Opinion of the European Data Protection Supervisor

on the proposal for a Regulation of the European Parliament and of the Council on structural measures improving the resilience of EU credit institutions and on the proposal for a Regulation of the European Parliament and of the Council on the reporting and transparency of securities financing transactions

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. On 29 January 2014, the Commission adopted two proposals on the regulation of the European banking system: a proposal for a Regulation of the European Parliament and of the Council on structural measures improving the resilience of EU credit institutions ('the proposal on credit institution resilience'),[3] and a proposal for a Regulation of the European Parliament and of the Council on the reporting and transparency of securities financing transactions ('the proposal on transparency of SFTs').[4] The proposals form part of the wide-ranging overhaul of financial regulation and supervision which the EU has undertaken since the onset of the financial crisis. They set out rules for preventing the biggest and most complex banks from engaging in proprietary trading, they would give supervisors the power to require those banks to separate certain potentially risky trading activities from their deposit-taking business and would increase transparency of certain transactions in the shadow banking sector. They are accompanied by a single impact assessment and were adopted together as a package.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2014) 43 final.
[4] COM(2014) 40 final.

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

2. Each proposal involves the processing of personal data including the publication of details about individuals who have been subject to sanctions for breaches of the proposed rules. It is regrettable therefore that the EDPS was not consulted prior to the adoption of the proposals, as required by Article 28(2) of Regulation (EC) No 45/2001[5]. The EDPS recognises the legitimate public policy goal behind these proposals, and welcomes the fact that some data protection safeguards are envisaged. However, there are several areas where greater attention to the rights of the individual is required.

2. GENERAL COMMENTS

3. Both proposals refer to the protection of personal data under EU law. Recital 33 of the proposal on credit institution resilience recalls that 'the disclosure of information relating to prudential supervision and for the application of this Regulation' may involve personal data which should '*be retained by the competent authority only for the period necessary in accordance with the applicable data protection rules*'. Recital 25 of the proposal on transparency of SFTs states, '*This Regulation respects the fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union, in particular the right to the protection of personal data, the right to respect private and family life (…). This Regulation must be applied according to these rights and principles*'.

4. Neither proposal includes a correct reference to the applicable data protection rules. Recital 33 of the proposal on credit institution resilience refers to Regulation (EC) No 45/2001, which addresses personal data processing by EU institutions and bodies. Given that, as indicated in Article 31 and Recitals 32 and 42 of the proposal, some personal information, notably on sanctions, may be provided by competent authorities to an EU body, the European Banking Authority (EBA), Regulation 45/2001 is indeed relevant. However, 'competent authority', under Article 5(7) of this proposal, is defined in another instrument, Regulation (EU) No 575/2013,[6] as '*a public authority or body officially recognised by national law, which is empowered by national law to supervise institutions as part of the supervisory system in operation in the Member State concerned*'. Such national supervisory bodies are subject to rules and obligations on data protection contained not in Regulation 45/2001 but rather in national provisions implementing Directive 95/46/EC.

5. Meanwhile, the proposal on transparency of SFTs envisages data processing by various physical or legal persons (including managers of alternative investment funds, trade repositories and national competent authorities) to which Directive 95/46/EC applies, and by the European Securities and Markets Authority (ESMA), another EU body, to which Regulation 45/2011 applies. However, the proposal contains no reference to applicable data protection law.

6. A correct and consistent reference to applicable law, citing both national provisions implementing Directive 95/46/EC and Regulation 45/2001, should therefore be included in both proposed instruments.

[5] See EDPS policy paper: "The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience", 4 June 2014, available on the EDPS website at www.edps.europa.eu.

[6] Article 4(1) point 40 of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.

3. SPECIFIC COMMENTS

3.1. Transparency of SFTs

7. Under Article 4 of the proposal on transparency of SFTs, counterparties to SFTs must keep a record of any transaction that '*they have concluded, modified or terminated for at least ten years following the termination of the transaction' and must report details of these transactions to a registered trade repository. These records and reports on SFTs will include 'at least: the parties to the SFT and, where different, the beneficiary of the rights and obligations arising from it*'.

8. Neither the proposal nor the impact assessment explains why a minimum retention period of ten years for information which includes personal data was considered proportionate and appropriate. The EDPS recommends that this provision should stipulate an appropriate maximum retention term for personal information. As it is envisaged that the ESMA will develop draft regulatory standards specifying the details of the SFT to be included, the EDPS will be pleased to provide advice on the inclusion of appropriate limitations and safeguards in due course.

3.2. Confidentiality and professional secrecy

9. Article 4(4) of the proposal on transparency of SFTs requires trade repositories (defined under Article 3(1) as '*the legal person that centrally collects and maintains the records of security financing transactions'*) and the ESMA to observe confidentiality, integrity and protection with respect to SFTs information. Article 18(1) states, '*The obligation of professional secrecy shall apply to all persons who work or have worked for the entities referred in Article 12(2) and the competent authorities referred to in Article 16, for ESMA, EBA and EIOPA or for auditors and experts instructed by the competent authorities or ESMA, EBA and EIOPA. No confidential information that those persons receive in the course of their duties shall be divulged to any person or authority except in summary or aggregate form such that an individual counterparty, trade repository or any other person cannot be identified, without prejudice to cases covered by criminal or tax law or to this Regulation.*'[7] .

10. Sub-articles 18(2) and 18(3), however, outline a derogation from this obligation:

> "18(2) *Without prejudice to cases covered by criminal or tax law, the competent authorities, ESMA, EBA, EIOPA, bodies or natural or legal persons other than competent authorities which receive confidential information pursuant to this Regulation may use it only in the performance of their duties and for the exercise of their functions, in the case of the competent authorities, within the scope of this Regulation or, in the case of other authorities, bodies or natural or legal persons, for the purpose for which such information was provided to them or in the context of administrative or judicial proceedings specifically relating to the exercise of those functions, or both. Where ESMA, EBA, EIOPA the competent authority or another authority, body or person communicating information consents thereto, the authority receiving the information may use it for other non-commercial purposes*.

[7] These 'entities' referred to in Article 12(2) of the proposal on transparency of SFTs include various national authorities and EU bodies, and also 'relevant authorities of a third country which have entered into an agreement with the EU or with the ESMA' (Article 83(1) of Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, OJ L 201, 27.7.2012, p.52).

8(3) Any *confidential information received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraphs 1 and 2. However, those conditions shall not prevent ESMA, EBA, EIOPA, the competent authorities or the relevant central banks from exchanging or transmitting confidential information in accordance with this Regulation and with other legislation applicable to investment firms, credit institutions, pension funds, insurance and reinsurance intermediaries, insurance undertakings, regulated markets or market operators or otherwise with the consent of the competent authority or other authority or body or natural or legal person that communicated the information*.".

11. These derogations in sub-articles 18(2) and 18(3) appear convoluted and vague as such could pose risks to relevant data subjects. The provisions do not indicate clearly the extent to which 'information' and 'confidential' information referred to in this article include personal data, although it is fair to assume that some personal information, such as the identity of employees or clients of a credit institution, would be involved. Furthermore, the list of individuals or organisations between whom information exchange is envisaged is very broad, goes beyond the competent authorities and EU bodies primarily concerned by the proposal, and does not address whether or not these other individuals or organisations need to obtain this information. The provisions do not indicate either whether the transfer of personal data to a third country, which is subject to specific restrictions under Articles 25 and 26 of Directive 95/46/EC, could take place under this derogation. It is unclear who would be legally responsible for its processing as data controller under Article 2(d) of Directive 95/46/EC and Article 2(d) of Regulation 45/2001.

12. We note that 'information' could be exchanged or 'transmitted' for purposes other than were originally processed. Insofar as this information includes personal data, the further use of the personal data for other purposes must respect the principle of purpose limitation set forth in Article 6(1)(b) of Directive 95/46/EC and Article 4(1)(b) of Regulation 45/2001. According to the principle of purpose limitation, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

13. The EDPS recommends that Articles 18(2) and 18(3) are reformulated to clarify whether or not personal data are within the scope of this derogation and, if so, to state that those data may only be processed for compatible purposes and in accordance with applicable data protection rules. It should also be clarified whether personal data transfers to third countries are envisaged and if so, that such transfers may only take place in accordance with national provisions implementing Articles 25 and 26 of Directive 95/46/EC.

3.3. Administrative sanctions and measures

14. Case law from the CJEU has established[8] that any publication obligation which entails the processing of personal data must be based on a balanced assessment of the public interest objective pursued and the need to respect individuals' rights to privacy and the protection of personal data, and on an assessment of whether there are less restrictive measures to attain the same objective. Such an 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 and accuracy of the data and

[8] Joined Cases C-92/09 and C-93/09, *Schecke*, judgment of 9 November 2010, paragraphs 56-64.

their deletion after an appropriate period of time[9]. Moreover, data relating to offences, criminal convictions or security measures benefit of a specific protection under Article 8(5) of Directive 95/46/EC and may only be processed under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national law.

15. Article 28(4)(c) of the proposal on credit institution resilience and Article 20(4)(c) of the proposal on transparency of SFTs each provide that, in the event of breaches of the proposed rules, competent authorities should have the power to issue 'a public warning indicating the person responsible and the nature of the breach'. As this could interfere with the individual's right to protection of personal data, such a power should not be exercised automatically but rather only on a case by case basis and where appropriate and proportionate.

16. In relation to whistleblowing, both proposals (Article 30(2)(c) of the proposal on credit institution resilience and Article 22(2)(c) of the proposal on transparency of SFTs) correctly provide for the protection of personal data both of the person who reports the breach and the natural person who allegedly committed the breach. Similarly, it is welcome that the proposals (Article 31 of the proposal on credit institution resilience and Article 23 of the proposal on transparency of SFTs) provide for competent authorities to communicate information to ESMA on any criminal sanctions for breaches only in an anonymous and aggregated format. These provisions envisage development by the EBA and ESMA respectively of implementing technical standards to determine procedures and forms for exchange of information; the EDPS would be pleased to advise on how to ensure adequate data protection safeguards as part of this process.

17. Article 32 of the proposal on credit institution resilience and Article 24 of the proposal on transparency of SFTs provide for the publication on the Internet of information on sanctions which would include the type and nature of the breach and the identity of the person subject to the decision. This provision includes a number of appropriate safeguards protecting the rights to privacy and to data protection of the individuals concerned, including a number of alternatives where the competent authority considers on a case-by-case basis that publication of the identity of a legal person would be disproportionate. As the CJEU has recently ruled,[10] publication on the Internet raises specific risks for privacy and data protection and the institution or body responsible for the processing is bound to ensure that the data are adequate, relevant and not excessive in relation to the purposes for which they are processed. In view of the particular intrusiveness of the publication of personal data on the internet in individuals' rights to privacy and data protection, the EDPS recommends reinforcing the safeguards by making it a requirement for all authorities to consider separately each case and its particular circumstances and to be guided by the principles of necessity and proportionality prior to any decision to publish the identity of the person subject to a sanction.

18. These provisions also would require competent authorities to ensure information on sanctions decisions to be accessible on the website for a minimum period of five years, while personal data in those decisions '*should be kept on the website of the competent authority for the period which is necessary in accordance with the applicable data*

[9] See detailed recommendations in EDPS Opinions of 10 February 2012 on proposals on markets in financial instruments and on proposals on criminal sanctions for insider dealing and market manipulation, available on the Consultation section of the EDPS website at www.edps.europa.eu.
[10] Case C-131/12 *Google Spain*, judgment of 13 May 2014, paragraph 93.

protection rules.' The CJEU held[11] in that respect that even initially lawful processing of accurate data may, in the course of time, become incompatible with Directive 95/46/EC where, having regard to all the circumstances of the case, the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed. A maximum retention period for personal data would therefore be more appropriate.

4. CONCLUSION

19. The EDPS is pleased to note that some account has been taken of data protection aspects in the proposals, and recommends a fuller integration of respect for the rights to privacy and the protection of personal data by means of the following changes:

    a) the inclusion of a general provision for all processing of personal data pursuant to the proposed regulations to be subject to the rules laid down in Directive 95/46/EC and Regulation 45/2001;

    b) an appropriate maximum term in the proposal on transparency of SFTs for personal information to be retained by counterparties to an SFT;

    c) regarding the provisions derogating from the obligation for confidentiality and professional secrecy in the proposal on transparency of SFTs, (i) clarification on whether or not personal data are within the scope of this derogation, and if so, the inclusion a statement that those data may only be processed for compatible purposes and in accordance with applicable data protection rules; (ii) clarification whether personal data transfers to third countries are envisaged and if so, add a statement that such transfer may only take place in accordance with national provisions implementing Articles 25 and 26 of Directive 95/46/EC;

    d) clarifying that the power to issue a public warning about identified individuals should not be exercised automatically but rather only on a case by case basis and where appropriate and proportionate;

    e) regarding the provisions for publication of sanctions, (i) the inclusion of a requirement in both regulations to consider separately each case and its particular circumstances on the basis of necessity and proportionality prior to any decision to publish the identity of the person subject to a sanction, and (ii) specifying a maximum retention period for personal data published as part of information on sanction decisions on competent authorities websites.

Done in Brussels, 11 July 2014

(**signed**)

Giovanni BUTTARELLI

[11] Case C-131/12 *Google Spain*, judgment of 13 May 2014, paragraph 93.