subsequent settlement of the damage between the controller and the processor, once the distribution of liability among them has been clarified. Add that this should also apply to the compensation of immaterial damage or distress
- Introduce a provision using the concept of single economic entity or single undertaking to allow holding liable the group for the breach committed by a subsidiary.
- Article 79: insert a margin of appreciation for supervisory authorities with regard to administrative sanctions. Add specifications highlighting the circumstances in which an administrative sanction shall be imposed. Ensure that non-compliance with a specific order of a supervisory authority normally qualifies for a higher administrative sanction than a single breach of the same general provision.

Chapter IX - Specific data processing situations (part II.11)
- Article 80: rephrase Article 80 and state that Member States shall provide for exemptions or derogations from the provisions of the Regulation as indicated if such is *necessary* for reconciling the right to data protection with the right to freedom of expression. Add, in the provision or in a recital, that when reconciling the two fundamental rights the essence of both rights should not be impaired.
- Add a substantive provision on public access to documents stating that personal data in documents held by public authorities and bodies may be publicly disclosed if such is (1) provided for by EU or national law, (2) necessary for reconciling the right to data protection with the right of public access to official documents and (3) constitutes a fair balance of the various interests involved.
- Replace in Article 81, 82, 83 and 84 the wording 'within the limits of this Regulation' by 'without prejudice to this Regulation'.

- Article 81: Align Article 81(1)(3) and 9(3) and clarify the scope and nature of Article 81. Further direction should be given on the requirement of consent, the determination of responsibilities and the security requirements.
- Article 83: include additional safeguards if special categories of data are processed. Make clear in Article 83(1) that the point of departure for research purposes should be that such processing is done with use of anonymised data. Clarify what is meant by the word 'separately' and ensure that separate storage actually protects the data subjects. Refer in Article 83(1)(b) to 'data which enables to relate certain information to a data subject' instead of ‘data enabling the attribution of information to an identified or identifiable data subject’. Exclude the limitation to rights of individuals via delegated acts.

Recommendations on the proposed Directive

Horizontal issues (part III.2)
- Article 59: specific acts in the area of police and judicial cooperation in criminal matters should be amended at the latest at the moment the Directive enters into force.
- Add a new provision introducing an evaluation mechanism for regular evidence based assessments of whether data processing activities of a certain scale do actually constitute a necessary and proportionate measure for the purposes of preventing, detecting, investigation and prosecuting criminal offences.
- Add a new provision to ensure that transfer of personal data from law enforcement authorities to other public bodies or to private parties is only permissible under specific and strict conditions.
- Add a new provision on specific safeguards in relation to the processing of data of children.

Chapter I and II - General provisions and principles (part III.3 and III.4)
- Article 3(4): substantiate further in line with Article 17(5) of the proposed Regulation.
- Article 4(b): include clarification in a recital stating that the notion of 'compatible use' is to be interpreted restrictively.
- Article 4(f): align with Article 5(f) of the proposed Regulation and amend Articles 18 and 23 accordingly.
- Article 5: include non-suspected persons as a separate category. Delete 'as far as possible' and specify the consequences of the categorisation.
- Article 6: delete 'as far as possible' in paragraphs 1 and 2.
- Article 7(a): change into a self standing provision ensuring in a general manner that all data processing operations are provided for by law, thereby fulfilling the requirements of the EU Charter of Fundamental Rights and ECHR.
- Article 7(b) to (d): replace by an additional, separate provision which exhaustively lists the grounds of public interest for which a derogation to the purpose limitation principle can be allowed.
- Add a new provision on the processing of personal data for historical, statistical and scientific purposes.
- Add an obligation for the competent authority to put mechanisms in place to ensure that time limits are established for the erasure of personal data and for a periodic review of the need for the storage of the data, including fixing storage periods for the different categories of personal data as well as regular checks on their quality.
- Article 8: include the strict wording of recital 26 in Article 8. Include what is envisaged by suitable measures going beyond regular safeguards.

Chapter III - Rights of the data subject (part III.5)

- Article 10: delete the reference to 'all reasonable steps' in Article 10(1) and (2). Include an explicit time limit in Article 10(4) and state that information should be given to the data subject at the latest within one month of receipt of the request. Replace the wording 'vexatious' in Article 10(5) by 'manifestly excessive' and provide further guidance on this notion in a recital.
- Add a new provision requiring the controller to communicate to each recipient to whom the data have been disclosed, any rectification, erasure or change of the data either or not carried out in accordance with Article 15 or 16, unless this proves impossible or involves a disproportionate effort.
- Articles 11 and 13: add a sentence in Article 11(4) and Article 13(1) stating that the controller should be required to assess in each specific case by way of a concrete and individual examination whether partial or complete restrictions for one of the grounds applies. Ensure a limited interpretation of the scope of Article 11(5) and Article 13(2). Delete the word 'omitting' in Article 11(4) and Recital 33.
- Article 15 and 16: add grounds and conditions for restricting the right to rectification and the right to erasure.
- Article 16: use the wording 'shall restrict processing' instead of 'shall mark' in Article 16(3). Include in Article 16 the obligation for the controller to inform the data subject before lifting any restriction on processing.

Chapter V - Controller and processor (part III.6)

- Article 18: state, also in Article 4(f), that the documentation requirement stems from the general obligation to be able to *demonstrate* compliance with the Directive. Include a requirement to keep information on the legal ground on which the data is transferred, with a substantive explanation especially if a transfer is based on Article 35 or 36.
- Article 19: substantiate the notion of data protection 'by default'.
- Article 23(2): align with Article 28(2) of the proposed Regulation.
- Article 24: include the identity of the recipients of the data.
- Insert a new provision, requiring the competent authorities to carry out a DPIA, unless a specific assessment, equal to a DPIA, has already been made during the legislative process.
- Article 26: align more closely with the procedures developed in Article 34(2) of the proposed Regulation.
- Article 30: deal with the issue of conflict of interest and lay down a minimum term of office of two years.
- Article 31: provide for an appropriate administrative attachment with due regard for the independent role of the DPO and with a view in particular to avoiding possible uneven relations or influence by high rank controllers.

Chapter V - Transfer to third countries (part III.7)

- Article 33: add the requirement that the transfer may only take place if the controller in the third country or the international organisation is a competent authority within the meaning of the proposed Directive.
- Article 35: delete Article 35(1)(b) or as a minimum include the requirement of a prior authorisation of the supervisory authority.
- Article 36: clarify in a recital that any derogation used to justify a transfer needs to be interpreted restrictively and should not allow the frequent, massive and structural transfer of personal data; even an individual case should not allow wholesale transfers of data and should be limited to data strictly necessary. Add additional safeguards such as the obligation to specifically document the transfers.

- Articles 35 and 36: add that in case of a negative decision on adequacy, transfers should be based (i) on Article 35(1)(a) if there is a legally binding international agreement allowing for the transfer under specific conditions guaranteeing an adequate protection, or (ii) on the derogations of Article 36(a) or (c).

Chapter VI and VII - Oversight mechanisms (part III.8)

- Article 44: provide more guidance in a recital on what is meant to be covered by 'judicial capacity'.
- Article 46: align the powers of the supervisory authorities vis-à-vis national police authorities with the powers under the proposal for a Regulation. Align Article 46(a) with Article 53 of the proposed Regulation and change the wording 'such as' in Article 46(a) and (b) into 'including'.
- Article 47: include that the annual activities report of the supervisory authorities must be presented to the national parliament and made public.
- Article 48: include the provisions of Article 55(2) to (7) of the proposed Regulation in Article 48.
- Consider the need for an enhanced cooperation mechanism also in the scope of application of the proposed Directive.

Done in Brussels, 7 March 2012

(**signed**)

Peter HUSTINX
European Data Protection Supervisor