ADDITIONAL EDPS COMMENTS ON THE DATA PROTECTION REFORM PACKAGE

I. ANONYMISATION AND PSEUDONYMISATION

1. Concepts

1. Many amendments have been proposed to define anonymisation and pseudonymisation, and to provide for special rules regarding data treated in this way[1]. While carefully considered measures *may* create incentives to increase the use of these techniques with the aim of improving data protection, too broad exemptions could lead to eroding the long-established concept of personal data as defined in Directive 95/46/EC. **In the EDPS' view, it should be ensured that amendments regarding the definition of anonymous data and pseudonymous data are fully consistent with the definition of personal data and that they do not lead to unduly removing certain categories of data from the scope of the Regulation, in particular in cases where it is not clear whether the data have indeed been fully anonymised. In such cases, the data should remain within the scope of the Regulation.**

2. In particular, one should not exclude from the scope of the Regulation, or some of its principles, certain categories of data which are not irreversibly *anonymised*. The EDPS also cautions against those amendments which confuse pseudonymisation with anonymisation and, as a consequence, remove *pseudonymised* data from the scope of the Regulation or some of its core principles. More specifically:
    - LIBE amendments 729, 730 and other similarly worded amendments suggesting a definition of 'pseudonymous' or 'pseudonymised' data could be accepted with some adjustments of their language, in line with our comments in point 2 below,
    - The EDPS advises against LIBE AM 726 and 728.
    - Amendments that would make pseudonymisation a sufficient reason to make data processing legitimate, such as LIBE AM 887, 897, 898, 900, or allow profiling with such data, e.g. LIBE AM 1568, 1585 should be **rejected**.

2. Definitions

3. The definition of personal data has been set forth in Article 2(a) of Directive 95/46/EC (read together with recital 26). Furthermore, the Article 29 Working Party provided guidance on the notion of personal data[2], distinguishing a number of

[1] In some cases, also encryption of data is considered in a similar way, while this is a completely different technical measure with limited effect mainly on data security.
[2] Article 29 Working Party Opinion 4/2007 on the concept of personal data, WP 136, 20.06.2007.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

criteria that help assess whether the definition applies. The essential criterion is the **identifiability** of the individual. This criterion contains two elements:

(a) whether the individual is *directly* or *indirectly* identifiable, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Article 2(a) Directive), and

(b) *in relation to whom*: the controller, the processor and any third party using reasonable means to identify that individual (recital 26 Directive).

4. It should furthermore be noted that means that could be used by the controller or any third party to identify an individual have increased since 1995 due to technological progress. This trend is expected to continue in the future.

5. **Anonymisation** of personal data means changing a data set so that it becomes impossible for the controller or for anyone else to identify a person to whom the data relate either directly or indirectly. **Anonymous data are not personal data and fall outside the scope of data protection legislation.** Anonymisation requires not only deleting all directly identifying attributes (e.g. names, civil registry numbers, phone numbers, biometric data) from the data set, but usually also data which in combination reveal unique characteristics and any further modifications[3], to prevent re-identifiability. Some types of personal data, such as biometric data, are sufficient by themselves to identify data subjects and therefore cannot be part of any anonymised data set by their very nature (e.g. facial photographs, fingerprints). Recent research suggests that also fine grained location data can be sufficient by itself to identify the individual it relates to. The concept of identification moreover involves the capacity to distinguish an individual from all other individuals ('singling out'), even when commonly used identifiers are not available.

6. On the other hand, **pseudonymised data** is by definition data relating to an identifiable individual, as the connection between the pseudonym and the identifying data (e.g. first and last names, address etc.) is known to the data controller or to a third party. Even if the pseudonym and its correlation with the identity are exclusively known to one given party (whether the controller or a trusted third party) and are not shared with anyone, **pseudonymised data remains personal data**[4]. **Pseudonymised data therefore falls within the scope of the Regulation**[5].

[3] If data sets contain a sufficient number of attributes, the probability is high that individuals have a unique combination of values and can be identified. Research has shown that even statistical data sets can be re-identified, if no specific measures are taken to avoid this. See as an example: http://www.census.gov/srd/papers/pdf/rrs2012-13.pdf

[4] Data records which do not contain common identifying attributes (such as name and address) but unique values used in transactions with many parties (such as IP addresses or cookie numbers) cannot even be considered pseudonymous as many third parties have knowledge of these attributes and may be able to identify the related individual. In such case, these data are personal data, as identifiable 'by reference to an identification number, location data, online identifier...'.

