Guidelines on data protection in EU financial services regulation

Contents

Table of Contents

10-point checklist for analysing data protection and privacy

This list of questions, developed for policymakers and legislators in the area of financial services regulation, is a summary of the 10-step methodology which the EDPS recommends in section 3 of these guidelines.

1. *Is personal information, and in particular sensitive data, likely to be processed - in other words collected, analysed or used in some way? And if so, what information?*
2. *Would the processing of personal information interfere with the individual's right to respect for private and family life, home and communications?*
3. *Is there a clear purpose for processing the personal information? Will the information be processed further for other purposes and, if so, are these compatible with the original purpose?*
4. *Is there a legal basis for processing the personal data?*
5. *On the basis of the impact assessment, what is a proportionate maximum period for which personal information will be stored or kept on file?*
6. *Who in the EU needs access to the data for the stated purposes?*
7. *Is it necessary to transfer personal information to third countries? What is the legal basis?*
8. *Are there sufficient guarantees that data subjects can exercise their rights to access and correction, as well as other relevant rights?*
9. *What technical and organisational security measures are appropriate, especially where large or complex databases and IT systems are envisaged?*
10. *Can you demonstrate to an independent supervisory authority that the processing of personal data complies with data protection law?*

1. Data protection and financial services regulation

Why data protection is relevant for financial services regulation

1. The objective of financial services regulation in the EU is to ensure financial stability, an efficient single market for financial services and market integrity and confidence.[1] Measures in this area include banking capital requirements and rules on the derivatives markets, insurance, securities and investment funds, financial markets infrastructure, retail financial services and payment systems. Since the onset of the financial crisis in 2008 over 40 new laws have been proposed, many flowing from commitments made by the G20, most of which have been adopted. This extensive body of regulation involves close supervision of the behaviour of traders and investors in the financial markets, through greater powers for supervisors, transparency for all market participants, control of risk-taking and protection of consumers, investors and taxpayers against risky activities. Other measures, like the directives on money laundering and terrorist financing, and the regulation on financial rules applicable to the EU's annual budget, impose obligations on financial institutions.

2. Most of these measures concern the actions of legal persons. Many however, like those covering surveillance, record keeping and reporting, information exchange, powers of competent authorities and sanctions for violation of the applicable rules, require the processing of personal information, that is, data relating to directly or indirectly identifiable natural persons. Some measures potentially interfere also with the right to privacy.

3. Respect for the rights of individuals to privacy and data protection, as enshrined in the Charter of Fundamental Rights of the European Union ('the Charter'), is an essential condition for the validity of EU legislation.[2] Data protection rules and principles flowing, in particular, from Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the European Union (TFEU), are meant to facilitate the free movement of information within the internal market, as well as to protect the rights and interests of the individual. Correct application of data protection rules and principles should therefore contribute to the efficiency and quality of policymaking and legislation in the area of financial services regulation.

The purpose of these guidelines

4. The EDPS aims to ensure that the EU institutions and bodies are aware of data protection requirements and integrate high standards of data protection in all new legislation[3]. This document is targeted at policymakers and legislators in the area of financial services regulation. It is part of the 'policy toolkit' for the EU institutions which the EDPS is developing to facilitate policymaking which respects the fundamental rights and freedoms in the Charter and in particular the rights to privacy and to the protection of personal data.[4] Drawing from the policy paper published earlier this year, 'The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience', from advice offered by the EDPS over recent years, both as an advisor to the EU institutions on policy and legislation and as the

[1] COM(2014) 279 final, A Reformed financial sector for Europe.
[2] See Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, judgment of the CJEU of 8 April 2014.
[3] EDPS Strategy 2013-2014, 'Towards excellence in data protection', 22 January 2013.
[4] EDPS Policy Paper, 'The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience', 4 June 2014.

relevant supervisory authority, and from insights gained during a seminar hosted by DG MARKT in February 2014, it addresses the types of measures in financial services regulation where data protection is most likely to be relevant.

How to use these guidelines

5. The guidelines are structured as follows:

   - section two summarises the nature of the rights to privacy and to the protection of personal data within the EU's fundamental rights framework;
   - section three describes the analytical steps required for assessing data protection aspects of proposed measures;[5]
   - section four illustrates the application of data protection rules by way of specific measures in current or proposed financial services regulation;
   - section five outlines how the EDPS proposes to continue to work with policy- and lawmakers in the area of financial services regulation in the future.

6. These guidelines are intended as a practical, step-by-step companion to the policymaking process which can accompany the Commission's guidelines on impact assessment. They will be kept under review and the EDPS would welcome feedback and comments on their usefulness.

7. The Commission's proposal for a General Data Protection Regulation provides for public authorities and bodies to carry out 'data protection impact assessments' ('if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question').[6] The EDPS accordingly recommends that policymakers refer to the latest international standards for privacy impact assessments, such as ISO standard 22307:2008 Financial Services - Privacy Impact Assessment.

2. Overview of the EU's data protection legal framework

The Charter of Fundamental Rights of the EU

8. An EU measure is only lawful if it complies with the Charter.[7] The rights to respect for private and family life and to the protection of personal data under Articles 7 and 8 of the Charter are closely related and even partly overlapping.[8] Data protection as a right has its roots in the right to privacy as articulated, in particular, in Article 8 of the European Convention on Human Rights (ECHR). Both rights are recent expressions of the universal, ethical principles of dignity and autonomy, and the right of every individual to develop his/her personality and to have a fair say on matters with a direct

[5] See EDPS Policy Paper, Section 4.3.
[6] Recital 73 and Article 33 of the Proposal for a General Data Protection Regulation, COM(2012) 11 final, 25.01.2012.
[7] Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof* and *Österreichischer Rundfunk*, judgment of the CJEU of 20 May 2003.
[8] Joined Cases C-92/09 and C-93/09, *Schecke* and *Eifert*, judgment of the CJEU of 9 November 2010, paragraphs 47-52.

impact on him/her. The common underlying intention is to prevent undue interference and to give individuals sufficient control over their own lives.

9. Under the Charter, which since the entry into force of the Lisbon Treaty now has the value of primary law in the EU, the rights to privacy and to data protection are separate rights. There is, therefore, no need in all cases, in the analysis of the right to data protection, to refer back to the earlier right to privacy. Relevant case law indicates the challenge for the Court of Justice of the European Union (CJEU) of developing a clear and consistent approach to enforcing these separate Charter rights and freedoms, whose differences are of considerable importance to the protection of the individual.

The right to privacy

10. The right to respect for private and family life, home and communications, as laid down in Article 7 of the Charter, protects the individual primarily against interference with his/her privacy.[9] It is a classic 'negative' right protecting the individual primarily against interference by the State. Any interference must, according to Article 52(1) of the Charter, be provided for by law, respect the essence of the right, and be justifiable, 'subject to the principle of proportionality', on grounds that it is 'necessary and genuinely meets the objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.' Furthermore, the concept of private life has evolved in case law to cover not only intimate situations but also individuals when engaged in purely personal, household or social activities.[10]

11. In practice, this requires that measures interfering with the right to privacy must be predicated on a proper, empirical assessment of other, less intrusive means.[11] The CJEU held that it would be a disproportionate interference with private life to publish the information on salaries of senior staff of semi-state undertakings.[12] In another ruling the court annulled an EU measure requiring publication of information on beneficiaries of agricultural aid on a website, having found no evidence that legislator had considered any less intrusive alternatives.[13]

The right to protection of personal data

12. Personal data covers all information relating to identified or identifiable persons. In the ECHR, data protection is not the subject of a separate right but is derived from Article 8 ECHR on the right to privacy, and this is reflected in the relevant case law. This is not the case in the EU with regards to the Charter for Fundamental Rights. Article 8 of the Charter formulates the protection of personal data as a separate, proactive right which entitles individuals to expect that their information will be processed, by *anyone* and not just the state, only if the essential requirements laid down in Article 8 (2) and (3) are fulfilled. It requires processing to be fair and lawful, transparent to the individual (the 'data subject' in EU law) and for specified purposes. The individual is entitled to access and rectification of his/her information, and his/her

[9] Article 7 of the Charter thus almost exactly corresponds with Article 8 of the ECHR, the only difference being the replacement of 'correspondence' in the ECHR with 'communications'.
[10] See also Article 29 Data Protection Working Party, Working document on the surveillance of electronic communications in the workplace, WP55, 2002.
[11] *Schecke*, paragraphs 81-85.
[12] *Rundfunk*, paragraph 74.
[13] *Schecke*, paragraphs 81-86.

rights must be subject to control by an independent authority. These conditions, based on some, though not all, of the principles in Directive 95/46/EC (hereafter referred to as the Data Protection Directive), may be regarded as the 'essence' of the right.[14] The right to the protection of personal data serves also to protect other fundamental rights and freedoms, in particular - but not exclusively - the right to privacy, in that it requires balancing other EU interests and objectives.[15]

13. Article 16 TFEU provides the legal basis for the adoption of rules relating to data protection and the free movement of such data within the EU. These rules (summarised below) provide for a system of checks and balances, including specific rights and obligations, procedures and oversight mechanisms. They apply to all personal data processing, wholly or partially by automatic means, or other means in or intended for a filing system, except where in the course of an activity which falls outside EU law or where it concerns a purely personal or household activity.[16] Each Member State is required to apply national provisions to processing which is 'carried out in the context of the activities of an establishment of the controller on the territory' of that state, including where the establishment itself is based in another Member State or indeed in a third country.[17] One or more of these instruments may therefore apply to measures in financial services regulation.

14. The EU framework does not, in other words, forbid personal data processing; on the contrary the EU encourages processing, through clarification for citizens, businesses and authorities of the 'rules of the game'.

Data protection and privacy as distinct rights

15. Data protection and privacy are therefore distinct rights, in both their nature and operation, and require separate analysis and application. The scope of data protection is broad. Whereas the determination of interference with privacy depends on context, data protection rules apply to all processing subject to certain exceptions.[18] Equally, in another sense, the right to privacy is broader than the right to data protection, in that it relates to the home and the family, and covers many other dimensions in addition to personal information.[19] So not all situations which fall within scope of data protection law are covered by the right of privacy, and not all situations affecting the right to privacy necessarily involve processing of personal data.

16. Some measures involve the processing of personal information, and as such must be compliant with data protection rules, even though they do not affect the right to privacy. For example, the CJEU found that it could not be construed as an interference with private life for an employer to keep a record of the names and salary details of his/her employees (though of course this would require, as data processing, compliance with EU rules on data protection).[20]

---

[14] As confirmed in by CJEU where it referred to an independent data protection supervisor as an 'essential component' of Article 8; Case C-14/10 *Commission v Austria*, judgment of the CJEU of 16 October 2012; C-288/12 *Commission v. Hungary*, judgment of the CJEU of 8 April 2014..

[15] Article 29 Working Party, Opinion 4/2007 on Personal Data, WP 136, 2007, p.7.

[16] Article 3 of Directive 95/46/EC.

[17] Article 4(1)(a) of Directive 95/46/EC. See also Case C-131/12, *Google Spain v. Agencia Española de Protección de Datos*, judgment of the CJEU of 13 May 2014, paragraph 52.

[18] See paragraph 13 above.

[19] See for example U.S. Supreme Court ruling in *Griswold v Connecticut* (1965).

[20] *Rundfunk*, paragraph 74.

17. In other cases, the processing of personal data does affect the right to privacy. In the *Rundfunk* judgement cited above, the CJEU found that where the employer communicates information - whether or not 'sensitive' - on employees with a third party (such as a public authority in the case in question) that would indeed infringe the right to privacy of the persons concerned.[21] Such an effect becomes likely where the information in question is sensitive (medical data for example), where the information is used for surveillance purposes or law enforcement, or where there is something permanent or systematic about the processing, like where the information is retained and not just collected and used.

18. The distinctiveness of the two rights was reflected to some extent in the ruling on the *Digital Rights Ireland* case concerning the mandatory retention of communications data. In that case the CJEU held that it was not enough to apply Article 7 on the right to privacy (despite this being the focus of the national courts which referred the related cases in question to the CJEU). Data retention constituted processing of personal data within the meaning of Article 8 and therefore also had to comply with the article's specific requirements.[22]

19. As these guidelines intend to explain, understanding the extent, purpose and legal basis of personal information processing helps inform the assessment of whether the proposed measure interferes with the right to privacy under Article 7 of the Charter.

Overview of the data protection framework

20. The legal framework governing the processing of personal data in the EU currently consists of four major instruments:

    - **Directive 95/46/EC**,[23] or the Data Protection Directive, is the central piece of legislation on the protection of personal data in Europe. It sets down general rules on the lawfulness of personal data processing and on the rights of the individuals whose data are processed (data subjects), and requires each Member State to ensure that there is an independent supervisory authority responsible for monitoring implementation of the directive.

    - **Regulation (EC) No 45/2001**[24] covers processing of personal data by EU institutions and bodies and establishes the EDPS as an independent supervisory authority.

    - **Directive 2002/58/EC**[25] concerns personal data processing in the electronic communications sector and sets rules of specific relevance including

[21] *Rundfunk*, paragraphs 74- 75.
[22] *Digital Rights*, paragraph 29.
[23] 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, OJ L 281, 23.11.1995, pp. 31 - 50**.** The directive is in the process of being revised and replaced by the proposed General Data Protection Regulation (footnote 6) which, once it enters into force, will require Directive 2002/58/EC and Regulation (EC) No 45/2001 to be revised to ensure alignment of the rules.
[24] 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, OJ L 008, 12.01.2001, pp. 1–22.
[25] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.07.2002, pp. 37–47.

confidentiality, billing and traffic data, and rules on unsolicited commercial communications.

- **Council Framework Decision 2008/977/JHA**[26] addresses police and judicial cooperation in criminal matters and includes rules applicable to exchanges of personal data, including national and EU databases and transmissions to competent authorities and to private parties for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

3. Ten analytical steps

21. As the preceding section indicates, the EU legal framework is complex. The EDPS has therefore prepared for financial services regulation a 10-step methodology which may assist policymakers in anticipating some of the potential difficulties.

1) Identify the personal information to be processed

Definition of personal data

22. Any measure that provides for the processing of personal information should specify clearly the types of personal information, and particularly any sensitive information, to be processed.

23. Personal data is defined[27] as any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, 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. This is a broad concept which covers much more than information that directly identifies an individual, such as a name, a national registration number or taxpayer identification number, and would include, for example, information related to remuneration, earned incomes and assets and the amounts of government subsidy allocated to individuals, biometric information, IP addresses, traffic and location data, daily work and rest periods and corresponding breaks and intervals.[28]

Sensitive information

24. Regulatory measures in the financial sector often require the processing of data relating to offences and criminal convictions, including suspicions of offences: these are referred to as '*sensitive data*'.[29] The other types of sensitive information under EU law include information revealing racial or ethnic origin, political opinions, religious

[26] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, pp. 60-71. The framework decision is also in the process of being revised and replaced by a proposed directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data; COM(2012) 10 final, 25.01.2012.

[27] Article 2(a) of Directive 95/46/EC.

[28] The Article 29 Working Party in Opinion 4/2007 analyses the four elements of the concept, i.e. 'any information', 'relating to', 'identified or identifiable' and 'natural person', each of which needs to be assessed to determine whether 'personal data' are at stake in any given situation. See also Section 4.1 of EDPS Policy Paper.

[29] Article 8 of Directive 95/46/EC describes 'special categories' of personal data. Article 10 of Regulation 45/2001 covers processing of these categories by an EU institution or body; Article 6 of Framework Decision 2008/977/JHA covers processing by a law enforcement authority.

or philosophical beliefs, trade-union membership and data concerning health or sexual life. In the EU, the processing of sensitive data is in principle prohibited unless it complies with strict conditions and applies appropriate confidentiality and security safeguards as required under national law.[30]

Anonymisation

25. Personal information which has been anonymised, that is, data that have been altered so that the data subject is no longer identifiable, is not subject to EU data protection rules.[31] However, technology increasingly makes it possible to re-identify a person using anonymised data, for example in combination with other sources of information which may be available, even publicly. The best means of ensuring that the individual is protected is therefore not anonymisation but rather to keep processing of personal data to the minimum necessary.

Definition of processing and the data controller

26. 'Processing' is defined as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.'[32] Any measure which implies personal data processing (whether or not it is judged to interfere with privacy) needs to be compliant with applicable data protection law.

27. The 'data controller' is the legal or physical person who determines the 'purposes and means' of the processing, and on whom in the EU fall most of the legal responsibilities and obligations for data protection, such as ensuring data quality, applying appropriate security measures and responding to the data subject's exercise of his or her rights. For any measure that involves processing of personal information, the identity of the data controller should be clear.

Recommendation

28. All measures that imply the processing of personal information should contain a substantive provision requiring the processing to be in compliance with EU and national data protection rules. This should be included in the basic instrument itself and not left to Commission delegated or implementing acts or to Member State transposing measures.[33] The provision should address as precisely as possible:

    a) the type of information to be processed, and particularly any sensitive data,

    b) how long the information will be retained,

    c) who will be able to access the information, and

    d) appropriate safeguards for protecting the rights of the individual.

[30] Article 8.5 of Directive 95/46/EC. See below paragraphs 59-61 on data security measures.
[31] Recital 26 of Directive 95/46/EC.
[32] Article 2(b) Directive 95/46/EC.
[33] See for example EDPS Opinion on the European Account Preservation Order, 13 October 2011, p. 4.

2) Assess whether information processing interferes with the right to privacy

29. Separate analyses are required to determine compliance of a proposed measure with the right to privacy, on the one hand, and the right to data protection, on the other. If there does appear to be an interference with the right to privacy, Article 52(1) of the Charter becomes relevant.[34]

Power to enter private premises in the Market Abuse Regulation

Any power to enter private premises in order to seize documents in any form is highly intrusive. In normal circumstances, on-site inspections by competent authorities should be limited to the business premises of the company in question and exclude inspection of private premises of employees except where strictly necessary.

The EDPS argued in his Opinion on the Commission's proposal that such a power should be generally subject to prior judicial authorisation. The Regulation as adopted includes a provision for prior judicial authorisation as required by national law.

Recommendation

30. Policymakers should consider, as part of the impact assessment, whether any interference is proportionate to the purpose of the measure, and whether other measures could achieve the desired outcome with less interference with the fundamental right at stake.[35] If an alternative means is not available, policymakers should aim to narrow the interference to what is strictly necessary for achieving the stated purposes.[36] This could be achieved through reducing the amount of information to be processed or by specifying safeguards of individuals' rights in the instrument itself.[37]

3) Define the purpose for processing of personal information

31. Personal data may only be collected for 'specified, explicit and legitimate' purposes and not be 'further processed in a way incompatible' with those purposes.[38] This is the *'purpose limitation'* principle. In financial services regulation, legitimate public interests include (but are not limited to) the stability of the financial system, transparency, preventing market abuse, increasing market integrity and investor protection, combating money laundering. Enforcement authorities may require information from third parties, such as population, social security, tax registers or telecom operators which includes personal data collected originally for other purposes. Any measures providing for this should apply explicitly the exemptions envisaged by Article 13 of the Data Protection Directive, under which Member States

[34] See paragraphs 10-11above.
[35] In Joined Cases C-92/09 and C-93/09, *Schecke*, the CJEU held in paragraph 81 that, when adopting measures imposing mandatory publication of certain information about beneficiaries of EU funds, the EU legislators should have taken into consideration methods of publishing such information which would be consistent with the objectives of such publication while at the same time causing less interference with those beneficiaries' right to respect for their private life in general and to protection of their personal data in particular.
[36] The CJEU has held that the due to the wide scope of the interference with individuals' fundamental rights, the scope of legislative discretion was necessarily reduced; *Digital Rights Ireland*, paragraph 48.
[37] See below paragraphs 50-58. EDPS Opinion on proposals on markets in financial instruments, 10 February 2012, paragraphs 40-2, 47.
[38] Article 6(1)(b) of Directive 95/46/EC, Article 4(1)(b) of Regulation 45/2001 and Article 3 of Framework Decision 2008/977/JHA.

may adopt legislative measures which are necessary to safeguard monitoring, inspection or regulatory functions connected with an economic or financial interest of a Member State or of the EU.

32. Any information collected under these measures should not be further used for other incompatible purposes. The Article 29 Working Party has provided guidance on the criteria for evaluating compatibility of purposes.[39] Further processing for other purposes which could adversely affect the rights of the individual is likely to be incompatible. For example, data initially collected for purpose of the counter-terrorism or anti-money laundering should not be further processed for tackling fraud and tax evasion, unless the applicable instrument clearly specifies these purposes.[40]

33. EU data protection rules also contain the principle of *'data minimisation'*, whereby only data which are adequate, relevant and not excessive for the defined purpose are collected and used.[41] For each type of personal information, policymakers should test the proportionality of the processing against the 'legitimate objectives pursued', and assess whether the purpose of the measure could be achieved without processing the information.[42]

Insider lists

'Insider information' refers to non-public facts about issuers of financial instruments which, if made public, would likely affect significantly the prices of those financial instruments or of related derivative instruments ('insider dealing'). Under Article 18 of the Market Abuse Regulation, issuers of financial instruments (or a person acting on their behalf or on their account) must produce a list of all persons who have access to inside information and who are working for the issuer under a contract of employment or who are performing tasks through which they have access to inside information, such as advisers, accountants or credit rating agencies. Such insider lists enable competent authorities to investigate possible insider dealing or market abuse.

Following EDPS's recommendation, the Market Abuse Regulation includes an explicit reference to the purpose of the lists, the main elements of the list, the reasons for persons to be included and a reference to the need to consult the EDPS on draft implementing technical standards, to be prepared by ESMA, on the precise format of insider lists and the format for updating them.

Recommendation

34. The measure should always specify the purposes for which personal information will be processed and, as far as possible, specify the further processing which may or may not be considerable compatible.

4) Establish a legal basis for the data processing

Possible legal grounds

35. Under Article 8(2) of the Charter, data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. These grounds are further specified in the Data Protection Directive

[39] See Article 29 Working Party Opinion 3/2013 on the principle of purpose limitation, 2013.
[40] See EDPS Opinion on anti-money laundering, 4 July 2013, pp. 8-9.
[41] Article 6(1)(c) of Directive 95/46/EC and Article 4(1)(c) of Regulation 45/2001.
[42] *Schecke* paragraph 74.

and in Regulation 45/2001.[43] The directive lists several possible grounds for legitimate processing:

a) it is based on the data subject's unambiguous consent

or it is necessary for:

b) the performance of a contract with the data subject;

c) compliance with a legal obligation imposed on the controller;

d) the protection of the vital interests of the data subject;

e) the performance of a task carried out in the public interest; or

f) the purposes of the legitimate interests pursued by the controller, subject to an additional balancing test to safeguard the data subject's rights and interests[44].

36. Regulation 45/2001 concerning the processing of personal data by EU institutions and bodies contains a similar formulation, but omits the ground of 'legitimate interest'. A commonly applied legal basis is the necessity of the processing for the performance of a task carried out in the public interest on the basis of EU law.[45]

Consent as a legal basis

37. Consent of the data subject may be an obvious legal ground, but it is not always an appropriate one due to the conditions which need to be fulfilled for valid consent.[46] For example, on the transparency of debtors' assets, lawful processing of information on debtors' assets should not be based on consent but rather on compliance with a legal obligation or the performance of a public interest.[47] For anti-money laundering measures, the EDPS has suggested 'necessity for compliance with a legal obligation' as an appropriate legal basis.[48] Measures aiming to increase transparency in financial markets should consider performance of a task in the public interest rather than consent. Consent may, however, be appropriate in *ad hoc* one-off situations where there is no chance of undue pressure on the data subject, or as an extra layer of protection for particularly confidential information.

Sensitive information

38. Sensitive information (that is, data on offences etc. - see definition in paragraph 24 above) may not be processed unless one of several exceptions apply:[49]

a) the data subject has given his/her explicit consent to the processing of those data, except where the laws of the Member State provide otherwise;

[43] Article 7 of Directive 95/46/EC and Article 5 of Regulation 45/2001.
[44] See Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.
[45] Article 5(a) Regulation 45/2001.
[46] Article 2(h) of Directive 95/46/EC and Article 2(h) of Regulation 45/2001.
[47] See EDPS Opinion on the Commission Green Paper on the Effective Enforcement of Judgements in the European Union: the Transparency of Debtors' Assets, 22 September 2008, paragraph 9-12.
[48] See EDPS Opinion on anti-money laundering, paragraph 33.
[49] Article 8(2) of Directive 95/46/EC.

b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards;

c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;

d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

Recommendation

39. Any measure involving personal information processing should be based on a proper analysis of the legal basis for that processing and where necessary specify, in the instrument itself, the legal basis for the processing. Any measure envisaging the processing of sensitive information (as defined in the Data Protection Directive), must be clear on which of the five exceptions to the general prohibition apply.

5) Evaluate and justify an appropriate retention period for the information

40. Personal information deemed necessary for the stated purposes should be deleted as soon as the data are no longer needed for those purposes, unless specific EU or national rules apply, such as those requiring the retention of the data for a given period, for example, for tax purposes.[50]

Data retention in monitoring of investment firms and potential money laundering

Recent measures have taken divergent approaches to the retention of personal information collected as part of the monitoring of compliance with EU rules.

The Market Abuse Regulation requires personal data processed as part of supervisory activities to be retained for a maximum of five years.

The revised Directive on Markets in Financial Instruments requires investment firms to retain records of all services, activities and transactions undertaken for five years, or 'up to seven years' if the information is requested by a competent authority.

The Commission's proposal for a new anti-money laundering directive proposes a retention period of five years after a payment has happened, which could be extended up to 10 years – a provision which the EDPS has questioned as arbitrary and lacking in empirical justification.

[50] Article 6(1)(e) of Directive 95/46/EC and Article 4(1)(e) of Regulation 45/2001. See EDPS Opinion on proposals on markets in financial instruments, paragraph 16.

41. Specifying the data retention period in a legal instrument improves legal certainty and is more consistent with best practice. The period should not be set in an arbitrary manner, but rather on the basis of objective criteria and a case-by-case analysis.

Recommendation

42. The legislators should thoroughly evaluate which retention period for the personal information to be processed would be sufficient for and proportionate to the stated purpose. The impact assessment should include an analysis of relevant options. Policymakers should also consider the possibility of a review clause which provides for or mandates at a later date the review and revision of the initial retention period. In the absence of an explicit time limit, the proposed instrument should at least require that data be deleted as soon as no longer necessary.

6) Identify which parties within the EU may have access to the personal information

43. Exchanges of personal information between private organisations and/or public authorities established in the EU also count as data processing within the scope of data protection rules. Separate rules apply to information exchange depending on whether the authority involved is:[51]

    - a law enforcement or judicial authority which may be subject to Framework Decision 2008/977/JHA; or
    - an administrative authority supervising credit or financial institutions which is likely to be subject, at national level, to the Data Protection Directive or, at an EU level, to Regulation 45/2001.[52]

Recommendation

44. Proposals should be as precise as possible about competent authorities in question including:

    - the types of information to be exchanged;
    - the purposes for which the information may be transmitted and further processed;[53] and
    - safeguards against access to the information by other external authorities or third parties which have an interest in the purpose pursued.[54]

7) Establish a correct legal basis for any transfer of personal information outside the EU

45. Transfer of personal data to third countries poses particular risks to the individual and any requirement for such disclosure must be balanced with the individual's rights.[55]

[51] See EDPS Opinion on anti-money laundering, pp. 7-8.
[52] Articles 7 and 8 of Regulation 45/2001 govern transfers of personal data within or between EU institutions or bodies, and to other recipients.
[53] EDPS Opinion on the financial regulation applicable to the general budget of the European Communities, 12 December 2006, pp.12-18, paragraph 22.
[54] See for example EDPS Opinion on anti-money laundering, pp. 21-22.
[55] For more detailed guidance see Article 29 Working Party Working Document 1/2009 on pre-trial discovery for cross-border civil litigation.

As a general principle, under Articles 25 and 26 of the Data Protection Directive and under Article 9 of Regulation 45/2001, personal data may only be transferred to a third country if, without prejudice to compliance with other applicable requirements, the recipient country is deemed by the Commission to have an adequate level of protection.[56] In the absence of an adequacy decision, personal data may be transferred if the transfer falls within a limited number of derogations, which include:

a) the data subject has given his/her consent unambiguously to the proposed transfer;

b) the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken in response to the data subject's request;

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;

d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.

46. These types of derogations must be interpreted carefully, restrictively and on a case-by-case basis.[57] In particular, the grounds of 'important public interest' implies interests identified as such by the national legislation applicable to data controllers established in the EU; the interests of, or even legal requirements laid down by, third countries are not in themselves valid or sufficient.[58] Certain measures in financial services regulation provide for controllers to go beyond their specific legal obligations in helping law enforcement or private stakeholders combat illegal activities, such as money laundering or fraud detection. If there is deemed to be an important public interest under national law in the Member State to which the data controller is subject, this derogation might apply to transfers of personal information to competent authorities of third countries where necessary for the supervision of parent undertakings situated in their territories which have a subsidiary in one or more Member States. However, 'public interest' cannot be used to justify repeated, massive or structural transfers of information, as the EDPS argued in relation to the proposed

[56] If the data is to be transferred to an international organisation, it must be deemed to ensure an adequate level of protection. See the current adequacy decisions issued by the European Commission http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (accessed 16.11.2014). Under Article 9 of Regulation 45/2001, the controller – i.e. the EU institution or body from which the transfer originates - also has the possibility to conduct an assessment of the adequacy of the level of protection afforded by the third country or international organisation in question. See EDPS, 'The Transfer of personal data to third countries and international organisations by EU institutions and bodies: Position Paper', 14 July 2014. If the data is to be transferred to an international organisation, it must be deemed to ensure an adequate level of protection. See the current adequacy decisions issued by the European Commission http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (accessed 16.11.2014).

[57] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, p.7.

[58] Article 29 Working Party, Working document on Article 26(1), pp. 14-15. The Working Party points out that Recital 58 of Directive 95/46/EC refers to international exchanges of data might be necessary 'between tax or customs administrations in different countries' or 'between services competent for social security matters, which implies the interest of authorities of an EU Member State and not only those of authorities in the third country.

mass transfer of personal and sensitive information to foreign countries for anti-money laundering purposes.[59]

47. If none of the derogations apply, the sender of the data must adduce adequate safeguards to ensure that data subjects are adequately protected[60] in an enforceable, legally-binding instrument. For private entities, this usually takes the form of an agreement by means of standard contractual clauses, Binding Corporate Rules or other *ad hoc* agreements between the sender and the recipient of the data. For the public sector, these safeguards may be covered by commitments contained in memoranda of understanding or legally-binding international agreements. Where adequate safeguards are adduced, applicable law may in addition require the sender of the information to notify or to obtain prior authorisation from competent data protection authority(ies).[61]

48. Article 13 of Framework Decision 2008/977/JHA provides for a separate specific regime for international transfers necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Recommendation

49. Measures which envisage transfer of personal data to third countries must be clear on the legal basis for the transfer, and should provide for case-by-case decisions which respect the principle of data minimisation (see above paragraph 33). It may be appropriate to provide explicitly for safeguards ensuring data quality, relevance, and confidentiality, and for prior express authorisation by the competent authority of further transfer of data to or by a third country.

8) Provide appropriate guarantees of individuals' data protection rights

a) Right to information

50. Individuals have the right to be sufficiently informed about the processing of their personal information and about their rights, whether or not the information has been collected directly from them or from other sources.[62] They should be informed at least about the identity of the controller who is responsible for the processing, the purposes of the processing, and any further information that may be relevant.

51. Measures should provide for appropriate guarantees that this right will be respected. For example, in the context of whistleblowing,[63] the person accused should be informed of the nature of the accusation. In the case of EU-wide databases containing personal information, the Commission or whoever is responsible for its management should ensure that the privacy policy is publicly available on its website.

---

[59] See EDPS Opinion on anti-money laundering, pp.11-12.

[60] The safeguards must guarantee adequate protection of the data by the recipient by providing detailed commitments on aspects such as the right for data subjects to enforce any breach of the importer or exporter's contractual obligations, obligations of the exporter and the importer, liability, mediation and jurisdiction details, governing law, supervision, etc.

[61] Under Regulation 45/2001, the EDPS has the possibility to issue an authorisation for the transfer of personal data.

[62] Articles 10 and 11 of Directive 95/46/EC, Articles 11 and 12 of Regulation 45/2001 and Article 16 of Framework Decision 2008/977/JHA.

[63] Whistleblowing schemes typically encourage members of an organisation with the promise of impunity to report breaches of existing rules by a former or current partner/colleague who might be personally liable under applicable law.

The right to information in the context of whistleblowing schemes

The Market Abuse Regulation provides for competent authorities and employers to have in place procedures for reporting actual and potential breaches of the regulation.

Whoever is the subject of accusations in a whistleblower's report should be informed by the person responsible for the whistleblowing scheme as soon as practicably possible after the information is first reported.

The accused should be informed of:

1) the entity responsible for the whistleblowing scheme,

2) the facts of the accusation,

3) the departments or services which might receive the report within his/her own company or in other entities or companies of the group of which the company is part, and

4) how to exercise his/her rights of access and rectification.

However, where there is, and so long as there remains, a substantial risk that such notification would jeopardise the ability of the company or competent authority to investigate effectively the allegation or to gather the necessary evidence, the person responsible for the whistleblowing scheme may delay informing the accused.

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, p. 13.

b) Right of access, rectification and erasure

52. After the processing has started individuals have the right to obtain from the data controller, without constraint, at reasonable intervals and without excessive delay or expense, information on the categories of data being processed, on the purpose for processing, on who is receiving it, and on the 'logic' involved in any automatic processing of his/her personal information. Individuals may obtain access to the personal information being processed in an intelligible form. This right of access, relevant in particular for persons accused by whistleblowers of wrongdoing, is closely related to the right to good administration, including the right to be heard before the adoption of a decision, the right to an effective remedy and the right to the defence of anyone who has been charged.[64]

53. If the processing does not comply with data protection rules because, for example, information is incomplete or inaccurate, individuals may obtain rectification, erasure

[64] Articles 41, 47 and 48 of the Charter of Fundamental Rights. The right for an individual ('data subject') to have access to data which has been collected concerning him or her is set forth in Article 8(2) of the Charter. This right is further detailed in Article 12 (a) of Directive 95/46/EC, in Article 13 of Regulation 45/2001 and in Article 17 of Framework Decision 2008/977JHA. Article 13 of Regulation 45/2001 specifies: 'The data subject should have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge from the controller (…)'. The CJEU has held that the right of access 'must of necessity relate to the past. If that were not the case, the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for the damage suffered.' Case C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, judgment of the CJEU of 7 May 2009, paragraph 54.

or blocking of the data.[65] This applies also where the personal data are 'inadequate, irrelevant or excessive in relation to the purposes of the processing, (...) are not kept up to date, or (...) are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.'[66] Finally, the data controller may have to notify third parties to whom the data have been disclosed of any rectification or erasure carried out, unless it involves a disproportionate effort.[67]

c) Right to object

54. Individuals have the right to object to processing of information concerning him or her at any time on compelling legitimate grounds relating to his or her particular situation.[68] If the objection is justified, processing of that information should stop.

55. Individuals also have the right not to be subject to 'a decision which produces legal effects concerning them or significantly affecting them and which is based solely on automated processing of data intended to evaluate certain personal aspects such as work performance, creditworthiness, reliability etc.'[69]

d) Limitations to data subjects' rights

56. A limitation to data subjects' rights may be justified by objectives of general interest, including the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions, an important economic or financial interest of a Member State or of the EU, including monetary, budgetary and taxation matters, and a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority.[70] If the rights are restricted, the measure may need to provide for additional safeguards, for example the period of time and circumstances in which restriction would apply.[71]

57. Such limitations must be exceptional and respect the conditions set out in Article 52(1) of the Charter. As soon as they are no longer necessary, the measure limiting the rights must cease to apply. On the proposed revision to the anti-money laundering directive, the EDPS recommended that the measure set a time limit after which the restriction to the right of access would no longer apply, and that such restriction

[65] Article 12 sub (b) of Directive 95/46/EC, Article 14 to 16 of Regulation 45/2001 and Article 17 of Framework Decision 2008/977JHA.
[66] Case C-131/12, *Google Spain*, paragraph 92. Article 6(1)(c) to (e) of Directive 95/46/EC and Article 4(1)(c) to (e) require the data controller to ensure the quality of the information processed, irrespective of any action by the individuals concerned.
[67] Article 12(c) of Directive 95/46/EC,
[68] Article 14 of Directive 95/46/EC and Article 18 of Regulation 45/2001.
[69] Article 15 of Directive 95/46/EC, Article 19 of Regulation 45/2001 and Article 7 of Framework Decision 2008/977/JHA. An exception to this right is if the decision a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or b) is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.
[70] Article 13 of Directive 95/46/EC and Article 20 of Regulation 45/2001.
[71] Under Article 20 of Regulation 45/2001 the data subject should be informed of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the EDPS. The data subject also has the right to have indirect access to his or her data through the intermediary of the EDPS, who informs him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made. See EDPS Guidelines on the Rights of Individuals with regard to the Processing of Personal Data, 25 February 2014, pp. 26-34. For an example see EDPS Opinion on anti-money laundering, pp.15-16.

should not apply to those cases that are subsequently considered unfounded or irrelevant.[72]

Recommendation

58. Measures which, in the light of these analytical steps, appear to be particularly intrusive, should be as explicit as possible in providing guarantees that individuals whose personal information is to be processed may exercise their rights. Any limitation on these rights should be explicitly provided for and justified in the measure, and be limited in time, in accordance with Article 52(1) of the Charter.

9) Consider appropriate data security measures

59. Financial services regulation relies on large databases and complex IT systems operated by financial entities or regulatory authorities. EU data protection rules require data controllers to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. This implies the need for the controller to identity, evaluate, prioritise and treat security risks as appropriate to the the specific processing operation. The processing of sensitive data in particular requires higher levels of security.

60. Appropriate technical and organisational measures for managing the risks identified could translate into functions supporting the overall compliance of the measure with data protection rules. They could facilitate individuals' right to access, verify and assure data quality, and ensure audit trails for data access, transfers and modification and elimination of data after the retention period. Specific measures could include:

    - encryption, for data confidentiality and integrity;
    - secure connections and measures to define and protect logical security perimeters, such as firewalls, intrusion prevention and detection systems;
    - preventing unauthorised physical access to the IT infrastructure and secure premises;
    - authorisation and authentication procedures for IT systems;
    - employee screening and segregation of duties; and
    - organisational measures to ensure appropriate reaction to security incidents, in particular personal data breaches.[73]

61. The Commission's proposed General Data Protection Regulation promotes the concepts of *privacy by design*, where data protection and privacy are integrated in new products, services and procedures from design phase and throughout all their

[72] See EDPS Opinion on anti-money laundering, pp.15-16.

[73] Article 4(3) of the ePrivacy Directive 2002/58/EC requires providers of publicly available electronic communication services to implement specific confidentiality and security requirements. It also requires them to report data breaches, and such a duty on all data controllers is envisaged in the General Data Protection Regulation. They may also be required under specific sectoral instruments or general civil law with respect to liability and are generally considered good practice.

lifecycle, and *privacy by default*, where the default settings of a system are privacy-friendly. The EDPS can provide practical advice on how to integrate these concepts into appropriate 'level 2' standards[74] for data processing in databases, early warning systems and other IT systems.

Recommendation

62. Measures which involve data processing by means of large IT systems should be predicated on careful assessment of their necessity. They should provide for appropriate technical and organisational safeguards for protecting personal and often sensitive data, and for consultation of the EDPS on the development of technical standards through delegated and implementing acts.

10) Provide for specific procedures for supervision of data processing

63. The processing of personal data is supervised by national data protection authorities and, for EU institutions and bodies such as European financial supervisory authorities, by the EDPS.[75] For example, under Regulation (EC) No 1060/2009 on credit rating agencies, where competent authorities may exchange information with the European Securities and Markets Authority (ESMA), processing by national competent authorities at national level is supervised by the data protection authorities while processing by ESMA is subject to supervision by the EDPS. Data controllers must notify to the competent data protection authority any processing likely to pose specific risks to the rights and freedoms of data subjects before the processing starts.[76] Risky processing likely to require such 'prior checking' by EDPS[77] includes:

    a) information processed relating to suspected offences, offences, criminal convictions or security measures, such as in whistleblowing schemes;

    b) operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct; and

    c) operations for the purpose of excluding individuals from a right, benefit or contract, for example in the assessment of consumers' creditworthiness.[78]

Recommendation

64. Measures which envisage operations which pose particular risks to the rights of individuals should specify the procedures for notifying competent data protection authorities and seeking prior checks of personal information processing.

4. Applying the methodology to measures in financial services regulation

This section, by way of illustration, applies the above 10-step methodology to three typical provisions with implications for the rights to privacy and to the protection of personal data contained in recently adopted instruments in the area of financial services regulation:

[74] Level 2 of the four level 'Lamfalussy approach' to financial services legislation followed by the EU refers to implementing measures adopted by the Commission on basis of drafting or advice from the European financial supervisory authorities. See http://ec.europa.eu/internal_market/securities/lamfalussy/index_en.htm (accessed 16.11.2014).
[75] Article 28 of Directive 95/46/EC and Article 41 of Regulation 45/2001.
[76] Article 20 of Directive 95/46/EC and Article 27 of Regulation 45/2001.
[77] Article 27(2) of Regulation 45/2001.
[78] See EDPS Opinion on credit agreements relating to residential property, 25 July 2011.

a. transparency and publication of sanctions;

b. whistleblowing schemes; and

c. recording of telecommunications and powers to request telephone and traffic data.

Transparency measures and publication of sanctions

Step 1: Identify the personal information to be processed

A number of measures, such as the Directive 2014/65/EU on markets in financial instruments and Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, envisage the publication of sanctions for breaches of financial services regulations, including identification of the person responsible for the breach. Monitoring of the activities of companies to ensure the integrity of the market is also likely to imply reporting requirements. Companies may be required to disclose personal information on their employees and/or on their clients.

Step 2: Assess whether information processing interferes with the right to privacy

Publication of names of persons judged to have breached the rules constitutes an interference with their right to privacy. This interference could be minimised in a number of ways:

a) It should not be automatic and should be avoided if the purpose can be achieved through less intrusive means. The authority should be able to exercise discretion on a case-by-case basis not to publish less serious violations, where the violation caused no significant harm or where the party has shown a cooperative attitude. Publication should be justified by the gravity of the breach and losses for third parties, the levels of personal responsibility and recidivism, plus any other specific circumstances.[79]

b) Any publication should be deferred until after the last instance of a judicial procedure is exhausted, and never in situations where the decision is subject to an appeal and where it is eventually annulled by a court.[80]

c) Before the publication of the decision, the undertaking concerned should be requested to indicate which information should be considered confidential and therefore not published.

d) The names of natural persons (employees or other individuals) should be deleted from the decisions which are published, and the functions of individuals to which reference is made in these decisions or other documents should be redacted and replaced by more general ones (e.g. 'manager').

Step 3: Define the purpose for data processing

Transparency is intended to help deter future breaches and to inform market operators of any particular breach. As an objective, although it affects the right to privacy and needs to reflect

[79] EDPS Opinion on insider dealing and market manipulation, 10 February 2012, paragraph 45; EDPS Opinion on activity of credit institutions and prudential supervision, 10 February 2012, paragraph 21; EDPS Opinion on credit rating agencies, 10 February 2012, paragraph 47.
[80] EDPS Opinion on proposals on markets in financial instruments, paragraph 61.

the requirements laid down by the CJEU,[81] it may be legitimately pursued on condition that confidentiality requirements are complied with.

Step 4: Establish a legal basis for data processing

An appropriate legal basis for publication would be the performance of a task in the public interest or compliance with a legal obligation imposed on the controller, rather than consent of the data subject.

Step 5: Evaluate and justify an appropriate retention period

Personal information should be kept by the company and/or by the oversight authority for no longer than is necessary and anonymised as soon as personal data are no longer relevant for the application of the EU regulation in question. Given that in most cases publication will be on the internet, Member States should be required to ensure that personal data are kept online for a reasonable period of time only, after which they should be systematically deleted.[82]

Step 6: Identify which parties within the EU may have access to the personal information

Individuals should only be able to access personal data on a need-to-know basis, and must not process them except on instructions from the controller.

Appropriate technical and organisational measures must be implemented to protect data against accidental or unlawful destruction, accidental loss, alteration and unlawful disclosure, for example through awareness raising among employees. Where on-request access by third parties such as law enforcement authorities is envisaged, it should be clear by which authorities and for which purpose the personal data may be further processed.

Step 7: Establish a correct legal basis for any transfer of personal information outside the EU

Cooperation between competent authorities in the EU with those in third countries typically involves exchange of information on cross-border trading and on parent undertakings in one state which have a subsidiary in another.

Where this exchange implies a transfer of personal information to a third country not deemed by the Commission to have an adequate level of protection, an important public interest ground recognised in national law may be appropriate. Any transfers should not be automatic but rather be based on a case-by-case assessment basis of its necessity and proportionality. Conditions should be applied to any further transfer to another third country, such as requiring express written authorisation of the Member State authority.[83]

[81] EDPS Opinion on proposals on markets in financial instruments**,** paragraph 51; Joined Cases C-92/09 and C-93/09, *Schecke*, paragraph 56-64.

[82] EDPS Opinion on insider dealing and market manipulation, paragraph 49-50*;* EDPS Opinion on proposals on markets in financial instruments, paragraph 64.

[83] EDPS Opinion on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, paragraphs pp. 14-16. An example of this provision is in Article 29 of the Market Abuse Regulation.

Step 8: Provide appropriate guarantees of individuals' data protection rights

Competent authorities should be proactive in informing data subjects before publication of any decision sanctioning them, and uphold their right to object on compelling legitimate grounds.[84]

Step 9: Consider appropriate data security measures

Any measure which aims to increase transparency should provide for staff members of competent authorities to respect professional secrecy and should prohibit the disclosure of confidential information.[85]

Whistleblowing schemes

Step 1: Identify the personal information to be processed

Procedures for reporting breaches or whistleblowing have implications for the protection of the personal data of the whistleblower and the person accused of wrongdoing.[86] Persons responsible for whistleblowing schemes should carefully assess whether it might be proportionate and appropriate to limit the number of persons entitled to eligible for reporting alleged misconduct, the categories of persons who may be incriminated and the breaches for which they may be incriminated.

Step 2: Assess whether information processing interferes with the right to privacy

The confidentiality of the identity of whistleblowers should be protected at all stages of the procedure, unless its disclosure is required by national law in the context of further investigation or subsequent judicial proceedings.[87]

Step 5: Evaluate and justify an appropriate retention period

Retention periods for personal data collected as part of the investigation into a report should be kept to a minimum. In principle there should be no need to retain data for longer than two months after completion of the investigation, unless legal proceedings or disciplinary measures are initiated against the incriminated person or, in cases of false or slanderous declaration, the whistleblower.

Step 8: Provide appropriate guarantees of individuals' data protection rights

Persons accused of wrongdoing must be able to exercise their right of defence, the right to be heard before the adoption of a decision which concerns him/her and the right to seek an effective judicial remedy against any decision or measure concerning him/her.[88] Whistle-blowers should be encouraged to file identified and confidential reports rather than

[84] Article 14 of Directive 95/46/EC. EDPS Opinion on proposals on markets in financial instruments, paragraph 62*;* EDPS Opinion on insider dealing and market manipulation, paragraph 48.

[85] EDPS Opinion on proposal for directive on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, paragraphs 17 and 18.

[86] 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.

[87] EDPS Opinion on proposals on markets in financial instruments**,** paragraph 67*;* EDPS opinion on Commission proposals on insider dealing and market manipulation**,** paragraph 54.; EDPS Guidelines on the rights of individuals with regard to the processing of personal data, p. 32

[88] EDPS Opinion on proposals on markets in financial instruments**,** paragraph 68.

anonymous reports, and those responsible for the scheme should disclose the identity of whistleblowers where the accusation has transpired to be malicious.[89]

Step 10: Provide for specific procedures for supervision of data processing

Any whistleblowing scheme implies the processing of personal information relating to suspected offences and, as such, implies specific risks to both the persons reporting the alleged wrongdoing and the accused. The scheme should therefore be submitted to the competent data protection authority for prior checking.

Recording of telecommunications and powers to request telephone and traffic data

Step 1: Identify the personal information to be processed

The categories of data related to communications to be processed should be clearly defined.[90] 'Traffic data' is defined in EU law as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.[91] These data typically include personal information, including the identity of the persons making and receiving the call, the time and duration of the call, the network used and, in the case of portable devices, the geographic location of the user. Some traffic data relating to internet and email use, such as the list of websites visited, may in addition reveal important details of the content of the communication.[92] In referring to communications data, a clear distinction should be made between 'traffic data' and information on the content of the communication (the 'conversation').

Step 2: Assess whether information processing interferes with the right to privacy

Often companies in the financial services sector record the content of the conversations concerning transactions.[93] Even where the conversations in question relate wholly or primarily to financial transactions or professional activities, records of these communications include personal data and access to this information by competent authorities represents a significant interference with the right to privacy. Unless strictly necessary, the measure should explicitly exclude access by competent authorities to the content of communications.[94] Access to communications data by the competent authority should require a prior judicial authorisation in the interest of harmonised application of EU legislation across all Member States.[95]

Step 3: Define the purpose for data processing

Information on telephone and electronic communications involving employees of a company can be valuable in investigating wrongdoing or breaches of a company's obligations. Any measure enabling access to this information should precisely define the purpose for this processing in accordance with Article 6(1) of the Data Protection Directive.[96] Powers to

[89] See EDPS Guidelines on the rights of individuals with regard to the processing of personal data, p. 32
[90] EDPS Opinion on proposals on markets in financial instrument, paragraph 34.
[91] Directive 2002/58/EC, Article 2.
[92] EDPS Opinion on Commission proposals on insider dealing and market manipulation, paragraph 24. EDPS Opinion on proposals on markets in financial instrument, paragraph 44.
[93] EDPS Opinion on proposals on markets in financial instrument, paragraph 20.
[94] EDPS Opinion on insider dealing and market manipulation, paragraphs 25, 32 and 34. EDPS Opinion on proposals on markets in financial instrument, paragraph 32.
[95] EDPS Opinion on insider dealing and market manipulation, paragraph 27; EDPS Opinion on credit rating agencies, paragraph 18.
[96] EDPS Opinion on proposals on markets in financial instrument, paragraph 28.

request traffic data should be clearly defined and should be limited to cases where there is a reasonable suspicion that such records may be relevant to prove a breach of the company's obligations.

Step 5: Evaluate and justify an appropriate retention period

The measure should stipulate an appropriate maximum period of data retention applicable to both undertakings and competent authorities in charge of supervision of the financial market/activity in question.[97]

Step 8: Provide appropriate guarantees of individuals' data protection rights

The measure should provide for the right of the addressee to have the decision on access to communications data as issued by the competent authority reviewed by the courts.[98] The measure should ensure that the data subject is informed of the right to rectify data relating to him/her and the right to have recourse to the EDPS.[99]

5. Working with the EDPS

65. Under Article 28(2) of Regulation 45/2001, the Commission is required to consult the EDPS when it adopts a legislative proposal relating to the protection of individual rights and freedoms with regard to the processing of personal data.

66. In practice, the EDPS has taken a proactive role in offering advice at all stages of the policymaking and legislative process, not only to the Commission but to also to the Parliament and the Council.[100] Furthermore, following discussions with the Commission, it was agreed and set down in a note from the Secretary General in December 2006 that Commission services should consult the EDPS informally prior to adoption of a proposal with a data protection dimension, and that where the Commission itself is the legislator (directives or regulations of the Commission, 'Comitology' or other decisions, negotiation mandate) or for non-legislative documents, formal consultation would take place before the adoption of the act by the College, without prejudice to an informal consultation during the preparatory phase. The EDPS wishes to continue and to intensify these working arrangements.

67. It is increasingly common for implementing measures and delegated acts to be prepared by EU financial supervisory authorities, usually following public consultation, and submitted to the Commission which then, in effect, has limited scope for amending these draft texts. The EDPS reserves the right to comment on these drafts by way of a public opinion, but in most cases it would be more appropriate to provide comments to the Commission directly, both formally after, and informally prior to, adoption of the instrument. For this advice to be valuable, the Commission ought to provide EDPS with reasonable time to review the documents.

68. The EDPS would welcome feedback on these guidelines and intends to review their effectiveness and relevance no later than 2019.

[97] EDPS Opinion on proposals on markets in financial instrument**,** paragraph 38.
[98] EDPS Opinion on insider dealing and market manipulation**,** paragraph 28**.**
[99] EDPS Opinion on a notification for prior checking received from the Data Protection Officer of the European Central Bank on the recording, storing and listening of telephone conversations in DG-M and DG-P, Brussels, 5 May 2006 (Case 2005-376), pp.11-13.
[100] See section 3.2 EDPS Policy Paper.

Brussels, 26 November 2014

Annex: EDPS opinions in the context of EU regulation of financial services

(On creation of the Early Warning System database) EDPS Opinion on a modified proposal for a Council Regulation amending Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities (COM(2006) 213 final) and on the proposal for a Commission Regulation (EC, Euratom) amending Regulation (EC, Euratom) No 2342/2002 laying down detailed rules for the implementation of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities, adopted on 12 December 2006, OJ C 94, 28.4.2007.

EDPS Opinion on a Commission Green Paper on the Effective Enforcement of Judgements in the European Union: the Transparency of Debtors' Assets, adopted on 22 September 2008, OJ C 20, 27.1.2009.

EDPS Opinion on the proposal for a Directive of the European Parliament and of the Council on Deposit Guarantee Schemes (recast), adopted on 9 September 2010, OJ C 323, 30.11.2010.

EDPS Opinion on the proposal for a Regulation of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories, adopted on 19 April 2011, OJ C 216/04, 22.07.2011.

EDPS Opinion on the Proposal for a Regulation of the European Parliament and of the Council establishing technical requirements for credit transfers and direct debits in euros and amending Regulation (EC) No 924/2009, adopted on 23 June 2011, OJ C 284/01, 28.09.2011.

(On consulting national credit databases to assess consumers' creditworthiness) EDPS Opinion on the proposal for a Directive of the European Parliament and of the Council on credit agreements relating to residential property, adopted on 25 July 2011, OJ C 377/02, 23.12.2011.

EDPS Opinion on a proposal for a Regulation of the European Parliament and of the Council creating a European account preservation order to facilitate cross-border debt recovery in civil and commercial matters, adopted on 13 October 2011, OJ C 373/03, 21.12.2011.

EDPS Opinion on a proposal for a Directive of the European Parliament and of the Council on markets in financial instruments repealing Directive 2004/39/EC of the European Parliament and of the Council, and on a proposal for a Regulation of the European Parliament and of the Council on markets in financial instruments and amending Regulation on OTC derivatives, central counterparties and trade repositories, adopted on 10 February 2012, OJ C 147, 25.5.2012.

EDPS Opinion on a proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation, and on a proposal for a Directive of the European Parliament and of the Council on criminal sanctions for insider dealing and market manipulation, adopted on 10 February 2012, OJ C 177, 20.6.2012.

EDPS Opinion on a proposal for a Directive on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, and on a proposal for a

Regulation on prudential requirements for credit institutions and investment firms, adopted on 10 February 2012, OJ C 175, 19.6.2012.

EDPS Opinion on a proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 1060/2009 on credit rating agencies, adopted on 10 February 2012, OJ C 139/02, 15.5.2012.

EDPS Opinion on the proposals for a Regulation on European Venture capital funds and for a Regulation on European social entrepreneurship funds, adopted on 14 June 2012, OJ C 335, 01.11.2012.

EDPS Opinion on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying the transfers of funds, adopted on 4 July 2013, OJ C 32, 04.02.2014.

EDPS Opinion 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, adopted on 9 July 2012, OJ C 336, 06.11.2012.

EDPS Opinion on a proposal for a Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions, adopted on 5 December 2013, OJ C 38, 08.02.2014.