Opinion of the European Data Protection Supervisor

on proposals for a Directive on insurance mediation, a Directive amending certain provisions of Directive 2009/65/EC on the coordination of laws, regulations and administrative sanctions relating to undertakings for collective investment in transferable securities and a Regulation on key information documents for investment products

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 Articles 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 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2], and in particular Article 28(2) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 3 July 2012, the Commission adopted a proposal for a Directive on insurance mediation (hereafter 'the IM Directive'), a proposal for a Directive amending certain provisions of Directive 2009/65/EC on the coordination of laws, regulations and administrative sanctions relating to undertakings for collective investment in transferable securities (hereafter 'the UCITS Directive') and a proposal for a Regulation on key information documents for investment products (hereafter 'the KID Regulation'). These proposals were sent to the EDPS for consultation on 5 July 2012.

2. The EDPS welcomes the fact that he is consulted by the Commission and recommends that a reference to this Opinion is included in the preambles of the proposed legal instruments.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.

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

3. Comparable provisions to the ones referred to in this Opinion are present in several pending and future proposals, such as those discussed in the EDPS Opinions on the legislative package on the revision of the banking legislation, credit rating agencies, markets in financial instruments (MIFID/MIFIR) and market abuse[3]. Therefore, this Opinion should be read in close conjunction with the EDPS Opinions of 10 February 2012 on the above mentioned initiatives.

4. The two proposed Directives and the proposed Regulation will affect the rights of individuals relating to the processing of their personal data in different ways as they deal with the investigatory powers of competent authorities including access to existing telephone records and traffic data, databases, publication of administrative sanctions including the identity of those responsible and the reporting of breaches (so called whistle blowing schemes).

5. As the issues discussed in this Opinion have been discussed in past EDPS Opinions in the Financial area, the EDPS intends to publish guidelines on these and other issues concerned in order to give guidance on how do deal with Data Protection issues in future Commission proposals in this area.

1.2. Objectives and scope of the proposals

6. The Commission states that strong, well-regulated retail markets that place the best interests of consumers at their heart are necessary for consumer confidence and economic growth in the medium and longer term. Specifically, according to the Commission, the above mentioned legislative proposals introduce new, consumer-friendly standards for information about investments, raise standards for advice, and tighten certain rules on investment funds to ensure their safety.

2. ANALYSIS OF THE PROPOSALS

2.1. General reference to data protection legislation

7. The **proposed UCITS Directive** (Article 104a), the **proposed IM Directive** (Article 32) and the **proposed KID Regulation** (Article 17) all entail substantive provisions that mention Directive 95/46/EC and Regulation (EC) No 45/2001.

8. In view of the data protection implications of the **proposed Directives** and the **proposed KID Regulation**, the EDPS suggests emphasising the full applicability of existing data protection legislation in one general substantive provision in all proposals and that the reference to Directive 95/46/EC is clarified by specifying that the provisions will apply in accordance with the national rules which implement Directive 95/46/EC.

2.2. Investigatory powers of the competent authorities

9. According to Article 26 of the **proposed IM Directive**, Member States shall supervise insurance or reinsurance undertakings and insurance or reinsurance

[3] EDPS Opinions of 10 February 2012, available at http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Opinions.

intermediaries. This supervision will be carried out by national competent authorities. Article 26(3) of the **proposed IM Directive** states that the competent authorities shall have all the investigatory powers that are necessary for the exercise of their functions. Furthermore, the competent authorities shall cooperate closely in the exercise of their sanctioning powers. It seems likely - or at least it cannot be excluded - that information exchanges will take place which include personal data within the meaning of Directive 95/46/EC and Regulation (EC) No 45/2001. The conditions for fair and lawful processing of personal data, as laid down in the Directive and the Regulation, should therefore be fully respected[4].

10. The EDPS acknowledges that the aims pursued by the Commission in the **proposed IM Directive** are legitimate. He understands the need for initiatives aiming at strengthening supervision of financial markets in order to preserve their soundness and better protect investors and the economy at large. However, investigatory powers relating to insurance intermediaries, insurance undertakings and their employees, given their potentially intrusive nature, have to comply with the requirements of necessity and proportionality, i.e. they have to be limited to what is appropriate to achieve the objective pursued and not go beyond what is necessary to achieve it. It is therefore essential in this perspective that the provisions are clear on the circumstances in which and the conditions on the basis of which they can be used. Furthermore, adequate safeguards should be provided against the risk of abuse.

11. According to the EDPS, the circumstances and the conditions for using the investigatory powers of the competent authorities should be more clearly defined in the legislative provision. Article 26(3) of the **proposed IM Directive** does not indicate the circumstances and the conditions under which documents and information can be requested. Nor does it provide for important procedural guarantees or safeguards against the risk of abuses. The EDPS therefore recommends limiting access to documents and information to specifically identified and serious violations of the proposed Directive and in cases where a reasonable suspicion (which should be supported by concrete initial evidence) exists that a breach has been committed[5].

12. The EDPS recommends introducing, in Article 26(3) of the **proposed IM Directive**, the requirement for competent authorities to request documents and information by formal decision, specifying the legal basis and the purpose of the request and what information is required, the time-limit within which the information is to be provided as well as the right of the addressee to have the decision reviewed by a court.

2.3. Power of the competent authorities to access existing telephone records and traffic data

[4] See EDPS Opinions of 10 February 2012 on credit rating agencies (para 23), markets in financial instruments (MIFID/MIFIR) (para 46) and market abuse (para 26), available at http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Opinions.

[5] See EDPS Opinions of 10 February 2012 on credit rating agencies (para 35) and market abuse (para 33), available at http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Opinions.

13. Article 98(2)(d) of the **proposed UCITS Directive** empowers the competent authorities to '*require existing telephone records and traffic data'*. However it clarifies that the request is subject to the existence of a '*serious suspicion'* that such records *'may be relevant to prove a breach by the UCITS, management companies, investment companies or depositories'*.

14. Data relating to use of electronic communication means may convey a wide range of personal information. Furthermore, processing of traffic data conflicts with the secrecy of correspondence as expressed in Article 8 of the European Convention of Human Rights. In view of this, Directive 2002/58/EC[6] (the E-Privacy Directive) in Article 6 has established the principle that traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. According to Article 15(1) of this Directive, Member States may include derogations in national legislation for specific legitimate purposes, but they must be necessary, appropriate and proportionate within a democratic society to achieve these purposes.

15. The EDPS acknowledges that the aims pursued by the Commission in the proposed Directive are legitimate.[7] It is therefore essential in this perspective that the provision is clearly drafted in compliance with Articles 15(1) of the E-Privacy Directive and that a reference to this Article is added to the provision in the proposed Directive.

2.3.1. Definition of telephone and data traffic records

16. The EDPS welcomes the link in Article 98(2)(d) of the **proposed UCITS Directive** to the E-Privacy Directive and the definition of 'traffic data' in Article 2(1)(b) of the E-Privacy Directive. However, as this definition does not include a definition of 'existing telephone records', we recommend specifying the categories of telephone records which competent authorities can require. Such data must be adequate, relevant, and not excessive in relation to the purpose for which they are accessed and processed.

2.3.2. Requirement of a judicial authorisation

17. The EDPS welcomes that according to Article 98(3) of the **proposed UCITS Directive** the power to require existing telephone records and traffic data shall require prior judicial authorisation. However, he recommends introducing the requirement for competent authorities to request telephone records and traffic data by formal decision of a judicial authority specifying the legal basis and the purpose of the request and what information is required, the time-limit within which the information is to be provided as well as the right of the addressee to have the decision reviewed by a court.

---

[6] Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37.

[7] See, e.g., Joined Cases C-92/09 and C-93/09, V*olker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-92/09) v. Land Hessen*, nyp, para 74.

2.4. EIOPA database

18. Article 3(4) of the **proposed IM Directive** states that the European Insurance and Occupational Pensions Authority (EIOPA) shall maintain a central database listing all insurance and reinsurance intermediaries which intend to carry out cross-border business. This database shall be publicly available on the Internet. It is unclear whether this database will include the personal data of natural persons. The wording of the Article only speaks about insurance intermediaries and reinsurance intermediaries. However, according to Article 3 of the **proposed IM Directive** information regarding natural persons (employees) is to be collected by national competent authorities and may be exchanged between them and EIOPA. This implies that also such information could be included in the database.

19. The creation of central database which is publicly available on the Internet (and which includes personal data) constitutes processing of personal data in the sense of Regulation (EC) No 45/2001. The EDPS welcomes the introduction of a legal basis for the database in Article 3 of the **proposed IM Directive**. However, the specific access rights and management rights in relation to the processing operations are not explicitly clarified.

20. The EDPS recommends the Commission to clarify the modalities of the EIOPA Database by introducing more detailed provisions in the proposed Directive. Such provisions must comply with the requirements of Regulation (EC) No 45/2001. In particular, the provision establishing the database must (i) identify the purpose of the processing operations and establish which are the compatible uses; (ii) identify which entities (EIOPA, competent authorities and potentially others) will have access to which data stored in the database and will have the possibility to modify the data; (iii) ensure the right of access and appropriate information for all the data subjects whose personal data may be stored and exchanged (iv) define and limit the retention period for the personal data to the minimum necessary for the performance of such purpose.

21. In any event and notwithstanding the recommendation made in paragraph 19, the implementing measures to be adopted should specify in detail the functional and technical characteristics of the database and should be notified to the EDPS for consultation.

2.5. Publication of sanctions

22. Article 99b of the **proposed UCITS Directive**, Article 27 of the **proposed IM Directive** and Article 22 of the **proposed KID Regulation** state that every administrative measure and sanction imposed for breaches shall be published without undue delay, including at least information on the type and nature of the breach and the identity of persons responsible for it, unless such disclosure would seriously jeopardise the financial markets. Recital 23 of the **proposed UCITS Directive** and Recital 46 of the **proposed IM Directive** furthermore state that the publication of sanctions should strengthen the dissuasive effect on the public at large.

23. The EDPS welcomes the reference in recital 23 of the **proposed UCITS Directive** to the Charter of Fundamental Rights and in particular the right to protection of personal data when publishing sanctions. However, he is not convinced that the mandatory publication of sanctions, as it is currently formulated, meets the requirements of data protection as clarified by the Court of Justice in the *Schecke* ruling.[8] The EDPS takes the view that the purpose, necessity and proportionality of the measure are not sufficiently established and that, in any event, adequate safeguards should be provided.[9]

2.5.1. Necessity and proportionality of the publication

24. Article 27 of the **proposed IM Directive**, Article 99b of the **proposed UCITS Directive** and Article 22 of the **proposed KID Regulation** seem to be affected by the same shortcomings highlighted by the CJEU in the *Schecke* ruling. It should be borne in mind that for assessing the compliance with data protection requirements of a provision requiring public disclosure of personal information, it is of crucial importance to have a clear and well-defined purpose which the envisaged publication intends to serve. Only with a clear and well-defined purpose can it be assessed whether the publication of personal data involved is actually necessary and proportionate.[10]

25. After examining the proposals and the Explanatory memorandums, the EDPS is under the impression that the purpose, and consequently the necessity, of this measure are not clearly established. If the general purpose is increasing deterrence, it should be better explained in a Recital, in particular, why alternative, less privacy-intrusive measures, such as heavier financial penalties (or other sanctions not amounting to naming and shaming) are not sufficient.

26. Furthermore, the proposals do not seem to take into account less intrusive methods, such as publication to be decided on a case by case basis. In the EDPS' view, the possibility to assess the case in light of the specific circumstances is more proportionate and therefore a preferred option compared to mandatory publication in all cases[11].

2.5.2. The need for adequate safeguards

27. The **proposed IM Directive**, the **proposed UCITS Directive** and the **proposed KID Regulation** should all foresee adequate safeguards in order to ensure a fair balance between the different interests at stake when publishing administrative measures and sanctions imposed for breaches. Safeguards are necessary in relation to the right of the accused persons to challenge a decision before a court and the

[8] Joined Cases C-92/09 and C-93/09, *Schecke*, paras 56-64.
[9] See in this regard also EDPS Opinion of 9 October 2012 on the Amendment to the Commission proposal on the financing, management and monitoring of the common agricultural policy, available at http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Opinions.
[10] See in this regard also EDPS Opinion of 15 April 2011 on the Financial rules applicable to the annual budget of the Union, OJ C 215, 21.7.2011, p. 13–18.
[11] See EDPS Opinions of 10 February 2012 on credit rating agencies (para 48), markets in financial instruments (MIFID/MIFIR) (para 59) and market abuse (para 46), available at http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Opinions.

presumption of innocence. The EDPS recommends that the text of the relevant Articles in all proposals specify that competent authorities are obliged to take appropriate measures with regard to both the situations where the decision is subject to an appeal and where it is eventually annulled by a court. For example, the following measures could be considered by national authorities: to delay the publication until the appeal court has defined the case or to clearly indicate that the decision is still subject to appeal and that the individual is to be presumed innocent until the decision becomes final, to publish a rectification in cases where the decision is annulled by a court.

28. The proposals should ensure that the rights of the data subjects are respected in a proactive manner. The texts should provide that data subjects are informed beforehand of the fact that the decision sanctioning them will be published, and that they are granted the right to object under Article 14 of Directive 95/46/EC on compelling legitimate grounds.[12]

29. The EDPS assumes that in most of the Member States the publication will take place on the Internet. Internet publications raise specific issues and risks concerning in particular the need to ensure that the information is kept online for no longer than is necessary and that the data cannot be manipulated or altered. The use of external search engines also entails the risk that the information could be taken out of context and channelled through and outside the web in ways which cannot be easily controlled.

30. The EDPS recommends obliging Member States to ensure that personal data of the persons concerned are kept online only for a reasonable period of time, after which they are systematically deleted. Moreover, Member States should be required to ensure that adequate security measures and safeguards are put in place, especially to protect from the risks related to the use of external search engines. These measures and safeguards may consist for instance of the exclusion the data indexation by means of external search engines.

2.6. Reporting of breaches

31. Article 30 of the **proposed IM Directive** and Article 99d of the **proposed UCITS Directive** require Member States to put in place effective mechanisms for reporting breaches, also known as whistle-blowing schemes. We welcome the fact that both the **proposed IM Directive** and the **proposed UCITS Directive** contain specific safeguards concerning the protection of the persons reporting on the suspected violation and more in general the protection of personal data.

32. The EDPS would like to highlight, as in the case of other Opinions[13], the need to introduce a specific reference to the need to respect the confidentiality of whistleblowers' and informants' identity. The confidentiality of the identity of

[12] See EDPS Opinion of 10 April 2007 on the financing of the Common Agricultural Policy, OJ 2007 C134/1 OJ C 134, 16.6.2007, p. 1–3.
[13] See for instance, the Opinion on financial rules applicable to the annual budget of the Union of 15.04.2011, and the opinion on investigations conducted by OLAF of 01.06.2011, both available at http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Opinions.

whistleblowers should be guaranteed at all stages of the procedure, so long as this does not contravene national rules regulating judicial procedures. In particular, the identity may need to be disclosed in the context of further investigation or subsequent judicial proceedings instigated as a result of the enquiry (including if it has been established that they maliciously made false statements about him/her).[14] In view of the above, the EDPS recommends adding in Article 30(2)(c) of the **proposed IM Directive** and in Article 99d(1)(c) of the **proposed UCITS Directive** the following provision: 'the identity of these persons should be guaranteed at all stages of the procedure, unless its disclosure is required by national law in the context of further investigation or subsequent judicial proceedings'.

33. The EDPS is pleased to see that both Article 30 of the **proposed IM Directive** and Article 99d of the **proposed UCITS Directive** requires Member States to ensure the protection of personal data of both accused and the accusing person, in compliance with the principles laid down in Directive 95/46/EC. He suggests however removing 'the principles laid down in', to make the reference to the data protection Directive more comprehensive and binding.

3. CONCLUSIONS

34. The EDPS recommends:

- that references to this Opinion are included in the preambles of all proposals;

- inserting provisions in all proposals emphasising the full applicability of existing data protection legislation. The EDPS also suggests that the reference to Directive 95/46/EC be clarified by specifying that the provisions will apply in accordance with the national rules which implement Directive 95/46/EC;

- in the case of the proposed IM Directive, limiting competent authorities´ access to documents and information to specifically identified and serious violations of the proposed Directives and in cases where a reasonable suspicion (which should be supported by concrete initial evidence) exists that a breach has been committed;

- in the case of the proposed IM Directive, introducing a requirement for competent authorities to request documents and information by formal decision by a judicial authority, specifying the legal basis and the purpose of the request and what information is required, the time-limit within which the information is to be provided as well as the right of the addressee to have the decision reviewed by a court of law;

- in the case of the proposed UCITS Directive, introducing the requirement for competent authorities to request telephone records and traffic data by formal decision of the competent authority specifying the legal basis and the purpose of the request and what information is required, the time-limit within which

[14] See Opinion on financial rules applicable to the annual budget of the Union 15/04/2011, available at http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Opinions.

the information is to be provided as well as the right of the addressee to have the decision reviewed by a court;

- in the case of the proposed IM Directive, clarifying the modalities of the EIOPA database by introducing more detailed provisions in the proposed Regulations. Such provisions must comply with the requirements of Regulation (EC) No 45/2001. In particular, the provision establishing the database must (i) identify the purpose of the processing operations and establish which are the compatible uses; (ii) identify which entities (EIOPA, competent authorities, Commission) will have access to which data stored in the database and will have the possibility to modify the data; (iii) ensure the right of access and appropriate information for all the data subjects whose personal data may be stored and exchanged (iv) define and limit the retention period for the personal data to the minimum necessary for the performance of such purpose;

- assessing the necessity of the proposed system for the mandatory publication of sanctions in all proposals and verify whether the publication obligation does not go beyond what is necessary to achieve the public interest objective pursued and whether there are not less restrictive measures to attain the same objective. Subject to the outcome of this proportionality test, the publication obligation should in any event be supported by adequate safeguards to ensure respect of the presumption of innocence, the right of the persons concerned to object, the security/accuracy of the data and their deletion after an adequate period of time;

- with regard to the reporting of breaches in all proposals (i) inserting provisions in the proposed Directives saying that: 'the identity of these persons should be guaranteed at all stages of the procedure, unless its disclosure is required by national law in the context of further investigation or subsequent judicial proceedings'; (ii) adding a paragraph requiring Member States to put in place 'appropriate procedures to ensure the right of the accused person of defence and to be heard before the adoption of a decision concerning him and the right to seek effective judicial remedy against any decision or measure concerning him'; (iii) removing 'the principles laid down' from the provisions.

Done in Brussels, 23 November 2012

(**signed**)

Giovanni Buttarelli
Assistant European Data Protection Supervisor