[5] Another completely different technique is encryption, which is the technical process of temporarily scrambling data into an unreadable or unintelligible form for confidentiality or integrity purposes, in such a way that eavesdroppers or hackers cannot read it, or modify it, while authorized parties can. Encrypted personal data should not be considered as anonymised data since the scrambling is only temporary, any holder of the key to

7. Taking these considerations into account, the EDPS suggests that any definition of 'a pseudonym' builds on the following elements:

   - 'pseudonymised data' refers to information relating to a natural person who can be identified, directly or indirectly (i.e. remains within the remit of 'personal data'),
   - the means that may be used to identify the person are effectively separated from the data involved, and
   - the identification by unauthorised persons is effectively prevented.

3. Consequences for further parts of the proposal

8. Since **pseudonymous data remains personal data**, the EDPS advises against amendments that exempt processing of pseudonymous data from core data protection principles, such as transparency, lawfulness of processing, and data subjects' rights. At the same time, the Regulation could include incentives for controllers or processors to the *'bona fide'* use of pseudonymous data, provided that the processing is subject to strict conditions (e.g. on security and confidentiality). That could be the case, for example, in the context of personal data breach provisions (Articles 31 and 32), depending on whether or not the data affected by the breach has been adequately protected against identification, or provisions on research and statistics (Article 83). It could also be considered for the design of new IT systems (Article 23 on data protection by design).

II. SCOPE OF THE REGULATION

1. Material scope

9. With regard to the material scope of the Regulation, the EDPS notes with concern a trend visible from numerous amendments proposed to **Article 2**, restricting the scope of application of the future Regulation by creating exceptions for specific sectors or processing situations (e.g. the financial sector or employment context). While the EDPS recognises that, in certain cases, special arrangements are justified, he notes that many of those are already covered in Chapter IX relating to specific data processing situations. Furthermore, a number of exceptions for specific purposes are defined in Article 21, which sets forth the conditions that any restriction to the rights and obligations provided in the Regulation should fulfil. Adding further exceptions in Article 2 would not only result in significant gaps in protection of the fundamental rights of EU citizens, but also goes against the very idea of creating a single (as comprehensive and uniform as possible) data protection framework for Europe. The EDPS therefore advises against those exceptions.

---

the encryption process can easily recover the data, and encryption can be broken without a key, given sufficient resources. Nevertheless, strong and up-to-date encryption can considerably reduce the risk (and consequences) of some data breaches and should therefore be recognized and encouraged as an important security measure (e.g. in Article 30) where applied properly.

(a) EU institutions and bodies

10. The EDPS notes a series of amendments (e.g. LIBE AM 666) which delete the exemption for EU institutions in Article 2, thus including EU institutions, bodies, offices and agencies in the scope of application of the future Regulation.

11. These amendments are in line with earlier EDPS recommendations[6] and should be supported in principle. At the same time, however, it should be stressed that **more than a simple deletion of the exception in Article 2 will be needed** in order to provide a coherent legal framework and sufficient legal certainty for all actors concerned, given the specific legal and institutional setting in which they operate. Indeed, Regulation (EC) 45/2001 currently applicable to EU institutions and bodies covers certain issues which are specific to the EU institutional context and which under the proposed general Regulation would remain unregulated. These include: (i) transfers of personal data between EU institutions, as well as between those institutions and other recipients; (ii) the rules applicable to data processing in internal telecommunications networks[7]; (iii) the rules governing the appointment of the European Data Protection Supervisor and the Deputy Supervisor; and (iv) a detailed catalogue of duties and powers of the EDPS which do not entirely overlap with those of the national supervisory authorities, and cannot entirely overlap since they e.g. deal with the relationship between the EDPS and the Court of Justice of the EU.

12. The EDPS therefore advises against the simple deletion of the exception of Article 2 without further text dealing with the above matters, and would at least be strongly in favour of a recital stressing the need to fully align the data protection framework for EU institutions and bodies with the Regulation by the time it becomes applicable[8].

(b) Courts in their judicial capacity

13. Among the amendments concerning the scope of the supervisory powers of the national data protection authorities (Article 51 of the proposed Regulation), the EDPS welcomes those which would allow Member States to extend such powers also to processing operations of courts acting in their judicial capacity (LIBE AM 2595). This is in line not only with Convention 108 and its protocol on independent supervision, but also with the tradition of several Member States and should be supported. This conclusion also builds on the fact that the current limitation in the Commission's proposal does not apply to public prosecutor offices as well.

2. Limitation *rationae temporis*

14. The EDPS considers that limiting the application of the Regulation in time (as e.g. in LIBE AM 664 and 665) is not necessary, given that the proposed *vacatio legis* (two years) appears long enough to bring all existing processing operations in line with the new rules. The EDPS advises against these amendments.

---

[6] See EDPS Opinion of 7 March 2012 on the data protection reform package, para.29-31.

[7] These rules are roughly equivalent to those included in Directive 97/66/EC which was later revised and replaced by the ePrivacy Directive 2002/58/EC.

[8] See Article 91(1) of the Commission proposal.

3. Territorial scope

15. As to the territorial scope of application, some amendments have been proposed to Article 3(1) that restrict the data subjects to be covered by the Regulation only to those **'residing in the Union'** (LIBE AM 700, LIBE AM 701, LIBE AM 703).

16. If accepted, these amendments would purport to deprive of protection large groups of data subjects which today are protected by Directive 95/46/EC. These include e.g. tourists, as well as processing activities conducted in the EU on data subjects residing abroad, creating a double legal standard within the Union. Furthermore, it should be noted that this restriction in secondary law is contrary to primary law, namely Article 16 TFEU and Article 8 of the EU Charter of Fundamental Rights, which explicitly afford the right to protection of personal data to 'everyone', meaning every individual who falls within the scope of EU law, irrespective of his or her place of residence. This has also been an important starting point in discussions with third countries. Given that the proposed Regulation limits the scope of the subjective rights in an appropriate manner, **the EDPS advises against these amendments.**

III. PURPOSE LIMITATION AND LAWFULNESS OF THE PROCESSING

1. Purpose limitation

17. The EDPS particularly welcomes LIBE AM 103 proposing **to delete Article 6(4)** as proposed by the Commission. **Article 6(4)** opens the possibility to process data for incompatible purposes as long as it has a legal basis in Article 6(1)(a) to (e). This text would, in effect, mean that it would always be possible to remedy the lack of compatibility by simply identifying a new legal ground for the processing. However, the EPDS underlines[9] that the prohibition of incompatible use and the requirement of lawfulness are cumulative requirements. 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 the Council of Europe Convention 108 which is binding on all Member States.

18. Today, the logic of Directive 95/46/EC is that incompatible use is only allowed subject to the conditions of Article 13 for certain reasons of public interest (cf. Article 21 of the proposed Regulation). Therefore, **the EDPS supports the deletion of Article 6(4)**, which would preserve the logic of Directive 95/46/EC (while a change of purpose would be possible under strict conditions in accordance with Article 21). The issue of compatibility is a key topic on which the Article 29 Working Party will adopt an opinion in the coming weeks. This opinion will provide substantive guidance and criteria for a common understanding of the notion of 'compatibility'.

19. The EDPS advises against amendments suggesting that further processing of data for health purposes should not be considered as incompatible (LIBE AM 821), as the further processing of such sensitive data may have strong implications on the privacy of individuals. Under current law, the scope for further processing depends on criteria such as those just referred to.

[9] See also EDPS Opinion of 7 March 2012, para. 115-124.

2. Lawfulness of the processing

20. The LIBE draft report proposes long prescriptive lists for **Article 6(1b) and 6(1c)** which would describe in what situations the legitimate interests of the controllers override the rights and interests of the data subjects and vice versa (LIBE AM 99-102). **In the EDPS' view, these prescriptive lists are counter-productive and should be rejected**.

21. The EDPS advises replacing these lists by a more concise provision, taking into account that there are many situations that cannot be foreseen in advance and that need to be assessed *in concreto* on a case-by-case basis. In addition, **a recital** could list the most typical relevant factors that should be taken into account when balancing the interests and fundamental rights at stake. If necessary, some examples can also be given of what might constitute 'legitimate interests'.

22. In contrast, the EDPS welcomes the proposed amendment to **Article 6(1a)** (LIBE AM 100), which calls for more transparency on 'the reasons for believing that its interests override the interests or fundamental rights and freedoms of the data subject.' This would encourage more accountability for the way in which an acceptable balance of interests should be struck.

23. Finally, the EDPS stresses that the concept of **explicit consent** as currently defined in the Commission proposal (in particular Articles 4(8), 6(1)(a) and 7) **should be maintained**. It provides for some flexibility as to its manner of expression (by a statement or a clear affirmative action) and builds on the requirement of 'unambiguous' consent which constitutes an essential element of the overall balance of data protection since 1995. EU data protection authorities have consistently interpreted the requirement of Article 7(a) of Directive 95/46/EC, in relation to Article 2(h), that the consent be 'unambiguous' as meaning that such consent needed to be 'explicit'[10] (so that, for instance, a lack of action or silence cannot be considered as unambiguous). Consequently, the EDPS recommends that amendments such as ITRE AM 83, IMCO AM 63, and proposed LIBE AM 757, 758, 760, 764-766 etc. be **rejected**.

IV. ROLES, RESPONSIBILITIES AND LIABILITY OF CONTROLLER VS. PROCESSOR

24. Amendments related to controller/processor's roles appear in many parts of the text, including in the definitions. Several amendments would remove the notion that the controller determines **not only the purposes but also 'the conditions and means'** of the processing, as defined in Article 4(5) of the proposal (e.g. ITRE AM 81; IMCO AM 62; LIBE AM 746, 747, 748). The criteria that the controller determines the 'purposes and means' of the processing were set forth in Directive 95/46/EC and developed in the WP 29 Opinion 1/2010 on the concepts of 'controller' and 'processor'. **These criteria have effectively contributed to the understanding and delineation of the roles of controllers and processors and should not be deleted.**

[10] See in particular Article 29 Working Party Opinion 15/2011 on the definition of consent, WP 187, 13.07.2011.

25. Many amendments aim at diminishing the responsibility of the processor foreseen in the proposal, for example by removing or weakening the obligations that the processor maintains documentation, carries out a data protection impact assessment (DPIA), or helps the controller comply with security requirements (i.e. ITRE AM 43, 229, 233, 238, 260; LIBE AM 1829, 1832, 1834, 1836, 1837, 2024). However, the extension of certain obligations to processors reflects the current growing role of processors in determining certain essential conditions of the processing (e.g. in the context of cloud computing, where they often decide on transfers and sub-processing). **In this context, processors should also be accountable for their processing.** The clarification that processors which do not follow instructions or go beyond the instructions become controllers (Article 26(4)) should remain. The EDPS therefore advises against suggestions in ITRE AM 231 and LIBE AM 1808-1810.

26. The **three components of accountability should remain: ensuring**, **demonstrating**, and **verifying compliance**. Several amendments from several committees that try to delete all or some of these aspects of accountability, with a view to reducing the burden on controllers (e.g. ITRE AM 199, 204, 207; LIBE AM 1658, 1661, 1687, 1688, 1834, 1836), should be rejected. In addition, amendments suggesting deleting Article 28 on documentation (LIBE AM 1825, 1826, 1830) should be rejected.

27. Albrecht AM 188 proposes that the documentation that needs to be kept under Article 28 essentially duplicates the information that must be given to the data subject under Article 14, in order to reduce administrative burdens. Although this seems like a simplification, as the list in Article 28 overlaps to a certain extent with the list of information to be provided to data subjects in Article 14, it is doubtful that the documentation listed in Article 14 (even as extended by Albrecht AM 125-133) is enough to verify compliance. In the EDPS' view, the information to be kept as documentation should contain sufficient information to allow the verification upon request by supervisory authorities of the following two aspects in relation to processing operations:

    (i) it should record evidence of how the system of control of processing operations is structured, and

    (ii) it should record evidence of how both are performing (e.g. on the basis of log files).

28. Finally, the EDPS welcomes amendments that describe in more details measures that organisations should implement internally to help ensure accountability (such as internal policies and procedures, training of staff, evidence of top-level management commitment, reviewing the effectiveness at regular defined intervals, suggested in ITRE AM 205, 210, 212, 213; LIBE AM 1684, 1698).

V. FLEXIBILITY, RISK-BASED APPROACH, MSMEs

29. Several amendments aim at introducing a risk-based approach with a detailed list of what would constitute risky processing operations. **The EDPS advises against amendments that may have as an effect that protection would only apply to the most risky processing operations.** The full protection foreseen in the Regulation

should apply to all processing operations, not only to the most risky ones (for example, the principle of data protection by design should not apply only 'where required' or following a risk based approach, as suggested by IMCO AM 138 and 140, ITRE 216). It should be taken into account that risk is inherent to any data processing. Furthermore, the EDPS recommends rejecting amendments that change the balance between risk and measures, e.g. in relation to Article 30 on security (ITRE AM 243, LIBE AM 1922, 1923, 1924, 1925, 1926). The required risk management will ensure proportionality of effort and risk.

30. In contrast, **the EDPS notes many positive elements in the progressive risk-based approach that is being pursued in Council**[11]. The approach suggests that more detailed obligations should apply where the risk is higher, and where it is lower the level of prescriptiveness should be reduced. A horizontal risk clause would be introduced in Article 22 and many provisions of Chapter IV of the Regulation would be redrafted with a view to giving more importance to **the principle of accountability**. Incentives are being sought in order to lighten controllers' obligations for organisations that have implemented measures that contribute to accountability.

31. In this respect, several amendments have also been put forward in Parliament to put more weight on the notion of accountability and to lighten up several obligations of the controller, including in relation to notifications to the supervisory authority (in particular regarding Articles 22-29 and 33-34). **The EDPS welcomes amendments that give more effect to the principle of accountability,** as he recognises the need for introducing more flexibility in respect of organisations that have put in place accountability mechanisms, such as the appointment of a data protection officer (DPO) or the implementation of recognised certification mechanisms.

32. On the other hand, lightening certain controller's obligations in this context should not lead to removing important obligations in respect of risky processing. In particular, the EDPS advises against amendments that would exempt controllers from the obligation to carry out a data protection impact assessment when they have appointed a DPO or are subject to a certification mechanism (JURI proposed AM 297) or when the processing is based on consent or on a legal obligation (LIBE AM 2020). In all these cases, processing that are particularly risky should still require conducting a data protection impact assessment in order to assess, and thereby, mitigate the risks. Furthermore, the EDPS advises against amendments that would remove the obligation for the controller to consult the supervisory authority prior to engaging into risky processing operations (e.g. ITRE AM 207, 208, 272, LIBE AM 2108). **The requirement to notify the supervisory authority in cases of risky processing should remain, while the modalities of the procedure with the supervisory authority may themselves be lightened.** For instance, incentives could be provided for those organisations that use specified accountability mechanisms so that the notification in such case would be handled in a speedy and simplified prior consultation procedure, only in order to verify good practice.

33. In this respect, the EDPS believes that **there should be more incentives for the use of data protection officers.** For instance, while certain obligations should remain applicable to the controller in respect of risky processing operations, such as

[11] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/135901.pdf.

the need to notify the processing to the supervisory authority for prior consultation, lighter procedures could be envisaged when a DPO has been appointed, whereby in such case the processing operation could start from the date of the notification, without having to wait for a reply from the supervisory authority. Furthermore, beyond the issue of deciding whether the appointment of a DPO should be made mandatory or optional, it should be recognised that every organisation needs to have mechanisms in place to deal with data protection requirements. This requires relying on several persons internally (such as in IT, legal, HR and compliance departments) to ensure compliance of the organisation's processing operations with these requirements. In many cases, entrusting an additional person with the overall responsibility for data protection issues across departments may prove not only beneficial but also necessary to the organisation.

34. Several amendments aiming at introducing new exceptions for micro-, small- and medium enterprises should be rejected as they would exempt them from general principles of the Regulation, and not only from specific provisions. For instance, they aim at removing the processing carried out by MSMEs for 'internal use' from the scope of the Regulation (LIBE AM 678-680) or at exempting MSMEs from maintaining the documentation foreseen in Article 28 (e.g. ITRE AM 235) or from carrying out a data protection impact assessment especially where processing is a core of their business (ITRE AM 160). Exceptions or limitations for specific provisions could be envisaged only where that is appropriate[12].

VI. TRANSFERS, INCLUDING PROPOSED ARTICLES 43a AND 44a

35. Amendments aiming at clarifying or adding elements to the principle of '**adequacy**' should be **rejected** as they are likely to only create confusion (JURI AM 53, LIBE AM 2383 to 2386).

36. Adequacy should remain possible for **sectors,** as is currently the case for certain adequacy decisions, for instance the US Safe Harbor (only applicable to some areas of the private sector), or Canada (only covering the private sector). Some amendments to Article 41.1 eliminate this possibility (LIBE AM 241). This would be contrary to the recognition of the 'adequacy principle' as a 'functional concept', in order to allow meaningful data exchange with third countries (or a processing sector within a third country). **The EDPS advises against these amendments.**

37. On the other hand, regarding the transfers to third countries declared inadequate, the Commission proposal was unclear as to whether Article 41(5) prohibits transfer to these countries in total or whether transfers would be possible under certain conditions (inconsistency between Recital 82 and Article 41(5)). In light of this, the EDPS considers that positive amendments to Article 42(1) have been included clarifying that appropriate safeguards can be adopted for those cases where the Commission has issued a non-adequacy decision in accordance with Article 41(5) (LIBE AM 2415, ITRE AM 305 first part of the AM, JURI AM 55). **These amendments should therefore be supported.**

38. The EDPS supports the amendments that **extend the scope of BCRs** (Article 43(1)(a)) so that they also apply **to their external subcontractors** (LIBE 2470 to

[12] See EDPS Opinion of 7 March 2012, para. 79-80.

2479). This extension could enhance protection and could contribute to legal certainty in areas such as cloud computing, which are characterised by a multitude of relations with subcontractors.

39. Some amendments have introduced a new **Article 43(a) on transfers not authorised under EU law** (Albrecht AM 259, LIBE AM 2490, also JURI AM 354). The EDPS supports these amendments that e.g. address the cases where a request from a foreign (third country) judge requires a controller or processor bound by EU data protection law to transfer personal data (e.g. e-discovery cases).

40. Another amendment proposes to add **a new Article 44a** (LIBE AM 2531) on transfers to cloud services under third country jurisdiction. More transparency is indeed welcome in this field. However, the risks that this amendment envisages to address by imposing certain requirements are not specific to cloud computing, but are the typical risks of international transfers. It is true that, in the cloud computing arena, these risks are more obvious and the data subjects' rights are more uncertain, because it is not always possible to know where the personal data are located, or what the possible risks inherent to the country (or countries) of destination are. Nevertheless, creating new requirements should not be done in a way that is not technologically neutral. **The EDPS would therefore advise against this amendment.**

VII. COOPERATION, CONSISTENCY, BINDING POWERS EDPB

41. In general the EDPS welcomes a mechanism that provides a 'one-stop-shop' for controllers but which does not grant *exclusive* competence to the 'lead authority' and thus allows data subjects to address the supervisory authority of their own country of residence (Albrecht report AM 277 introducing a new Article 54(a)).

42. The EDPS welcomes amendments (in the draft Albrecht report) that remove the possibility for the Commission to intervene at different occasions in the context of the consistency mechanism and to overrule a decision of a national supervisory authority in a specific matter by way of adopting an implementing act (as was foreseen in Articles 58, 59, 60(1) and 62(1)(a) of the proposed Regulation). As underlined in his Opinion of 7 March 2012, these powers of the Commission would prejudice the independence of national supervisory authorities guaranteed under Chapter VI and would be contrary to the TFEU, the EU Charter of Fundamental Rights and the case law of the Court of Justice of the EU.

43. Among the options presented, the EDPS would prefer the one proposed by the Albrecht draft report on Chapters VI and VII. However, the draft report leaves some questions unresolved as regards the architecture of the system. The EDPS believes that further thinking is needed on the role of the EDPB in the consistency mechanism, on issues such as whether or not it should be issuing binding decisions, and if so under which modalities. Such reflection should take particularly into account the need for uniformity in the EU as well as the need to offer a legal remedy to individuals and organisations. The point of departure of such reflection should be that national supervisory authorities remain primary responsible and accountable in their national legal systems.

44. **The EDPS recommends rejecting the amendments proposed by the ITRE opinion**, which water down the consistency mechanism and would give an important role to powerful lobbies. The EDPS would also advise against amendments aimed at allowing controllers, data subjects or 'stakeholders' to trigger the consistency mechanism, as this would render the system impracticable (see for example IMCO AM 195 or ITRE AM 352). Individuals should always be able to seek judicial redress in their own national courts.

45. Finally, the EDPS considers that the European Data Protection Board could benefit from an appropriate IT tool to support the information exchanges among the supervisory authorities, such as the Internal Market Information System IMI[13], and notes that, should the use of an IT tool be considered, it might require a legal basis to be included in the Regulation.

VIII. SANCTIONS

46. The EDPS recalls that in his Opinion of 7 March 2012 he advocated strengthening the new right for organisations and associations defending data subjects' rights to lodge a complaint before a supervisory authority or to bring an action to court (Articles 73 and 76 of the proposed Regulation). He therefore considers that **amendments which would weaken such collective action** (or even eliminate it altogether, as in LIBE AM 2777 and following) **should not be supported.**

47. The Opinion also called for more flexibility in applying sanctions for breaches of the Regulation. A margin of appreciation for supervisory authorities is an indispensable element of a consistent and scalable enforcement scheme, in particular in view of the different options that would be available to supervisory authorities to impose *remedial* sanctions in case of a breach of the Regulation (see Article 53(1)(a)). From this point of view, **the EDPS welcomes amendments which grant supervisory authorities a wider margin of appreciation in deciding whether or not to impose a sanction,** in particular with respect to cases of non-compliance which was not intentional (e.g. Albrecht AM 318). At the same time, he considers that including lists of additional 'aggravating' or 'mitigating' criteria (as in Albrecht AM 316-317, ITRE AM 371-372, IMCO AM 206-207) requires further study to ensure a good balance between legal certainty on the one hand, and the needs of supervisory authorities to exercise their powers with sufficient flexibility.

48. Finally, the EDPS welcomes the attempts at ensuring **consistency** of the approach on sanctioning at EU level, for example through the European Data Protection Board (e.g. involving guidelines and exchange of information on sanctions which have been imposed).

[13] The IMI was formally set up by the Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC, OJ L 316, 14.11.2012.

IX. PRELIMINARY FINDINGS ON THE DIRECTIVE[14]

1. Scope of application

49. As explained under section II.1(a) above, the EDPS welcomes in principle that the proposed Directive would also apply to EU institutions and bodies (LIBE AM 270-272) although he wishes to stress that given the specific legal and institutional setting in which they operate, further clarifications are needed which are not addressed in the proposals currently on the table.

2. Data protection principles

50. The EDPS notes that several amendments attempt to address the issue of further processing for '**incompatible use**'. The EDPS recalls that any derogation to the principle of 'compatible use' should only be allowed for purposes that are clearly and exhaustively defined and subject to appropriate safeguards. In this context, he notes that LIBE amendments 66, 347, 350 contain several positive elements that could be used as a good basis for further development. As mentioned above (see section III.1), the EDPS would like to draw the attention to the opinion of the WP29 on purpose limitation to be adopted in the coming weeks. This opinion will provide further guidance and criteria for a common understanding of the notion of 'compatible use'.

51. The EDPS welcomes the amendments which strengthen the obligation to distinguish between the different categories of data subjects and the different degrees of accuracy and reliability of the data (e.g. LIBE AM 60, 318-319). These obligations - which are specific to the law enforcement sector - are important both for data subjects and for law enforcement authorities. Comparable obligations are also foreseen in EU legislation for police cooperation[15]. In this context, LIBE amendments 314-317 which delete the obligation to distinguish between categories of data subjects are not acceptable.

52. The EDPS takes note with satisfaction of the amendments creating an obligation for Member States to provide for specific rules on the consequences of the categorisation of data subjects (LIBE AM 330-331). He also welcomes LIBE AM 351 which introduces specific safeguards for 'non-suspects' in line with the recommendations made by the WP 29 in its Opinion of 26 February[16].

3. Exchange of information with private parties

53. The EDPS welcomes the intention to regulate the exchange of information between the law enforcement sector and private parties with a view to clarify - to some extent - the legal uncertainty about situations in which activities of the private sector and of the law enforcement sector interact with each other (e.g. where data are collected for commercial purposes and further accessed for law enforcement purposes but also where information is transferred from a law enforcement authority to private parties or non law enforcement authorities).

[14] These preliminary findings are based on the proposed LIBE amendments.
[15] See for instance article 14(1) of Europol Decision.
[16] Opinion 01/2013 of 26 February 2013 providing further input into the discussion on the draft Police and Criminal Justice Data Protection Directive.

54. As for the **access by law enforcement authorities to data initially processed for non-law enforcement purposes**, the EDPS positively notes that LIBE AM 58 and 310 introduce specific conditions and safeguards for accessing these data. He considers, however, that LIBE AM 310 which only requires a valid legal basis that ensures sufficient guarantees for the data subject, is too broad and does not provide the necessary safeguards. This amendment alone should therefore not be accepted.

55. With regard to the transmission of data by law enforcement authorities to other parties (i.e. non law enforcement authorities and private parties), the EDPS welcomes the intention to address this issue and the introduction of specific conditions for such transmission (e.g. LIBE AM 162). However, he wishes to draw attention in particular to amendments which intend to regulate transfers to non law enforcement authorities and private parties outside the EU (LIBE AM 589-590), as the proposed wording of these amendments undermines the level of protection (see below 'transfer of data to third parties').

4. Roles and responsibilities of the controller

56. The EDPS welcomes amendments which introduce essential elements of the principle of accountability which are missing from the Commission proposal. In particular, the EDPS welcomes the obligation for the controller to *demonstrate* compliance (e.g. LIBE AM 480), to perform a data protection impact assessment (e.g. LIBE AM 27-28, 110, 113) and to consult the DPA prior to the processing of personal data (e.g. LIBE AM 541 to 543). He also positively notes several amendments in so far as they strengthen the role and the status of the DPO (e.g. LIBE AM 120-123, 570, 573, 575-576, 578).

5. Transfer of data to third countries

57. The EDPS welcomes the requirement for the controller in the third country or international organisation to be a competent authority for law enforcement purposes (LIBE AM 126, 584) as foreseen in existing legal instruments in the area of police and judicial cooperation. Furthermore, he also welcomes in substance the additional conditions introduced by LIBE amendments 126 and 591.

58. He recalls that **any transfer to non law enforcement authorities or private parties should be strictly limited and subject to strong safeguards**. This is all the more important when such recipients are outside the EU. As already mentioned above, LIBE amendments 589 and 590 which envisage such transfer do not provide sufficient safeguards. Furthermore, these amendments raise serious concerns as according to their current wording transfer of data to non law enforcement authorities or private parties in third countries would be easier than to law enforcement authorities.

59. Finally, in his Opinion of 7 March 2012 the EDPS criticised the sole assessment of the controller as a legal ground to allow transfers to a third country and therefore welcomes the amendments proposing to remove this possibility (LIBE AM 33, 602).

6. Powers of supervisory authorities

60. In his Opinion, the EDPS has emphasized that if some limited exception may be justified **with regard to courts acting in their judicial capacity**, he does not see

any reason to limit the powers of the supervisory authorities outside this specific context. He therefore welcomes the amendments that align the supervisory authorities' powers vis-à-vis law enforcement authorities with the powers under the proposed Regulation (e.g. LIBE AM 142-645). He also welcomes LIBE amendments 645 and 649 insofar as they take into account the WP29 concerns about the need (i) to ensure that all supervisory authorities involved have access to the same information and (ii) to identify the information that is accessible[17].

7. Specific acts in the area of police and judicial cooperation in criminal matters

61. In his Opinion, the EDPS has regretted that specific acts in the area of police and judicial cooperation in criminal matters have been left untouched. He has stressed that the two years period referred to in Article 61(2) of the proposed Directive for the Commission to review these acts would lead to an unacceptably long period during which the current, widely criticised patchwork remains in force. Therefore, LIBE amendment 671 which deletes the obligation of such review is unacceptable.

Brussels, 15 March 2013

[17] Opinion 01/2013 of 26 February 2013 providing further input into the discussion on the draft Police and Criminal Justice Data Protection Directive.