**Opinion of the European Data Protection Supervisor**

**on the Commission proposal for a Regulation of the European Parliament and of the Council on improving securities settlement in the European Union and on central securities depositories (CSDs) and amending Directive 98/26/EC**

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 7 March 2012, the Commission adopted a proposal for a Regulation of the European Parliament and of the Council on improving securities settlement in the European Union and on central securities depositories (CSDs) and amending Directive 98/26/EC ('the proposal'). This proposal was sent to the EDPS for consultation on the same day.

2. The EDPS welcomes the fact that he is consulted by the Commission and recommends that references to this Opinion are included in the preambles of the proposed Regulation.

3. The proposal contains provisions which may in certain cases have data protection implications for the individuals concerned such as the investigative powers of the competent authorities, the exchange of information, the keeping of records, the outsourcing of activities, the publication of sanctions and the reporting of breaches.

[1] OJ L 281, 23.11.1995, p.31.
[2] OJ L 8, 12.01.2001, p. 1.

4. There are comparable provisions to the ones referred to in this Opinion in several pending and possible future proposals, such as those discussed in the EDPS Opinions on the European Venture Capital Funds and the European Social Entrepreneurship Funds[3], the legislative package on the revision of the banking legislation, credit rating agencies, markets in financial instruments (MIFID/MIFIR) and market abuse[4]. Therefore, the EDPS recommends reading this Opinion in close conjunction with his Opinions of 10 February 2012 on the above mentioned initiatives.

### 1.2. Objectives and scope of the proposal

5. Any trade in securities on or off a trading venue is followed by a post-trade flow of processes, leading to the settlement of the trade, which means the delivery of securities to the buyer against the delivery of cash to the seller. CSDs are key institutions that enable settlement by operating so-called securities settlement systems. They are the institutions which facilitate the transactions concluded on the markets. CSDs also ensure the initial recording and the central maintenance of securities accounts that record how many securities have been issued by whom and each change in the holding of those securities.

6. While generally safe and efficient within national borders, CSDs combine and communicate less safely across borders, which means that an investor faces higher risks and costs when making a cross-border investment. The absence of an efficient single internal market for settlements also raises other important concerns such as the limitation of security issuers' access to CSDs, different national licensing regimes and rules for CSDs across the EU, and limited competition between different national CSDs. These barriers result in a very fragmented market while cross-border transactions in Europe continue to increase and CSDs become increasingly interconnected.

7. The proposal aims at addressing these problems by introducing an obligation to represent all transferable securities in book entry form and to record these in CSDs before trading them on regulated venues, harmonising settlement periods and settlement discipline regimes across the EU, and introducing a common set of rules addressing the risks of CSDs' operations and services.

8. The proposal will complete the regulatory framework for securities market infrastructures, alongside the Directive 2004/39 on markets in financial instruments (MIFID) for trading venues, and the proposal for a regulation on derivative transactions (EMIR) for central counterparties.

## 2. ANALYSIS OF THE PROPOSAL

### 2.1 Applicability of data protection legislation

[3] EDPS Opinion of 14 June 2012, available at www.edps.europa.eu.
[4] EDPS opinions of 10 February 2012, available at www.edps.europa.eu.

9. The EDPS welcomes the attention specifically paid to data protection in the proposal. Recitals and provisions of the proposal mention the Charter of Fundamental Rights, Directive 95/46 and Regulation 45/2001[5]. In particular, recital 45 of the proposal states that Directive 95/46/EC governs the processing of personal data carried out in the Member Sates pursuant to the proposal and that Regulation 45/2001 governs the processing of personal data carried out by European Securities and Markets Authority ('ESMA') under the proposal. Furthermore, the EDPS notes that some provisions of the proposal explicitly refer to Directive 95/46/EC and/or Regulation 45/2001 or to 'relevant data protection legislation'[6].

10. The EDPS suggests rephrasing the provisions by emphasising the full applicability of existing data protection legislation in one general provision referring to Directive 95/46 as well as Regulation 45/2001. Moreover, the reference to Directive 95/46/EC should be clarified by specifying that the provisions will apply in accordance with the national rules which implement Directive 95/46/EC. The EDPS furthermore recommends including this type of overarching provision in a substantive provision of the proposal.

### 2.2. Investigatory powers of the competent authorities

11. Article 10.3 of the proposal states that competent authorities shall have all the supervisory and investigatory powers necessary for the exercise of their functions. The provision clearly implies that the proposal will lead to exchanges of personal data (e.g. on members of the management boards of CSDs and/or credit institutions as well as any other persons who control their business operations). It seems likely -or at least it cannot be excluded- that documents and information requested will include personal data in the meaning of Directive 95/46/EC and Regulation (EC) 45/2001. In this case, it should be ensured that the conditions for fair and lawful processing of personal data as laid down in the Directive and the Regulation are fully respected.

12. The EDPS acknowledges that the aims pursued by the Commission in the proposal 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 members of the management boards of CSDs and/or credit institutions as well as any other person who controls their business operations or is responsible of a breach of the proposal, 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 which they can be used. Furthermore, adequate safeguards should be provided against the risk of abuse.

[5] i.e. recitals 42, 45 and 46 as well as Articles 23, 28 and 62 of the proposal.
[6] see Articles 23.7, last paragraph, Article 28.1.(i) , 60.2 last paragraph and 62.2 (c).

13. 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 basic act. Article 10.3 of the proposal 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 proposal and in cases where a reasonable suspicion (which should be supported by concrete initial evidence) exists that a breach has been committed[7].

14. The EDPS recommends introducing 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 Exchange of information

*2.3.1 Cooperation between competent authorities and with ESMA*

15. The proposal contains provisions requiring competent authorities to closely cooperate. In a general way, Article 12 of the proposal foresees that competent authorities shall cooperate closely between them and with ESMA for the application of the proposal. Article 59.3 in particular states that in the exercise of their sanctioning powers, competent authorities shall cooperate closely to ensure that the administrative sanctions and measures produce the desired results of the proposal and shall coordinate their action in order to avoid possible duplication and overlap when applying administrative sanctions and measures to cross border cases.

16. In some cases, this cooperation will undoubtedly involve the exchange of information related to identified or identifiable individuals, for example the persons working within the management bodies of CSDs. Such exchange will therefore constitute a processing of personal data under Article 2 (b) of Directive 95/46/Ec and Article 2 (b) of Regulation (EC) No 45/2001.

17. The EDPS recognises the importance of ensuring cooperation with a view to an effective and consistent application of the proposal, including efficient supervision of CSDs. However, as far as this cooperation will involve the processing of personal data, these provisions are too vague and do not fulfil the basic legal requirements.

18. A basic requirement of data protection law is that information must be processed for specified, explicit and legitimate purposes and that it may not be further processed in a way incompatible with those purposes. The data used to achieve the

[7] See EDPS Opinions of 10 February 2012 on credit rating agencies (paragraph 35) and market abuse (paragraph 33), and opinion of 14 June 2012 on European Venture capital funds and on European Social entrepreneurship funds (paragraph 23), available at www.edps.europa.eu.

purposes should furthermore be adequate, relevant and not excessive in relation to these purposes[8].

19. The proposal neither specifies the purposes of exchange of information between competent authorities when cooperating with each other nor the kind of data that will be exchanged, including any personal data of identified or identifiable persons.

20. Furthermore, Article 6 of Directive 95/46/EC and Article 4 of Regulation (EC) No 45/2001 require that personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The EDPS notes that the proposal does not lay down any concrete time limit for the retention of the personal data potentially processed under the proposal. This is in contradiction with the requirements set out by data protection legislation, and may at least result in undue diversity in national implementation or practice.

21. On the basis of the foregoing, the EDPS urges the legislator to specify the purposes for which personal data can be processed by national competent authorities and ESMA, to specify the kind of personal information that can be processed under the proposal and fix a precise, necessary and proportionate data retention period for the above processing.

*2.3.2Exchange of information with third countries*

22. The EPDS notes the reference to Directive 95/46/EC and the Regulation (EC) 45/2001 in Article 23.7 of the proposal regarding the transfer of personal data by a Member State or by ESMA under a cooperation agreement.

23. However, in view of the risks concerned in such transfers the EDPS recommends adding specific safeguards such as for example a case-by-case assessment and the existence of an adequate level of protection of personal data in the third country receiving the personal data.

24. A good example of such a provision containing appropriate safeguards can be found in Article 23 of the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation[9].

---

[8] See Article 6 of Directive 95/46/EC and Article 4 of Regulation (EC) No 45/2001.

[9] Article 23 of the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation COM (2011) 651 states as follows:

'1. The competent authority of a Member State may transfer personal data to a third country provided the requirements of Directive 95/46/EC, particularly of Articles 25 or 26, are fulfilled and only on a case-by-case basis. The competent authority of the Member State shall ensure that the transfer is necessary for the purpose of this Regulation. The competent authority shall ensure that the third country does not transfer the data to another third country unless it is given express written authorisation and complies with the conditions specified by the competent authority of the Member State. Personal data may only be transferred to a third country which provides an adequate level of protection of personal data'.

2. The competent authority of a Member State shall only disclose information received from a competent authority of another Member State to a competent authority of a third country where the competent authority of the Member State concerned has obtained express agreement of the competent

## 2.4 Record keeping

25. Article 27 establishes that CSDs shall maintain '*for a period of at least five years*' all records on services and activity provided in order to enable the competent authority to monitor compliance with the proposal.

26. Article 6.1 (e) of Directive 95/46/EC requires that personal data should not be kept longer than is necessary for which the data were collected or for which they are further processed. In order to comply with this obligation, the EDPS suggests replacing the minimum retention period of 5 years with a maximum retention period when records contain personal data. The chosen period should be necessary and proportionate for the purpose for which data have been collected.

## 2.5 Outsourcing of services or activities

27. Under Article 28 of the proposal, a CSD outsourcing services or activities to a third party shall remain fully responsible for discharging all of its obligations under the proposal and shall ensure - among other things - that the service provider meets the standards set down by the relevant data protection legislation which would apply if the service provider were established in the Union.

28. The EDPS notes the reference to data protection legislation and the obligation to lay down data protection standards in a contract between the parties concerned. However, he considers that the use of the criterion of the establishment of the service provider is not relevant in order to determine which data protection legislation that is applicable.

29. Under Article 4 of Directive 95/46, applicable data protection legislation is determined according to the place of establishment of the controller. Article 2 (d) (e) of the Directive 95/46 defines the controller as 'a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data' while the processor is 'a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'.

30. Taking into account the full responsibility remaining on the CSD, this latter would be the controller and the service provider would most probably be considered as a processor. It follows that the applicable law to the processing of personal data by the processor would be the one applicable to the controller with some exceptions related to security requirements (Article 17.3 of Directive 95/46).

31. Therefore, the EDPS recommends rephrasing article 28.1 (i) as follows: 'The CSD ensures that the service provider provides its services in full compliance with the national rules, applicable to the CSD, implementing Directive 95/46/EC on the

---

authority which transmitted the information and, where applicable, the information is disclosed solely for the purposes for which that competent authority gave its agreement.
3. Where a cooperation agreement provides for the exchange of personal data, it shall comply with Directive 95/46/EC.'

protection of individuals with regard to the processing of personal data and on the free movement of such data. The CSD is responsible (...)'.

## 2.6 Mandatory publication of sanctions

*2.6.1 Necessity and proportionality*

32. One of the proposal's objectives is to reinforce and approximate Member States' legal framework concerning administrative sanctions and measures. The proposal provides for the power of the competent authorities to impose sanctions, not only on CSD's and designated credit institutions, but also on the members of their management bodies and any other persons who effectively control their business as well as to any other legal or natural person who is held responsible for a breach of the proposal.

33. Article 60.4 of the proposal obliges competent authorities to publish every administrative sanction or measure imposed for a breach of the proposal including information on the identity of the persons responsible for the breach unless such disclosure would seriously jeopardise the stability of financial markets or cause a disproportionate damage to the parties involved. In the latter case, competent authorities shall publish the measures and sanctions on an anonymous basis.

34. The EDPS welcomes that both Article 60.2 and recital 42 of the proposal state that the publication shall comply with fundamental rights as laid down in the Charter of Fundamental rights of the European Union, in particular the right to respect of private and family life and the right to the protection of personal data. However, the EDPS considers that the mandatory publication of sanctions, as it is currently formulated, does not meet the requirements of data protection law as clarified by the Court of Justice in the *Schecke*[10] ruling. He takes the view that the purpose, necessity and proportionality of the measure are not sufficiently established and that, in any event, adequate safeguards for the rights of the individuals should have been foreseen.

35. Article 60.4 of the proposal seems to be affected by the same shortcomings highlighted by the ECJ in the *Schecke* judgment. It should be borne in mind that when 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.[11]

36. Neither the proposal, the explanatory memorandum nor the impact assessment clearly establish the purpose, and consequently the necessity, of this measure. If the general purpose is increasing deterrence, the EDPS suggest to better explain in a recital, in particular, why alternative measures not affecting privacy, such as

[10] Joined Cases C-92/09 and C-93/09, *Schecke*, paragraphs 56-64.

[11] See also in this regard 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.

heavier financial penalties (or other sanctions not amounting to naming and shaming) are not sufficient.

37. Furthermore, the proposal does not seem to take into account less intrusive methods of naming and shaming, such as considering the need for publication on a case by case basis. In particular, this would seem to be *prima facie* a more proportionate solution, especially if one considers that publication is itself a sanction under Article 60.2 and that Article 61 provides that when determining the type and level of sanctions the competent authorities should take account of the relevant circumstances (i.e. case by case assessment), such as the gravity of the breach, the degree of personal responsibility, the size and the financial strength of the responsible person, losses for third parties, etc. The mandatory publication of sanctions in all cases under Article 60.4 is inconsistent with the sanctioning regime set out in Articles 60 and 61.

*2.6.2 The need for adequate safeguards*

38. The proposal should foresee adequate safeguards in order to ensure a fair balance between the different interests at stake. Firstly, safeguards are necessary in relation to the right of the accused persons to challenge a decision before a court and the presumption of innocence. The EDPS recommends specifying in the text of Article 60.4 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.[12]

39. Secondly, the proposal should ensure that the rights of the data subjects are respected in a proactive manner. The EDPS appreciates the fact that the proposal foresees the possibility to exclude the publication in cases where it would cause disproportionate damage. However, a proactive approach should imply 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.

40. Thirdly, while the proposal does not specify the medium on which the information should be published, in practice, it is imaginable 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[13].

[12] For example, the following measures could be considered by national authorities: to delay the publication until the appeal is rejected 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.

[13] See in this regard the document published by the Italian DPA, "Personal Data As Also Contained in Records and Documents by Public Administrative Bodies: Guidelines for Their Processing by Public Bodies in Connection with Web-Based Communication and Dissemination", available on the website of the Italian DPA, http://www.garanteprivacy.it/garante/doc.jsp?ID=1803707.

41. In view of the above, it is necessary to oblige 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[14]. 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[15].

42. Finally, under Article 7.2 of the proposal, CSDs and other market infrastructures are required to put in place procedures enabling them to take appropriate measures to suspend any participant that systematically causes settlement fails and to disclose its identity to the public only after giving that participant the opportunity to submit observations before such a decision is taken. The EDPS welcomes the conditions of 'systematic' failures and the obligation to give the data subject the opportunity to submit its observations beforehand. However the EDPS considers that more guidance about the wording 'systematically' should be provided, for instance in a recital. Furthermore, he highlights that the above mentioned safeguards to ensure the right of the accused persons to challenge a decision before a court, the security of the data published on the Internet and their deletion after an adequate period of time also apply to the public disclosure of the identity of person responsible of settlement fails.

*2.6.3 Conclusion*

43. The EDPS is of the view that the provision on the mandatory publication of sanctions -as it is currently formulated- does not comply with the fundamental right to privacy and data protection. The legislator should carefully assess the necessity of the proposed system and verify whether the publication obligation goes beyond what is necessary to achieve the public interest objective pursued and whether there are 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 appropriate period of time.

## 2.7 Reporting of breaches

44. Article 62 of the proposal requires Member States to put in place effective mechanisms to encourage reporting of breaches, also known as whistle-blowing schemes. The EDPS welcomes the fact that the proposal contains specific safeguards concerning the protection of the persons reporting on the suspected violation and more in general the protection of personal data. Nonetheless, he would like to draw the attention to the following additional points.

[14] These concerns are also linked to the more general right to be forgotten, the inclusion of which in the new legislative framework for the protection of personal data is under discussion

[15] These measures and safeguards may consist for instance of the exclusion of the data indexation by means of external search engines.

45. The EDPS highlights, as in the case of other Opinions[16], 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 whistleblowers should be guaranteed at all stages of the procedure, so long as this is not in breach of national rules on judicial procedures. In particular, the identity may need to be disclosed in the context of further investigations 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).[17] In view of the above, the EDPS recommends adding in Article 62.2(b) 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*'.

46. The EDPS is pleased to see that Article 62.2(c) 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.

47. As for the practical implementation of these measures, the EDPS would like to recall the recommendations made by the Article 29 Working Party in its 2006 Opinion on whistle-blowing.[18]

## 3. CONCLUSIONS

48. The EDPS welcomes the attention specifically paid to data protection in the proposal.

49. The EDPS makes the following recommendations:
    - Include references to this Opinion in the preamble of the proposal;
    - Rephrase provisions emphasising the full applicability of existing data protection legislation in one general provision referring to Directive 95/46/EC as well as regulation 45/2001 and clarify the reference to Directive 95/46/EC by specifying that the provisions will apply in accordance with the national rules which implement Directive 95/46/EC. The EDPS furthermore recommends including this type of overarching provision in a substantive provision of the proposal;
    - Limit competent authorities' access to documents and information to specifically identified an serious violations of the proposal and in cases where

[16] 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 www.edps.europa.eu .

[17] See opinion on financial rules applicable to the annual budget of the Union 15/04/2011, available at www.edps.europa.eu

[18] Article 29 Working Party: Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

a reasonable suspicion (which should be supported by concrete initial evidence) exists that a breach has been committed;

- Introduce a 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 of law;
- Specify the kind of personal information that can be processed and transferred under the proposal, define the purposes for which personal data can be processed and transferred by competent authorities and fix a proportionate data retention period for the above processing or at least introduce precise criteria for its establishment;
- In view of the risks concerned regarding transfers of data to third countries, add in Article 23.7 specific safeguards such as for example a case-by-case assessment and the existence of an adequate level of protection of personal data in the third country receiving the personal data;
- Replace the minimum retention period of 5 years in Article 27 of the proposal with a maximum retention period when records contain personal data. The chosen period should be necessary and proportionate for the prupose for which data are processed;
- Rephrase article 28.1 (i) as follows: 'The CSD ensures that the service provider provides its services in full compliance with the national rules, applicable to the CSD, implementing Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The CSD is responsible (...)';
- Add in Article 62.2. (b) a provision 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' and remove in Article 62.2 (c) 'the principles laid down in';
- In light of the doubts expressed in the present Opinion, assess the necessity and proportionality of the proposed system of mandatory publication of sanctions. Subject to the outcome of the necessity and proportionality test, in any event provide for 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.

Done in Brussels, 09 July 2012

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor