Opinion of the European Data Protection Supervisor

on the Commission Regulation establishing a Union Registry for the trading period commencing on 1 January 2013, and subsequent trading periods, of the Union emissions trading scheme

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],

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1.1. Background

1. On 18 November 2011, the Commission adopted Commission Regulation (EU) No 1193/2011 establishing a Union Registry for the trading period commencing on 1 January 2013, and subsequent trading periods, of the Union emissions trading scheme pursuant to Directive 2003/87/EC of the European Parliament and of the Council and Decision No 280/2004/EC of the European Parliament and of the Council and amending Commission Regulations (EC) No 2216/2004 and (EU) No

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

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

920/2010 (the 'Regulation').[3] The Regulation was sent to the EDPS for consultation on the same date.

2. Already before the adoption of the Regulation, the EDPS was given the possibility to provide informal comments. Some of these comments have been taken into account in the Regulation, and the EDPS notes that the data protections safeguards have been strengthened as a result.

3. The EDPS welcomes the fact that he is formally consulted by the Commission and that a reference to the present Opinion is included in the preamble of the instrument adopted.

1.2. Objectives and scope of the Regulation

4. The EU Emissions Trading System ('ETS') is one of the policies introduced across the European Union ('EU') to help meet EU greenhouse gas emissions reduction targets under the Kyoto Protocol. The ETS creates a compliance regime for operators and aims at ensuring that emissions are effectively capped across the EU.[4]

5. The Regulation amends and will replace as of 1 January 2013 earlier Commission Regulations on the subject, in particular, Commission Regulations (EC) No 2216/2004 and (EU) No 920/2010[5], both adopted to provide the rules 'for a standardised and secured system of registries'.

6. One of the key novelties introduced via the Regulation is the establishment, as of 2012, of a centralised, Union Registry, instead of the previous system of a combination of national registries.

7. The Union Registry and the so-called European Union Transaction Log (or 'EUTL'), which has already been in place at the EU level, are two sub-systems hosted and operated by the European Commission. They have two different functions but are complementary systems.

8. The Union Registry holds the accounts of actors involved in the ETS (e.g. operator holding accounts, aircraft operating holding accounts, trading accounts, auction accounts) and records transactions performed between accounts. The Union Registry, thus, is a central electronic registry at EU level to support emission trading by account holders within and across Member States.

9. The EUTL, in turn, records the allocations, transfer and cancellation of CO2 emission allowances in the EU and checks the consistency and coherence of certain operations.

2. Objectives and structure of the EDPS opinion

10. While the main objective of the Regulation is not the processing of personal data, the Regulation nevertheless requires the processing of personal data, including criminal record information and information on suspected criminal activities. These

[3] OJ L315, 29.11.2011, p. 1.
[4] For further information on the ETS, see http://ec.europa.eu/clima/publications/docs/ets_en.pdf.
[5] OJ L 386, 29.12.2004, p. 1 and OJ L 270, 14.10.2010, p. 1.

data are processed in order to ensure that the accounts will not be misused for criminal activities.

11. The personal data may relate to individuals acting on behalf of the account-holders such as their 'directors' and authorized representatives. In addition, account-holders themselves may also be natural persons. If so, their personal data may also be processed. Further, some data are also collected about beneficial owners of the account-holders, who may also be individuals.[6]

12. In light of the -often sensitive- personal data that are required to be processed under the Regulation, the EDPS recommends that adequate data protection safeguards should be established in the Regulation.

13. Considering that the Regulation has already been adopted, the primary objective of this Opinion is to help ensure that the EDPS recommendations will be taken into account when the Regulation will be amended, which is foreseen for the end of 2012.

14. In addition, the recommendations provided in the Opinion may also serve to guide the Commission and national administrators when implementing the necessary data protection safeguards at the practical level. For more detail on practical implementation, see paras 41-43 calling for the preparation of a comprehensive data protection policy, para 36 on other practical measures such as help menus and warning messages in the Union Registry, and training materials, and para 40 on system documentation and publication of information on the Union Registry website.

15. Section 3 of this Opinion briefly outlines what personal data are required to be processed pursuant to the Regulation, focusing on sensitive data. This description is necessary in order to put into context the recommendations provided in Sections 4-12 of this Opinion. Section 4 calls for further clarifications on what personal data are processed under the Regulation, who processes such data and where the data are stored, focusing, again, on sensitive data. Sections 5-12 contain the remaining recommendations of the EDPS, while Section 13 outlines his conclusions.

3. Personal data required to be processed under the Regulation

Information processed by national administrators in connection with account opening and account management

16. A large part of the personal data required to be processed under the Regulation is collected by national administrators in EU Member States from applicants when they apply for the opening of an account in the Union Registry (see Articles 12-24, which, in turn, refer to various annexes). These 'national administrators' are the entities responsible for managing on behalf of a Member State a set of user accounts under the jurisdiction of a Member State in the Union Registry.

17. In order to open an account, the Regulation requires that the applicants submit information, including personal data, to the national administrator. The information

[6] See Section 3 below for more detail on the categories of data, including sensitive data, processed under the Regulation.

required varies depending on the type of account (see, in particular, Annexes II, III, IV, V and VII).

18. The data range from personal identification numbers, names, job titles, addresses, fixed and mobile telephone numbers, dates and places of birth and preferred languages, to copies of identity cards, passports, proofs of permanent residence, and criminal records.

19. In addition, some information must also be provided to the national administrators on the legal entity's beneficial owners in the context of prevention of the use of the financial system for the purpose of money laundering and terrorist financing (see Annex III, point 5(d)).

20. Further, Article 20 requires national administrators to refuse to open an account in certain circumstances, including when they have reasonable grounds to believe that the accounts may be used for fraud involving allowances or Kyoto units, money laundering, terrorist financing or other serious crimes. It is not specified, and presumably left for national law to determine, what additional information (beyond the documents required to be submitted by the Regulation) a national administrator may access to come to a conclusion that such 'reasonable doubts' exist.

21. Similarly to Article 20, a number of other provisions relating to account management also require processing sensitive personal data by the national administrator on suspected criminal activities. These include:

- Article 22 on refusal of authorised representatives;
- Article 31 on suspension of accounts;
- Article 30 on closure of accounts and removal of authorised representative 'on the administrator’s initiative'; and
- Article 71 on 'suspension of access to allowances or Kyoto units in the case of a suspected fraudulent transaction'.

Information exchanges among national administrators, the Commission, and third parties including law enforcement agencies

22. The referred Article 71, as well as various other articles of the Regulation (including Articles 36(4), 70, 72, 73 and 83), call for exchange of data, including information on suspected criminal activity, among national administrators, the Commission, and third parties including law enforcement agencies.

23. Article 71(3) of the Regulation requires the national administrator (or the Commission) to 'immediately inform the competent law enforcement authority of the suspension [of an account]'. Article 72 requires national administrators to cooperate with the relevant competent authorities and requires notification of known or suspected money laundering, terrorist financing or criminal activity. Article 36(4) imposes other specific notification requirements. Further, Article 83(8) specifically allows, although it does not require, notification of certain specific suspicious transaction patterns to tax and law enforcement authorities.

24. Article 70(2) and (3) call for notification of security breaches or risks among national administrators and the Commission in cases in which these may lead to suspension of access to the Union Registry.

25. Further, Art 73(1) provides that the 'Commission may instruct the central administrator to temporarily suspend the acceptance by the EUTL of some or all processes originating from the Union Registry if it is not operated and maintained in accordance with the provisions of this Regulation. It shall immediately notify national administrators concerned'.

26. Article 83(7) requires that national administrators 'shall make available through secure means to all other national administrators and the central administrator'[7] the names and identities of persons for whom they refused to open an account, or whom they refused to nominate as an authorised representative, and the names and identities of the account holder and authorised representatives of accounts to which access has been suspended or which has been closed due to (among others) certain known or suspected criminal activities. Although this is not explicitly stated in the Regulation, as explained by the Commission, this provision is intended to reduce the risk that account-holders and their representatives who have been refused the account-opening, or whose accounts have been suspended or closed due to suspected criminal activities, could subsequently successfully reapply to open an account in another Member State. Re-application in another Member State after refusal or suspension is in itself not prohibited under the Regulation. Neither does the failure of an earlier application in one Member State exclude the possibility of a subsequent successful application in another Member State. However, to discourage forum-shopping, and ensure effective cooperation, the Regulation has put in place an information exchange mechanism, which functions, as a matter-of-fact, as a black-list, and alerts national administrators that heightened scrutiny of any new applications of the individuals or organizations concerned may be necessary.[8]

27. Article 83(2)-(6) allows direct access to the Union Registry and the EUTL to Europol and access on request to certain other third parties including law enforcement and tax authorities (see Section 7 for more detail).

4. Further clarifications needed regarding the personal data processed under the Regulation

Are personal data stored and exchanged in the Union Registry or outside of it?

28. The Regulation does not specify whether any part of the personal data processed in connection with account management will also be recorded in the Union Registry. Neither does the Regulation specify whether the information exchanges among national administrators and the Commission take place within or outside the Union Registry and the EUTL. Based on the text of the Regulation alone it is thus also not clear whether any sensitive data is recorded and stored in the Union Registry and the EUTL.

29. This specification is of crucial importance considering that pursuant to Article 81(1) of the Regulation, data stored in the Union Registry are required to be stored for 15 years. This is a long retention period that may not be appropriate for the storage of many categories of sensitive data.[9]

[7] On the central administrator, see Section 5 below.
[8] See Section 10 on specific recommendation on this blacklist.
[9] See Section 9 on retention periods.

30. Based on further information provided by the Commission, it appears that much of the data collected when opening an account, such as actual copies of criminal records, or copies of passports, identity cards and documents providing proof of residence, are not uploaded onto the Union Registry, but rather, processed and stored locally, by national administrators, subject to national data protection laws.

31. With respect to criminal records, it appears that no information is to be systematically uploaded onto the Union Registry. However it cannot be excluded that a national administrator may not include, for example, an observation in the comment field in the database indicating the reasons for refusal of opening an account. With respect to identity documents, it appears that expiry dates and ID or passport numbers are uploaded onto the Union Registry but not copies of the actual documents themselves.

32. It also appears that the fact whether an account opening was refused, or an account was suspended may be recorded in the Union Registry[10].

Clarifications on whether the Union Registry and EUTL may contain sensitive data

33. Based on the foregoing, the EDPS recommends that the text of the Regulation should be revised to include the clarifications regarding what data are processed within and outside of the Union Registry and the EUTL. To this effect the EDPS would particularly welcome a general provision in the Regulation that no special categories of personal data,[11] and in particular, no criminal records, or information regarding actual or suspected fraud or other criminal activities are recorded in the EUTL or in the Union Registry.[12]

34. Any exceptions from this general rule should be specifically set forth and must be necessary and proportionate. For example, as noted in para 27, it appears that the fact whether an account opening was refused, or an account was suspended may be registered in the Union Registry. Combined with the name of the account holder, which may be a natural person, or with the names of its representatives (e.g. directors), this information may constitute sensitive personal data. This and similar exceptions should be adequately justified, and specifically set forth in the Regulation.

Use of open comment fields

35. As noted in para 30 above, it appears that no criminal record information is to be systematically uploaded onto the database. However, as explained in para 31, it cannot be excluded that a national administrator may include, for example, a comment in the database indicating the reasons for refusal of opening an account. To address these situations, the EDPS recommends that the Regulation clearly prohibit the use of open fields for the entry of sensitive data, except if this is necessary and proportionate for the management of the Union Registry, and specifically allowed under the Regulation (see para 34 above).

[10] The Commission explained that in any event, this information is not 'transferred internationally' (See Section 11 below on international transfers.)
[11] See Article 8 of Directive 95/46/EC.
[12] This should also be made clear in the data protection policy referred to in paras 41-43.

36. At the practical level, the EDPS recommends that clear instructions should be provided for users of the Union Registry (via a help-menu, warning message, training materials and/or otherwise) to indicate that no such information is to be included in the comment fields.

Information regarding beneficial owners

37. The EDPS also recommends that the Regulation should clarify what information will be processed regarding beneficial owners (see para 19 above).

5. The central administrator

38. Articles 4 and 5 (read in conjunction with Article 3(2) of the Regulation and Article 20 of Directive 2003/87/EC) provide that a central administrator, designated by the Commission, shall operate and maintain the Union Registry as well as the EUTL.

39. It is not clear from the Regulation whether the central administrator will be part of the European Commission, whether it will be another EU institution/agency/body, or an entity organized under the laws of one of the Member States. Neither is it clear what will be the respective obligations of the Commission and the central administrator nominated by it, should these two entities be different. On these issues clarifications would be necessary. In particular, if the intention is for the Commission to act as a central administrator, as this has been explained to the EDPS by the Commission, this should also be clearly stated in the text of the Regulation itself.

40. In addition, the EDPS recommends that this information should also be made clear at the practical level, in system documentation, including in the data protection policy referred to in paras 41-43 and on the publicly available part of the Union Registry website.

6. Allocation of tasks and responsibilities: adoption of a data protection policy

41. Clarifications would also be welcome on the allocation of tasks and responsibilities between national administrators and the central administrator, with respect to data protection.

42. The EDPS recommends specifying in a comprehensive data protection policy for the ETS or in a similar document prepared in collaboration among the Commission and national administrators, which entity will be responsible for what, with reference to the data protection regime that applies in each case. This document could make clear, for example, who should provide notice to data subjects, be responsible for acting when access, rectification, blocking, or erasure is requested by data subjects, who bears responsibility for the security of the Union Registry and the EUTL, and who makes decisions regarding their design.

43. The requirement to adopt such a document could be specifically foreseen in the Regulation itself. The main elements of this framework should also be clarified in the Regulation itself.

7. Access to data by Europol and other third parties

44. Article 83 deals with the confidentiality of the information contained in the EUTL and the Union Registry. The Article sets out to whom and under which circumstances the data can be provided. The default rule, in para 1, is that all information in the EUTL and the Union Registry is considered confidential, unless otherwise required by 'Union law, or by provisions of national law that pursue a legitimate objective compatible with this Regulation and are proportionate'.

45. The remainder of the Article provides that a number of specifically listed entities (including law enforcement and tax authorities of Member States, the European Anti-Fraud Office, the European Court of Auditors, Eurojust and others) may obtain data stored in the Union Registry and the EUTL, upon request, if such requests are necessary for the performance of their tasks. Article 83(5) specifically mentions that this may also include 'anonymous transaction data for the purpose of looking for suspicious transaction patterns'. Article 83(5) further provides that these entities, in turn, 'may notify suspicious transaction patterns to other entities listed' above.

46. In addition, Europol has permanent access, for purposes of the performance of its tasks in accordance with Council Decision 2009/371/JHA establishing the European Police Office. Europol shall keep the Commission informed of the use it makes of the data.

47. The EDPS, first, recommends that the purposes of access to data by the entities listed, including Europol, be further defined. Simply listing the names of the entities to which transfers can be made does not constitute sufficient 'definition of purpose' under data protection laws. Instead of simply providing a list of entities it may be appropriate to provide that access under Article 83 would be limited to cases where this is necessary and proportionate for purposes precisely identified and listed in the Regulation.

48. The EDPS here also reminds that, in principle, all possible purposes of transfers of personal data should be specified and compatible with the original purpose for which they were collected. Any extension to matters not falling within the scope of the operation of the Union Registry (e.g. money laundering, terrorist financing or other serious crimes) should be extensively justified and clearly framed.

49. In this regard, the EDPS notes that Commission Regulation (EU) No 920/2010, now amended by the Regulation, provided a more specific description of the purposes, mentioning, in its Article 75(3) that transfers were possible ‘if such requests are justified and necessary for the purposes of investigation, detection and prosecution of fraud, tax administration or enforcement, money laundering, terrorism financing or serious crime’. A similar, but more restrictive, formulation would, in any event, be preferable to a simple list of the entities to which transfers can be made, which is the case in the current Regulation. For example, the formulation used in the Regulation with regard to account refusals might also be appropriate here, while still allowing sufficient flexibility for law enforcement and tax authorities: transfers thus could be restricted to cases when this is necessary and proportionate for purposes of investigation, detection and prosecution of 'fraud involving allowances or Kyoto units, money laundering, terrorist financing or other serious crimes for which the account may be an instrument'.

50. Further, with regard to access to 'anonymous transaction data for the purpose of looking for suspicious transaction patterns', it must be emphasized that the data will continue to be considered as 'personal data', and thus, subject to data protection law, so long as the individuals can be indirectly identified. The fact that some 'anonymization techniques' have been used, does not mean that the data are necessarily considered as 'anonymized' in the meaning of recital 26 of Directive 95/46/EC.[13] A dataset may contain personal data, and may possibly lead to identification of an individual even after direct identifiers have been removed and various additional anonymization techniques have been used.[14] Considering that data regarding account-holders are recorded and retained for 15 years in the Union Registry and EUTL, it is unlikely that during this retention period any data regarding the transactions can be considered truly anonymous in the sense of not being retraceable to the individuals who initiated those transactions. In addition, if the objective of this provision is to allow law enforcement to identify, after having found 'a suspicious transaction pattern', which account-holders followed that particular pattern, in order to investigate and prosecute these account-holders or the individuals who acted on their behalf, then this objective in itself is such that it requires subsequent identification of the individuals concerned.

51. The EDPS recommends that the Regulation be clarified to avoid any misunderstanding on this point. Safeguards should also be added, in the Regulation, and in any event, also at the practical level, to ensure the application of adequate anonymization techniques before any bulk transactional data are transferred for what essentially constitutes data mining. In addition to pseudo-anonymization (for example, by key-coding account-holders), additional anonymization techniques may need to be used if pseudo-anonymization itself is not effective enough, for example, because there is a likelihood that despite pseudo-anonymization the transactions may be linked to the same persons.[15]

52. The EDPS notes that with regard to anonymization, considering the direct access of Europol to the Union Registry and the EUTL, specific provisions should also be foreseen to ensure that Europol will only access personal data after adequate anonymization techniques have been applied.

53. Finally, the EDPS points out that the confidentiality requirement set forth in para 1 of Article 83 should not only apply to personal data held in the Union Registry and the EUTL, but also to all personal data held outside these databases, which are required to be processed under the Regulation. Confidentiality is important for the various personal data processed locally by national administrators and also for the data exchanged among national administrators and the Commission, importantly, but not only, with regard to the black-list referred to in paras 26 and further discussed in Section 10 below.

8. Publication of personal data on the Internet

[13] Recital 26, see notably: 'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person'.

[14] See pages 15 to 20 of the Opinion of the Article 29 Data Protection Working Party on the concept of personal data (WP 136). See also relevant provisions of a number of EDPS opinions, for example, Section 3.1 of the EDPS Prior Checking Opinion of 3 September 2010 on the European Surveillance System ('TESSy').

[15] See page 18 of the WP29 Opinion referred in footnote 14 above.

54. To help ensure transparency, the public part of the Union Registry website displays certain information including a limited amount of personal data (e.g. contact information) regarding account holders and their representatives. Some of the information is mandatory, some optional. Article 83(9) and (10) provide that account holders may opt-in or opt-out of the publication of certain personal data of their own or of their directors.

55. Indeed, each of Annexes II, IV, VI, VII, and XII specifies, item by item (i) what information is displayed on the Internet, (ii) what is not, (iii) what is displayed only if specifically requested (opt-in), and (iv) what is displayed unless specifically requested not to (opt-out).

56. The EDPS welcomes these clarifications and has no further comments as to which categories of data should be published and which ones should not, and what type of consent is required in each case.

57. The EDPS would, however, welcome a general provision in the Regulation that no personal data other than those specifically provided for in the Regulation will be made publicly available via the website.

9. Retention period

Introduction and general remarks

58. Article 81(1) of the Regulation provides that 'The Union Registry and every other [Kyoto Protocol] registry shall store records concerning all processes, log data and account holders for 15 years or until any questions of implementation relating to them have been resolved, whichever is later.'

59. The EDPS took notice that the data storage requirements were established in accordance with the Data Exchange Standards of the United Nations Framework Convention on Climate Change, agreed by all parties to the Kyoto Protocol including the EU and all the Member States of the EU.[16]

60. Nevertheless, the EDPS recommends that Article 81(1) be clarified further to remind that the data retention requirements are in accordance with EU data protection legislation, which requires that personal data should be kept 'no longer than is necessary for the purposes for which the data were collected or for which they are further processed'.[17]

61. In light of the data protection requirements, but also taking into account the international obligations under the Kyoto Protocol, the EDPS recommends that the Regulation more clearly define what categories of personal data must be retained for 15 years and for what categories of personal data this retention period does not apply.

62. In addition, for those categories of personal data to which this retention period does not apply (for example, because they are processed outside the Union Registry),

[16] See the Data Exchange Standards for Registry Systems under the Kyoto Protocol, Technical Specifications (Version 1.1.8), in particular, Section 7 on 'Data Logging Specifications' on page 66, available on-line at http://unfccc.int/files/kyoto_mechanisms/registry_systems/application/pdf/des_full_ver_1.1.8.pdf.
[17] Article 6(e) of Directive 95/46/EC.

adequate specific retention periods should be established or -when this is sufficient– the Regulation should at least require the establishment of adequate retention periods under national laws, in compliance with national provisions implementing Directive 95/46/EC.

Main concerns regarding data retention: sensitive data, including criminal records and data on suspected offences

63. In the analysis, the EDPS particularly recommends that the Commission should specifically address the issue of criminal record information (including any information or 'comment' indicated in the database as to the content of such criminal records, for example, on the occasion of refusal of account opening, or on the occasion of suspending an account). Under national law, criminal records are routinely deleted after set periods of time from the criminal records databases held by Member States. A blanket rule requiring the storage of information about the criminal records of an account-holder, or director, for fifteen years, which may be long after these records have been deleted from the criminal registry of the given Member State, would be excessive.

64. The EDPS also emphasises his concerns regarding the retention of data relating to account-holders, representatives or directors under investigations, especially if they have subsequently proved to be innocent. This may be the case, for example, if an entity's request to open an account was refused while it was under investigation for fraud involving allowances or Kyoto units. To illustrate: Article 20(2)(b) provides that a national administrator may refuse to open an account 'if the prospective account holder, or, if it is a legal person, any of the directors, is under investigation or has been convicted in the preceding five years for fraud involving allowances or Kyoto units, money laundering, terrorist financing or other serious crimes for which the account may be an instrument'. This is then complemented by Article 83(7), which requires that 'national administrators shall make available through secure means to all other national administrators and the central administrator the names and identities of persons for whom they refused to open an account in accordance with Article 20(2) ...'

65. Establishing adequate and non-excessive retention periods for such data are clearly necessary, whether the personal data are processed within the Union Registry or outside of it.

66. To address these concerns, the EDPS recommends that the Regulation specifically clarify the retention periods for sensitive data relating to account-holders and their representatives, including any criminal record data or data relating to investigations or suspicions. For example, the following provisions may be appropriate:

- for data that are collected and processed outside the EUTL and the Union Registry, the Regulation could provide that these shall be subject to proportionate retention periods specified in accordance with national provisions implementing Directive 95/46/EC;
- for the case if any sensitive data are processed within the Union Registry or the EUTL, or if any sensitive data are exchanged via another formalized data exchange mechanism among the national administrators and the central administrator, the Regulation should specifically establish adequate and non-excessive retention periods, after consultation with Member States. Establishment of a comprehensive and consistent framework for data retention is particularly important for the

periodically updated blacklists on account-holders or representatives suspected of criminal activities, which is foreseen under Article 83(7).

Secondary concerns

67. The need for retention for 15 years of long outdated addresses, phone numbers, passport numbers, or dates of birth of directors who no longer hold their positions in the companies in question is doubtful. For these and similar categories of data, shorter retention periods could presumably be specified.

Start of retention period

68. The EDPS also recommends that the Commission clarify when the retention periods start, for example, whether this will be as of the date of uploading the information on the electronic database.

10. Additional safeguards for data exchanges under Article 83(7): blacklisting account-holders and representatives for suspected or known criminal activities

69. The blacklists foreseen in Article 83(7)[18] require adequate data protection safeguards to be implemented at the practical level. In addition, the Regulation itself should also specify at least that:

- adequate notice should be provided to data subjects about the fact that they have been black-listed;
- a mechanism should be foreseen to accommodate data subjects' requests regarding access, rectification, blocking, or erasure;
- a mechanism should be foreseen to ensure that the information contained in the blacklist is accurate and up-to-date;
- all personal data should be deleted when their retention is no longer necessary (see also para 66 above);
- access to the blacklist should be clearly limited to national administrators and the central administrator and for specific purposes related to account management such as prevention of 'forum shopping' (any exceptions, if allowed, should be clearly stated in the Regulation and be adequately justified).

11. Data transfers to International Transaction Log

70. Article 6(1) provides that the Union Registry shall maintain a communication link with the United Nations Framework Convention on Climate Change (UNFCCC) International Transaction Log ('ITL') for the purposes of communicating transactions that transfer Kyoto units.

71. Article 6(1), in turn, provides that the EUTL shall also maintain a communication link with the ITL for the purposes of recording and checking transfers referred to under paragraph 1.

72. Considering these communication links, and thus, the exchange of data under these arrangements, the EDPS recommends that the Regulation clarify what, if any, personal data are transferred to the ITL. In any event, the EDPS recommends that

[18] See para 26 above.

the Regulation specifically provide that no special categories of data shall be transferred to the ITL.

73. For example, as noted in para 32, the fact whether an account opening was refused, or an account was suspended appears to be registered in the Union Registry. Combined with the name of the account holder, which may be a natural person, or with the names of the representatives of the account-holder (e.g. directors), this information may constitute sensitive personal data. The prohibition of transfer could apply to these and similar situations.

12. Data security

74. On security, Article 4(4) of the Regulation provides that '[t]he Union Registry shall conform to the functional and technical specifications for data exchange standards for registry systems under the Kyoto Protocol elaborated pursuant to Decision 12/CMP.1 and comply with the hardware, network, software and security requirements set out in the Data Exchange and Technical Specifications provided for in Article 79'.

    Article 79(2), in turn, provides that 'The Data Exchange and Technical Specifications shall be drawn up in consultation with the Administrators' Working Group of the Climate Change Committee and shall be consistent with the functional and technical specifications for data exchange standards for registry systems under the Kyoto Protocol elaborated pursuant to Decision 12/CMP.1.'

75. If the central administrator is/will be part of the Commission or another EU institution, agency or body, the EDPS recommends that a reference be also made to the relevant provisions of Regulation (EC) No 45/2001 (Articles 22 and 23).

76. In addition, the EDPS recommends that the Regulation itself should also contain a minimum set of security safeguards. These could include, for example, that:

- the Union Registry and the EUTL are operated in accordance with a system-specific security plan, developed after making a comprehensive risk assessment, and taking into account international standards and best practices in Member States, and
- the security plan and its implementation are periodically audited by an independent third party.

13. Conclusions

77. The EDPS recommends that the Regulation should, when it will be amended, as foreseen, later in 2012:

- clarify further what personal data are to be processed under the Regulation, and what personal data are stored and processed in the Union Registry and the EUTL. The EDPS would in particular welcome a general provision in the Regulation that no special categories of personal data shall be recorded in the EUTL and the Union Registry (Section 4);
- establish clearly whether the central administrator will be part of the European Commission, will be another EU institution/agency/body, or an entity organized under the laws of one of the Member States (Section 5);

- require the adoption of a data protection policy to allocate tasks and responsibilities (Section 6);
- define more specifically the purposes of access to data by third parties, including Europol, and provide adequate safeguards for anonymization in case of data mining (Section 7);
- prohibit publication of sensitive data (Section 8);
- be amended with regard to retention periods to ensure that the data retention requirements are in accordance with EU data protection legislation (Section 9);
- ensure that adequate notice should be provided to data subjects about the fact that they have been blacklisted and that a mechanism is available to ensure rights of access of data subjects and that the information contained in the blacklist is accurate and up-to-date; ensure adequate retention periods, limits on access and limits on the purposes for which the black-list may be used (Section 10);
- prohibit transfers of sensitive personal data outside the European Union, in particular, to the International Transaction Log (Section 11); and
- provide additional clarifications on security and accountability (audits) (Section 12).

78. In addition, the EDPS recommends that his comments be taken into account by the Commission and Member States when implementing the necessary data protection safeguards at the practical level. This may include adoption of a data protection policy, provision of information on the Union Registry website, other practical measures such as help menus and warning messages in the Union Registry, and provision of training materials.

Done in Brussels, 11 May 2012

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor