ISSN 1725-2423

Official Journal of the European Union

C 101

English edition

Information and Notices

Volume 54

1 April 2011

Notice No | Contents | Page

EN

Price: EUR 3

(Continued overleaf)

II *Information*

IV *Notices*

EN

([1]) Text with EEA relevance

(Continued on inside back cover)

I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the proposal for a Regulation on the marketing and use of explosives precursors

(2011/C 101/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Articles 7 and 8,

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

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 20 September 2010, the European Commission adopted a proposal for a Regulation on the marketing and use of explosives precursors [3] ('the Proposal'). On 11 November 2010, the Proposal as adopted by the Commission was sent to the EDPS for consultation in accordance with Article 28(2) of Regulation (EC) No 45/2001. The EDPS welcomes the fact that he is consulted by the Commission and that reference to this consultation is made in the recitals of the Proposal.

2. The main aim of the proposed measures is to reduce the risk of attacks by terrorists or other criminals using home-made explosive devices. To this end, the Regulation limits the access of the general public to certain chemicals, which can be misused as precursors to home-made explosives. In addition, the Proposal places the sales of such chemicals under stricter control by means of reporting suspicious transactions and thefts.

3. In this opinion, the EDPS calls the legislators' attention to a number of relevant data protection issues and provides recommendations to ensure the fundamental right to the protection of personal data.

II. ANALYSIS OF THE PROPOSAL AND RELEVANT DATA PROTECTION ISSUES

1. Measures proposed by the Commission

4. The Proposal addresses the problems of the misuse of certain chemicals, which are widely available to the general public on the market, as precursors to home-made explosives. Articles 4 and 5 of the Proposal deal with the prohibition of sale to the general public, which is combined with a licensing scheme and requirement to record all licensed transactions. Article 6 requires economic operators to report suspicious transactions and thefts. Finally, Article 7 addresses the need for data protection.

Articles 4 and 5: Prohibition of sale, licensing and recording of transactions

5. The sales of certain chemicals, above specified concentration thresholds, to members of the general public will be prohibited. Sales of higher concentrations would only be allowed to users who can document a legitimate need to use the chemical.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2010) 473.

6. The scope of the prohibition is limited to a short-list of chemical substances and their mixtures (see Annex I to the Proposal), and the sales of these substances to the general public. The restrictions do not apply to professional users or in business-to-business operations. Furthermore, the availability to the general public of the short-listed substances is limited only if they are above certain concentration levels. In addition, substances can still be obtained upon presentation of a license from a public authority (documenting legitimate use). Finally, an exception applies to farmers who are allowed to purchase ammonium nitrate to be used as fertiliser without a license irrespective of concentration thresholds.

7. Licenses will also be required if a member of the general public intends to import the short-listed substances to the European Union.

8. An economic operator which makes a substance or mixture available to a licensed member of the general public is required to verify the license presented and keep a record of the transaction.

9. Each Member State is required to lay down the rules for granting the license. The competent authority in the Member State shall refuse to grant the license to the applicant if there are reasonable grounds for doubting the legitimacy of the intended use. Licenses granted shall be valid in all Member Sates. The Commission may draw up guidelines on the technical details of the licenses to assist their mutual recognition.

Article 6: Reporting of suspicious transactions and thefts

10. The sales of a broader range of chemicals of concern (those listed in Annex II, in addition to all those listed in Annex I, which are already subject to the licensing requirement) will be subject to reporting of suspicious transactions and thefts.

11. The Proposal requires each Member State to designate a national contact point (with a clearly identified telephone number and e-mail address) for the reporting of suspicious transactions and thefts. Economic operators are required to report any suspicious transactions and thefts without delay, mentioning, if possible, the identity of the client.

12. The Commission shall draw up and update guidelines to assist the economic operators to recognize and notify suspicious transactions. The guidelines will also include regular updates to a list of additional substances not included in either Annex I or II, for which voluntary reporting of suspicious transactions and thefts is encouraged.

Article 7: Data protection

13. Recital 11 and Article 7 require that the processing of personal data under the Regulation must always be carried out in accordance with EU data protection laws, in particular, Directive 95/46/EC [4] and national data protection laws implementing this Directive. The Proposal contains no further provisions on data protection.

2. **More specific provisions are required to adequately protect personal data**

14. Reporting suspicious transactions and thefts and the licensing and recording scheme foreseen in the Regulation require processing of personal data. They both imply — in any case to some extent — interference with private life and the right to the protection of personal data, and thus require adequate safeguards.

15. The EDPS welcomes that the Proposal contains a separate provision (Article 7) on data protection. With that said, this single — and very general — provision foreseen in the Proposal is insufficient to adequately address the data protection concerns raised by the proposed measures. In addition, the relevant articles of the Proposal (Articles 4, 5 and 6) also fail to describe in sufficient detail the specificities of the data processing operations foreseen.

16. To illustrate, with regard to licensing, the Regulation requires that economic operators keep a record of the licensed transactions, without, however, specifying what personal data those records should contain, how long they should be kept, whom they can be disclosed to and under what conditions. Nor is it specified what data will be collected when processing license applications.

17. As for the requirement to report suspicious transactions and thefts, the Proposal establishes a reporting requirement, without, however, specifying what constitutes a suspicious transaction, what personal data should be reported, how long the information reported should be kept, whom it can be disclosed to and under what conditions. Nor does the Proposal provide further details regarding the 'national contact points' to be designated, or any database that these contact points may establish for their Member States, or any eventual database that might be established at EU level.

18. From a data protection point of view, the collection of data regarding suspicious transactions is the most sensitive subject in the Proposal. The relevant provisions should be clarified so as to ensure that the data processing remains proportionate and abuse is prevented. To achieve this, conditions for processing data should be clearly specified and adequate safeguards should be applied.

[4] Cited in footnote 1.

19. Importantly, data should not be used for any other purpose than the fight against terrorism (and other crime involving misuse of chemicals for home-made explosive devices). Data should also not be retained for long periods of time, especially if the number of potential or actual recipients were to be large, and/or if the data were to be used for data mining. This is even more important in those cases where it can be shown that the initial suspicion was unfounded. In those cases there needs to be a specific justification for further retention. By way of illustration, the EDPS mentions in this context the ruling of the European Court of Human Rights in the case of S and Marper v the United Kingdom (2008) ([5]), according to which the long term retention of the DNA of persons not convicted of a criminal offence was a breach of their right to privacy under Article 8 of the European Convention on Human Rights.

20. For these reasons, the EDPS recommends that Articles 5, 6 and 7 of the Proposal should contain further and more specific provisions to adequately address these concerns. Some specific recommendations will be made below.

21. In addition, it should also be considered whether specific and more detailed provisions can be drawn up in an implementing Commission Decision in accordance with Articles 10, 11 and 12 of the Proposal to address additional data protection issues at the practical level.

22. Finally, the EDPS also recommends that the Commission guidelines on suspicious transactions and on the technical details of the licenses should include further specific provisions on data processing and data protection. Both guidelines, as well as any possible implementing decision in the area of data protection, should be adopted after consulting the EDPS and — where the implementation at the national level is at stake — the Article 29 Data Protection Working Party. The Regulation itself should clearly foresee this and should also specifically list the main issues to be dealt with in the guidelines/implementing decision.

3. **Recommendations with respect to licensing and recording of transactions**

3.1. ***Recommendations for Article 5 of the Proposal***

Maximum retention period and categories of data collected

23. The EDPS recommends that Article 5 of the Regulation should specify a maximum retention period (*prima facie*, not exceeding two years) as well as the categories of personal data to be recorded (not exceeding name, license number and items purchased). These recommendations flow from the principle of necessity and proportionality: the collection and conservation of personal data should be limited to what is strictly necessary for the purposes pursued (see Article 6(c) and (e) of Directive 95/46/EC). If such specifications are left to national law or practice, this will probably lead to unnecessary uncertainties and unequal treatment of similar situations in practice.

Prohibition of collecting 'special categories of data'

24. Further, Article 5 of the Regulation should also expressly prohibit — in connection with the licensing procedure — the collection and processing of 'special categories of data' (as defined in Article 8 of Directive 95/46/EC) such as, among others, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs.

25. This should also help ensure that applicants will not be treated in a discriminatory way, for example, on account of their race, nationality or political or religious affiliation. In this context, the EDPS emphasizes that ensuring a high level of data protection is also a means contributing to fighting racism, xenophobia and discrimination, which, in turn, can contribute to preventing radicalisation and recruitment into terrorism.

3.2. ***Recommendations for the guidelines/implementing decision***

Data collected during the licensing process

26. The Regulation provides that license applications are to be rejected if there are reasonable grounds for doubting the legitimacy of the intended use. In this regard, it would be helpful if the guidelines or implementing decision specified the data that can be collected by the licensing authorities in connection with the license application.

Purpose limitation

27. The guidelines or implementing decision should provide that the records should only be disclosed to competent law enforcement authorities investigating terrorist activities or other suspected criminal abuse of explosive precursors. The information should not be used for any additional purposes (see Article 6(b) of Directive 95/46/EC).

Information to data subjects on recording of transactions (and on reporting of suspicious transactions)

28. The EDPS further recommends that the guidelines or implementing decision should specify that the licensing authority — who is best positioned to provide such a notice directly to the data subjects — should inform license holders about the fact that their purchases will be recorded and may be subject to reporting if found 'suspicious' (see Articles 10 and 11 of Directive 95/46/EC).

([5]) S. and Marper v the United Kingdom (December 4, 2008) (Application nos. 30562/04 and 30566/04).

4. Recommendations with respect to reporting of suspicious transactions and thefts

4.1. *Recommendations for Article 6 of the Proposal*

29. The EDPS recommends that the role and nature of the national contact points should be clarified in the Proposal. The Impact Assessment, in paragraph 6.33 refers to the possibility that these contact points may not only be 'law enforcement authorities' but also 'associations'. The legislative documents provide no further information in this regard. This should be, in particular, clarified in Article 6.2 of the Proposal. In principle, data should be held by law enforcement authorities — if this will not be the case, the reasons for this should be very clearly justified.

30. Furthermore, Article 6 of the Regulation should specify the personal data to be recorded (not exceeding name, license number, items purchased, and reasons giving rise to suspicion). These recommendations flow from the principle of necessity and proportionality: the collection of personal data should be limited to what is strictly necessary for the purposes pursued (see Article 6(c) of Directive 95/46/EC). In this context, similar considerations apply as expressed in point 23.

31. Article 6 of the Regulation should also expressly prohibit — in connection with the reporting procedure — the collection and processing of 'special categories of data' (as defined in Article 8 of Directive 95/46/EC) such as, among others, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs (see also points 24-25).

32. Finally, Article 6 should set a maximum retention period, taking into account the purposes of the data storage. The EDPS recommends that — unless a suspicious transaction or theft has led to a specific investigation and the investigation is still ongoing — all reported suspicious transactions and thefts should be deleted from the database after the lapse of a specified period (*prima facie*, at the latest two years following the date of report). This should help ensure that in cases where the suspicion has not been confirmed (or even investigated further), innocent individuals would not be kept on a 'black-list' and 'under suspicion' for an unduly long period of time (see Article 6(e) of Directive 95/46/EC). Too wide divergences on this point at the national level should in any case be avoided.

33. This limitation is also necessary to ensure the principle of data quality (see Article 6(d) of Directive 95/46/EC) as well as other important legal principles such as the presumption of innocence. This may not only result in a more adequate level of protection for the individuals, but at the same time, should also allow law enforcement to more effectively focus on those more serious cases where the suspicion will likely be ultimately confirmed.

4.2. *Recommendations for the guidelines/implementing decision*

Criteria for suspicious transactions should be defined

34. What transaction might be 'suspicious' is not defined in the Proposal. However, Article 6(6)(a) of the Proposal foresees that the Commission 'shall draw up and update guidelines' and shall provide information on 'how to recognize and notify suspicious transactions'.

35. The EDPS welcomes that the Proposal requires the Commission to draw up guidelines. These should be sufficiently clear and concrete and prevent an overbroad interpretation so as to minimize the transmissions of personal data to law enforcement authorities and to prevent any arbitrary or discriminatory practices, for example, on account of race, nationality or political or religious affiliation.

Purpose limitation, confidentiality, security, and access

36. The guidelines/implementing rules should further provide that the information should be kept secure and confidential and should only be disclosed to competent law enforcement authorities investigating terrorist activities or other suspected criminal abuse of explosive precursors. The information should not be used for additional purposes, for instance, to investigate unrelated matters by tax or immigration authorities.

37. The guidelines/implementing decision should further specify who should have access to the data received (and stored) by the national contact points. Access/disclosures should be limited on a strict need-to-know basis. Publication of a list of possible recipients should also be considered.

Rights of access to data subjects

38. The guidelines/implementing decision should provide for rights of access to data subjects, including, when appropriate, correction or deletion of their data (see Articles 12-14 of Directive 95/46/EC). The existence of this right — or any potential exceptions under Article 13 — may have important implications. For example, under the general rules, the data subject has also the right to know if his/her transaction has been reported as suspicious. The (potential) use of this right, however, could prevent the seller of explosives precursors to communicate suspicious transactions of the buyer. Therefore, any exceptions should be clearly justified and specifically set forth, preferably in the Regulation, or in any event, in the guidelines/implementing decision. A redress mechanism should also be foreseen, with the involvement of the national contact points.

5. **Additional comments**

Periodic review of effectiveness

39. The EDPS welcomes that Article 16 of the Proposal provides for a review of the Regulation (five years after adoption). Indeed, the EDPS is of the Opinion that any new instruments should prove in periodic reviews that they continue to constitute effective means of fighting terrorism (and other criminal activity). The EDPS recommends that the Regulation should specifically provide that during such a review, the Regulation's effectiveness, as well as its effects on fundamental rights, including data protection, should also be considered.

III. **CONCLUSIONS**

40. The EDPS recommends adding to the Proposal further, more specific provisions to adequately address data protection concerns. In addition, the Commission guidelines on suspicious transactions and on the technical details of the licenses — and an eventual implementing decision on data protection — should also include further specific provisions on data processing and data protection. The guidelines (and the implementing decision, if any) should be adopted after consulting the EDPS and — where appropriate — the Article 29 Working Party with representatives of data protection authorities in the Member States.

41. Article 5 of the Regulation should specify a maximum retention period (*prima facie*, not exceeding two years) for the recorded transactions as well as the categories of personal data to be recorded (not exceeding name, license number and items purchased). Processing of special categories of data should be expressly prohibited.

42. The role and nature of the contact points should be clarified in Article 6 of the Proposal. This provision should also specify a maximum retention period for the data reported on suspicious transactions (*prima facie*, not exceeding two years) as well as the personal data to be recorded (not exceeding name, license number, items purchased, and reasons giving rise to suspicion). Processing of special categories of data should be expressly prohibited.

43. Further, the guidelines/implementing decision should specify the data that can be collected by the licensing authorities in connection with the license application. They should also clearly limit the purposes for which data can be used. Similar provisions should also apply to the records of suspicious transactions. The guidelines/implementing decision should specify that the licensing authority should inform license holders about the fact that their purchases will be recorded and may be subject to reporting if found 'suspicious'. The guidelines/implementing decision should further specify who should have access to the data received (and stored) by the national contact points. Access/disclosures should be limited on a strict need-to-know basis. They should also provide for appropriate rights of access to data subjects and clearly set forth and justify any exceptions.

44. The effectiveness of the measures foreseen should be periodically reviewed, at the same time also considering their impact on privacy.

Done at Brussels, 15 December 2010.

Peter HUSTINX

European Data Protection Supervisor

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council — 'EU Internal Security Strategy in Action: Five steps towards a more secure Europe'

(2011/C 101/02)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Articles 7 and 8,

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 the request for an opinion in accordance with Regulation (EC) No 45/2001 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], in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 22 November 2010, the Commission adopted a Communication entitled 'EU Internal Security Strategy in Action: Five steps towards a more secure Europe' (hereinafter the 'Communication') [3]. The Communication was sent to the EDPS for consultation.

2. The EDPS welcomes the fact that he was consulted by the Commission. Already before the adoption of the Communication, the EDPS provided informal comments on the draft text, some of which have been taken into account in the final version of the Communication.

Context of the Communication

3. The EU Internal Security Strategy (hereinafter the ISS), addressed in the Communication, was adopted on 23 February 2010 under the Spanish Presidency [4]. The strategy lays out a European security model, which integrates among others action on law enforcement and judicial cooperation, border management and civil protection, with due respect for shared European values, such as fundamental rights. Its main objectives are to:

— present to the public the existing EU instruments that already help to guarantee the security and freedom of EU citizens and the added value that EU action provides in this area;

— further develop common tools and policies using a more integrated approach which addresses the causes of insecurity and not just the effects;

— strengthen law enforcement and judicial cooperation, border management, civil protection and disaster management.

4. The ISS aims to target the most urgent threats and challenges to EU security such as serious and organised crime, terrorism and cybercrime, the management of EU external borders and building resilience to natural and man-made disasters. The strategy provides for general guidelines, principles and directions on how the EU should react to these issues and it calls upon the Commission to propose timed actions to implement the strategy.

5. Furthermore, it is important to refer in this context to the recent Justice and Home Affairs Council Conclusions on the creation and implementation of an EU policy cycle for organised and serious international crime adopted on 8-9 November 2010 [5] (hereinafter 'November 2010 Conclusions'). This document follows the Council's Conclusion on the Architecture of Internal Security of 2006 [6], and calls upon the Council and the Commission to define a comprehensive ISS based on the EU common values and principles as reaffirmed in the EU Charter on Fundamental Rights [7].

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2010) 673 final.
[4] Doc. 5842/2/10.
[5] 3043rd Justice and Home Affairs Council meeting, 8-10 November 2010, Brussels.
[6] Doc. 7039/2/06 JAI 86 CATS 34.
[7] The EU policy cycle for serious international and organised crime addressed in the November 2010 Conclusions consists of four steps: 1) policy developments on the basis of a European Union Serious and Organised Crime Threat Assessment (EU SOCTA), 2) policy setting and decision-making through the identification by the Council of a limited number of priorities, 3) implementation and monitoring of annual Operational Action Plan (OAP) and 4) at the end of the policy cycle a thorough evaluation which will also serve as an input o the future policy cycle.

6. Amongst the directions and goals that should drive the implementation of the ISS, the November 2010 Conclusions refer to the reflection on a proactive and intelligence-led approach, stringent cooperation between the EU agencies, including further improving their information exchange and the aim of making citizens aware of the importance of the Union's work to protect them. Moreover, the Conclusions call the Commission to develop together with the experts of relevant agencies and Member States a Multi-Annual Strategic Plan (hereinafter MASP) for each priority, defining the most appropriate strategy to tackle the problem. It also calls on the Commission to develop through consultation with the Member States' and EU Agencies' experts an independent mechanism to evaluate the implementation of the MASP. The EDPS will come to these issues later on in this Opinion as they are closely linked or have significant impact on the protection of personal data, privacy and other related fundamental rights and freedoms.

Content and objective of the Communication

7. The Communication proposes five strategic objectives, all having links with privacy and data protection:

— disrupting international crime networks,

— preventing terrorism and addressing radicalisation and recruitment,

— raising levels of security for citizens and businesses in cyberspace,

— strengthening security through border management, and

— increasing Europe's resilience to crisis and disasters.

8. The *ISS in Action* as proposed in the Communication, puts forward a shared agenda for Member States, the European Parliament, the Commission, the Council, agencies and others, including civil society and local authorities, and proposes how they all should work together over the next four years to achieve the goals of the ISS.

9. The Communication builds on the Lisbon Treaty and acknowledges the guidance provided by the Stockholm Programme (and its Action Plan) which highlight in Chapter 4.1 the need for a comprehensive ISS based on respect for fundamental rights, international protection and the rule of law. Moreover, in accordance with the Stockholm Programme, developing, monitoring and implementing the internal security strategy should become one of the priority tasks of the Internal Security Committee (COSI) set up under Article 71 TFEU. In order to ensure the effective enforcement of the ISS, it should also cover security aspects of an integrated border management and, where appropriate, judicial cooperation in criminal matters relevant to operational cooperation in the field of internal security. It is also important to mention in this context that the Stockholm Programme calls for an integrated approach to ISS which should also take into account the external security strategy developed by the EU as well as other EU policies, in particular those concerning the internal market.

Aim of the Opinion

10. The Communication refers to various policy areas which form part of or have impact on a broadly understood concept of 'internal security' in the European Union.

11. The aim of this Opinion is not to analyze all policy areas and specific topics covered by the Communication, but to:

— look at the very objectives of the ISS proposed in the Communication from a specific perspective of privacy and data protection, and — from that angle — stress the necessary links with other strategies currently discussed and adopted at the EU level;

— specify a number of data protection notions and concepts which should be taken into consideration when designing, developing and implementing the ISS at EU level;

— provide, where useful and appropriate, suggestions on how data protection concerns could best be taken into account when implementing the actions proposed in the Communication.

12. The EDPS will do so by highlighting in particular the links between the ISS and the Information Management Strategy and the work on the comprehensive data protection framework. Moreover, the EDPS will refer to such concepts as: Best Available Techniques and 'Privacy by design', privacy and data protection impact assessment, and data subject's rights, which have direct impact on the design and implementation of the ISS. The Opinion will also comment on a number of chosen policy areas such integrated border management, including EUROSUR and the processing of personal data by FRONTEX, as well as other fields such as cyberspace and TFTP.

II. GENERAL COMMENTS

The need for a more comprehensive, inclusive and 'strategic' approach to EU strategies related to the ISS

13. Various EU strategies based on the Lisbon Treaty and the Stockholm programme and having a direct or indirect impact on data protection, are being currently discussed and proposed at EU level. The ISS is one of them and it is closely linked with other strategies (either addressed in recent Commission's Communications or envisaged for the near future) such as the EU Information Management Strategy and the European Information Exchange Model, the strategy on the implementation of the EU Charter of Fundamental Rights, the comprehensive data protection strategy and the EU Counter-terrorism policy. In this Opinion, the EDPS pays particular attention to the links with the Information Management Strategy and the comprehensive data protection framework based on Article 16 TFEU, which have most evident policy links with the ISS from a data protection perspective.

14. All these strategies constitute a complex 'patchwork' of interrelated policy guidelines, programmes and action plans which call for a comprehensive and integrated approach at EU level.

15. In more general terms, this approach of 'linking the strategies' if taken on board in the future actions would show that there is a vision at EU level when it comes to *EU strategies* and, that these strategies, and the recently adopted Communications which elaborate on them, are closely interlinked, which is the case, the Stockholm Programme being the common reference point for all of them. It would also result in positive synergies between different policies falling within the area of freedom, security and justice and would avoid any possible duplication of work and efforts in this area. Equally important, this approach would also lead to more effective and coherent application of data protection rules in the context of all interlinked strategies.

16. The EDPS highlights that one of the pillars of the ISS is an efficient information management in the European Union which should be grounded on the principles of necessity and proportionality in order to justify the need for exchange of information.

17. Moreover, as mentioned in the EDPS opinion on the Communication on Information Management ([8]), the EDPS underlines that all new legislative measures which would facilitate the storage and exchange of personal data should only be proposed if they are based on concrete evidence of their need ([9]). This legal requirement should be transformed into a pro-active policy approach when implementing the ISS. The need of a comprehensive approach to the ISS inevitably also leads to the need for assessment of all instruments and tools existing already in the field of internal security before proposing new ones.

18. In this context, the EDPS also suggests more frequent use of clauses providing for periodical evaluation of existing instruments, such as included in the Data Retention Directive which is currently being evaluated ([10]).

Data protection as an objective of ISS

19. The Communication refers to the protection of personal data in the paragraph 'Security policies based on common values' where it mentions that the tools and actions to be used to implement the ISS must be based on common values including the rule of law and respect of fundamental rights as laid down in the EU Charter of Fundamental Rights. In this context, it stipulates that 'Where efficient law enforcement in the EU is facilitated through information exchange, we must also protect the privacy of individuals and their fundamental right to protection of personal data'.

20. That is a welcome statement. However as such it cannot be considered as sufficiently addressing the issue of data protection in the ISS. The Communication neither elaborates on data protection ([11]) nor explains how respect for privacy and protection of personal data will be ensured in practice in the actions implementing the ISS.

([8]) Opinion of 30 September 2010 on the Communication from the Commission to the European Parliament and the Council — Overview of information management in the area of freedom, security and justice.

([9]) This is a legal requirement; see in particular ECJ Judgment in Joined Cases C-92/09 and C-93/09 of 2 November 2010. In more specific contexts, the EDPS has also advocated this approach in other opinions on legislative proposals related to the area of freedom, security and justice: e.g. Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II); Opinion of 20 December 2007 on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes; Opinion of 18 February 2009 on the Proposal for a Regulation concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…](establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third- country national or a stateless person); Opinion of 18 February 2009 on the Proposal for a Regulation establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person; and Opinion of 7 October 2009 on the proposals regarding law enforcement access to EURODAC.

([10]) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54).

([11]) Data protection in only mentioned more specifically in the context of the issue of the processing of personal data by FRONTEX.

21. According to the EDPS *ISS in Action* should have as one of its objectives a broadly understood *protection* which would ensure the *right* balance between on the one hand, the protection of citizens against the existing threats and, on the other hand, the protection of their privacy and the right to the protection of personal data. In other words, security and privacy concerns must be equally taken serious in the development of the ISS which would be in line with the Stockholm Programme and the Council Conclusions.

22. In short, providing security while fully respecting privacy and data protection should be mentioned as a very objective of the EU Internal Security Strategy. This should be reflected in all actions taken by Member States and EU institutions to implement the strategy.

23. In this context the EDPS refers to the Communication (2010) 609 on a comprehensive approach on personal data protection in the European Union. ([12]) The EDPS will soon issue an opinion on this Communication, but emphasises here that efficient ISS can not be put in place without the support of a solid data protection scheme complementing it and providing for mutual trust and better effectiveness.

III. NOTIONS AND CONCEPTS APPLICABLE TO THE DESIGN AND IMPLEMENTATION OF ISS

24. It is clear that some of the actions that derive from the ISS objectives may increase the risks for individuals' privacy and data protection. To counterbalance these risks, the EDPS would like to specifically draw attention to such concepts as 'Privacy by design', privacy and data protection impact assessment, data subject rights and best available techniques (BATs). All of them should be taken into account in the implementation of the ISS and can usefully contribute to more privacy friendly and data protection oriented policies in this field.

Privacy by design

25. The EDPS has advocated on various occasions and in various opinions the concept of 'built in' privacy ('Privacy by design' or 'Privacy by default'). This concept is currently developed both for the private and public sector, and therefore must also play an important role in the context of EU internal security and the area of police and justice ([13]).

26. The Communication does not mention this concept. The EDPS suggests that this concept is referred to in the targeted actions to be proposed and undertaken to implement the ISS, in particular in the context of Objective 4 'Strengthen security through border management' where there is clear mention of an enhanced use of new technologies for border checks and border surveillance.

Privacy and data protection impact assessment

27. The EDPS encourages the Commission to reflect — as part of the future work on the design and implementation of the ISS based on the Communication — on what should be meant by a real 'privacy and data protection impact assessment' (PIA) in the area of freedom, security and justice, and in particular in the ISS.

28. The Communication refers to threat and risk assessments. This is welcomed. However it does not — in any point — refer to privacy and data protection impact assessments. The EDPS believes that the work on the implementation of the Communication on ISS provides a good opportunity to elaborate such privacy and data protection impact assessments in the context of internal security. The EDPS notes that neither the Communication nor the Commission's Impact Assessment Guidelines ([14]) specifies this aspect and develops it into a policy requirement.

29. Therefore, the EDPS recommends that in the implementation of future instruments a more specific and rigorous impact assessment on privacy and data protection is conducted, either as a separate assessment or as part of the general fundamental rights' impact assessment carried out by the Commission. This impact assessment should not only state general principles or analyze policy options, as it is the case currently, but should also recommend specific and concrete safeguards.

30. Consequently, specific indicators and features should be developed to ensure that each proposal having impact on privacy and data protection in the field of EU Internal Security is subject to thorough consideration, including such aspects as proportionality, necessity and purpose limitation principle.

31. Additionally, it could be helpful in this context to refer to Article 4 of the RFID Recommendation ([15]) in which the Commission called upon the Member States to ensure that industry, in collaboration with relevant civil society

([12]) Communication from the Commission to the European Parliament, the Council and the European and Social Committee and the Committee of Regions on a comprehensive approach on data protection in the European Union, COM(2010) 609.

([13]) The EDPS in his opinion on the Commission's Communication on the Stockholm Programme recommended that there should be a legal obligation for builders and users of information systems to develop and use systems which are in accordance with the principle of 'Privacy by design'.

([14]) SEC(2009) 92, 15.1.2009.

([15]) C(2009) 3200 final, 12.5.2009.

stakeholders, develops a framework for privacy and data protection impact assessments. Furthermore, the Madrid Resolution, adopted in November 2009 by the International Conference of Privacy and Data Protection Commissioners, encouraged the implementation of PIAs prior to the implementation of new information systems and technologies for the processing of personal data or substantial modifications in existing processing.

Data subjects' rights

32. The EDPS notes that the Communication does not address specifically the issue of the data subjects' rights which constitute a vital element of data protection and should have impact on the design of ISS. It is essential to ensure that across all different systems and instruments dealing with EU internal security, the persons subject to them enjoy similar rights relating to how their personal data are processed.

33. Many of the systems referred to in the Communication establish specific rules on data subjects' rights (targeting also such categories of persons as victims, suspected criminals or migrants), but there is a lot of variation between the systems and instruments, without good justification.

34. Therefore, the EDPS invites the Commission to look more carefully into the issue of the alignment of data subjects' rights in the EU in the context of the ISS and Information Management Strategy in the near future.

35. Particular attention should be paid to redress mechanisms. The ISS should guarantee that whenever individuals' rights have not been fully respected, data controllers should provide for complaints procedures which are easily accessible, effective and affordable.

Best Available Techniques

36. The implementation of the ISS will inevitability build upon the use of an IT infrastructure that will support the actions envisaged in the Communication. Best Available Techniques (BATs) can be seen as enablers of the correct balance between the achievement of the objectives of the ISS and respect of the rights of individuals. In the present context, the EDPS would like to reiterate the recommendation made in previous opinions ([16]) regarding the need for the Commission to define and promote together with industry stakeholders concrete measures for the application of BATs. Such application means the most effective and advanced stage in the development of activities and their methods of operation, which indicate the practical suitability of particular techniques for providing the results envisioned in an efficient way and in compliance with the privacy and data protection EU framework. This approach is fully in line the 'privacy by design' approach, mentioned before.

37. Where relevant and feasible, reference documents on BATs should be elaborated to provide guidance and greater legal certainty for the actual implementation of the measures framed by the ISS. This could also promote the harmonisation of such measures throughout the different Member States. Last but not least, the definition of privacy and security friendly BATs will facilitate the supervisory role of Data Protection Authorities by providing them with privacy and data protection compliant technical references adopted by data controllers.

38. The EDPS also notes the importance of a correct alignment of the ISS with the activities already carried out under the seventh Framework Programme for Research and Technological Development and the Security and Safeguarding Liberties Framework Program. A joint vision pursuing to provide BATs will enable the innovation in the knowledge and capabilities required to protect citizens while respecting fundamental rights.

39. Finally, the EDPS points to the role which European Network and Information Security Agency (ENISA) can play in the elaboration of guidelines and the assessment of the security capabilities required to ensure the integrity and availability of the IT systems, and also in the promotion of these BATs. With regard to this, the EDPS welcomes the inclusion of the Agency as key player in the improvement of capabilities for dealing with cyber attacks and fighting against cybercrime ([17]).

Clarification of actors and their roles

40. In this context, more clarification is also needed when it comes to the actors which form part of or contribute to the ISS architecture. The Communication refers to various actors and stakeholders such as citizens, judiciary, EU agencies, national authorities, police, and business. The

([16]) EDPS Opinion on Intelligent Transport systems, of July 2009 and EDPS Opinion on the RFID Communication of December 2007, see also EDPS Annual Report 2006, p. 48.

([17]) The EDPS envisages adopting an opinion on the legal framework of ENISA, still in December 2010.

specific roles and competences of these actors should be better addressed in the specific actions to be proposed in the implementation of the ISS.

IV. SPECIFIC COMMENTS ON POLICY FIELDS RELATED TO ISS

Integrated border management (IBM)

41. The Communication refers to the fact that with the Lisbon Treaty, the EU is better placed to exploit synergies between border management policies on persons and goods. In relation to movement of persons, it mentions that 'the EU can treat migration management and the fight against crime as twin objectives of the integrated border management strategy'. The document perceives border management as a potentially powerful means of disrupting serious and organised crime ([18]).

42. The EDPS also notes that the Communication identifies three strategic strands: 1) an enhanced use of new technology for border checks (the SIS II, VIS, entry/exit system and registered traveller programme); 2) an enhanced use of new technology for border surveillance (European Border Surveillance System, EUROSUR) and 3) an enhanced coordination of Member States through FRONTEX.

43. The EDPS wishes to use the opportunity of this Opinion to recall his requests made in a number of previous opinions that a clear policy on border management — fully respecting data protection rules — is established at EU level. The EDPS believes that the current work on the ISS and Information Management are very good occasions to take more concrete steps towards a coherent policy approach to these areas.

44. The EDPS notes that the Communication does not only refer to the existing large scale-systems and those that might be put in operation in the near future (such as SIS, SIS II and VIS), but — in the same lines — also to the systems that might be proposed by the Commission in the future but the decision on which has not been taken yet (i.e. Registered Travellers Programme (RTP) and Entry/exit system). It should be recalled in this context that the objectives and legitimacy of the introduction of these systems still need to be clarified and demonstrated, also in light of the results of specific impact assessments carried out by the Commission. If this does not happen, the Communication can be read as anticipating the decision making process, and consequently not taking into account the fact that the final decision on whether the RTP and the entry/exit system should be introduced in the European Union has not yet been taken.

45. The EDPS therefore suggests that in the future work on the implementation of the ISS, such anticipations are avoided. As mentioned earlier, any decision on the introduction of new privacy intrusive large-scale systems should only take place after an adequate evaluation of all existing systems has taken place, with due regard to necessity and proportionality.

EUROSUR

46. The Communication mentions that the Commission will present a legislative proposal to set up EUROSUR in 2011 to contribute to internal security and the fight against crime. It is also mentioned that EUROSUR will make use of new technologies developed through EU funded research projects and activities, such as satellite imagery to detect and track targets at the maritime border, e.g. tracing fast vessels transporting drugs to the EU.

47. In this context, the EDPS notes that it is not clear whether and if so to which extent the legislative proposal on EUROSUR to be presented by the Commission in 2011 will also envisage the processing of personal data in the context of EUROSUR. The Commission has not taken a clear position on this in the Communication. This issue is even more relevant given that the Communication makes clear links between EUROSUR and FRONTEX at tactical, operational and strategic level (see comments below on FRONTEX) and asks for close cooperation between the two.

The processing of personal data by FRONTEX

48. The EDPS has issued an opinion on the revision of the FRONTEX Regulation on 17 May 2010 ([19]) in which he called for real debate and in-depth reflection on the issue of data protection in the context of strengthening the existing tasks of FRONTEX and granting it new responsibilities.

49. The Communication refers to the need to enhance the contribution of FRONTEX at the external borders under Objective 4 *Strengthen security through border management*. In this context, the Communication mentions that based on experience and in the context of the EU overall

([18]) Press release on the EU Internal Security Strategy in Action — five steps towards a more secure Europe Memo 10/598.

([19]) EDPS Opinion of 17 May 2010 on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX).

approach to information management, the Commission considers that enabling FRONTEX to process and use this information, with a limited scope and in accordance with clearly defined personal data management rules, will make a significant contribution to dismantling criminal organisations. This is a new approach compared to the Commission proposal on the revision of the FRONTEX Regulation, currently subject to discussion in the European Parliament and the Council, which was silent about processing of personal data.

50. Against this background, the EDPS welcomes the fact that the Communication provides for some indication as to the circumstances when such processing might prove necessary (e.g. risk analysis, better performance of joint operations or exchange of information with Europol). More specifically, the Communication explains that currently the information on criminals involved in trafficking networks — which FRONTEX comes across — cannot be further used for risk analysis or better targeting future joint operations. Moreover, relevant data on suspected criminals do not reach the competent national authorities or Europol for further investigations.

51. Nevertheless, the EDPS notes that the Communication does not refer to the ongoing discussion on the revision of the FRONTEX legal framework which, as mentioned earlier, tackles this issue in order to provide for legislative solutions. Moreover, the wording of the Communication emphasising the role of FRONTEX in the context of the objective to dismantle criminal organisations, can be read as broadening the mandate of FRONTEX. The EDPS suggests that this point is taken into account both in the revision of the FRONTEX Regulation and in the implementation of ISS.

52. The EDPS also draws attention to the need to ensure that there is no duplication of tasks between Europol and FRONTEX. In that context, the EDPS welcomes that the Communication mentions that duplication of tasks between FRONTEX and Europol should be avoided. However, this issue should also be more clearly addressed both in the revised FRONTEX Regulation and in the actions implementing the ISS which provide for close cooperation between FRONTEX and EUROPOL. This is of particular importance from the point of view of the principles of purpose limitation and data quality. This remark also applies to the future cooperation with such agencies as the European network and Information Security Agency (ENISA) or the European Asylum Support Office.

The use of biometrics

53. The Communication does not address specifically the current phenomenon of the increased use of biometric data in the area of freedom, security and justice, including the EU large-scale IT systems and other border management tools.

54. The EDPS therefore takes this opportunity to recall his suggestion ([20]) that this matter of high sensitivity from the perspective of data protection is taken seriously into account in the implementation of the ISS, in particular in the context of border management.

55. The EDPS also recommends that a clear and strict policy on the use of biometrics in the area of freedom, security and justice based on a serious evaluation and a case-by-case assessment of the need for the use of biometrics in the context of the ISS, with full respect for such fundamental data protection principles as proportionality, necessity and purpose limitation, is developed.

TFTP

56. The Communication announces that the Commission will develop in 2011 a policy for the EU to extract and analyse financial messaging data held on its own territory. In this context, the EDPS refers to his Opinion of 22 June 2010 on processing and transfer of Financial Messaging Data from the EU to the US for purposes of the Terrorist Finance Tracking Programe (TFTP II) ([21]). All critical remarks expressed in that Opinion are equally valid and applicable in the context of the envisaged work on a EU framework on financial messaging data. Therefore, they should be taken into account in the discussions on this issue. Particular attention should be paid to the proportionality of extracting and processing large amounts of data on people who are not suspects, and to the issue of effective oversight by independent authorities and by the judiciary.

Security for citizens and business in cyberspace

57. The EDPS welcomes the importance attached in the Communication to preventive actions at EU level and is of the view that the strengthening of security in IT networks is an essential factor contributing to a well-functioning information society. Also, the EDPS supports the specific activities improving capacities to deal with cyber attacks, building capacities in law enforcement and judiciary bodies, and creating partnerships with the industry to empower citizens and business. Also, ENISA's role as facilitator of many of the actions provided in this objective is welcome.

([20]) See in particular EDPS Opinion on the Communication on the overview of information management in the AFSJ mentioned in footnote 8.

([21]) EDPS Opinion of 22 June 2010 on the Proposal for a Council Decision on the conclusions of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to United States for the purposes of Terrorist Finance Tracking Programme (TFTP II).

58. However, the *ISS in Action* does not elaborate on law enforcement actions envisaged in cyberspace, how these activities could put individual rights at risk and what the required safeguards should be. The EDPS calls for a more ambitious approach on appropriate guarantees; this approach should be set forth to protect the fundamental rights of all individuals, including those who may be affected by actions designed to counter any possible criminal activities in this area.

V. **CONCLUSION AND RECOMMENDATIONS**

59. The EDPS asks for linking various EU strategies and Communications in the process of the implementation of the ISS. This approach should be followed by a concrete action plan supported by a real assessment of needs, the outcome of which should be a comprehensive, integrated and well-structured EU policy on ISS.

60. The EDPS also takes this opportunity to highlight the importance of the legal requirement of a real assessment of all existing instruments to be used in the context of the ISS and information exchange before proposing new ones. In this context, the inclusion of provisions requiring regular assessments of the efficiency of relevant instruments is highly recommended.

61. The EDPS suggests that in the preparation of the Multi-Annual Strategic Plan requested by the November 2010 Council Conclusions, account is taken of the ongoing work on the comprehensive data protection framework on the basis of Article 16 TFEU, in particular Communication (2009) 609.

62. The EDPS makes a number of suggestions on notions and concepts relevant from a data protection perspective which should be taken into account in the field of ISS, such as Privacy by design, Privacy and Data Protection Impact Assessment, Best Available Techniques.

63. The EDPS recommends that in the implementation of future instruments an impact assessment on privacy and data protection is conducted, either as a separate assessment or as part of the general fundamental rights' impact assessment carried out by the Commission.

64. He also invites the Commission to develop a more coherent and consistent policy on the prerequisites for use of biometrics in the field of ISS, and more alignment at EU level in terms of data subjects' rights.

65. The EDPS finally makes a number of comments on the processing of personal data in the context of border management and in particular by FRONTEX and possibly in the context of EUROSUR.

Done at Brussels, 17 December 2010.

Peter HUSTINX

European Data Protection Supervisor

Opinion of the European Data Protection Supervisor on the Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person)

(2011/C 101/03)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

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

HAS ADOPTED THE FOLLOWING OPINION

I. INTRODUCTION

1. On 11 October 2010, the European Commission adopted an Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) ('the Proposal') [3]. On the same day, the Proposal as adopted by the Commission was sent to the EDPS for consultation in accordance with Article 28(2) of Regulation (EC) No 45/2001. The EDPS welcomes the fact that he is consulted by the Commission and asks that reference to this consultation is made in the recitals of the Proposal.

2. Eurodac was established by Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention [4]. A recast proposal for the amendment of the Eurodac Regulation was adopted by the Commission in December 2008 [5] (hereafter the December 2008 proposal). The EDPS commented on that proposal in an opinion of February 2009 [6].

3. The December 2008 proposal was designed to ensure a more efficient support to the application of the Dublin Regulation and to properly address data protection concerns. It also aligned the IT management framework to that of the SIS II and VIS Regulations by providing for the taking over of the tasks of the operational management for Eurodac by the future Agency for the operational management of large-scale IT systems in the area of freedom, security and justice [7] (hereinafter: IT Agency) [8].

4. The Commission then adopted an amended proposal in September 2009 in which it introduced the possibility for Member States' law enforcement authorities and Europol to access the Eurodac central database for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2010) 555 final.
[4] OJ L 62, 5.3.2002, p. 1.
[5] Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), COM(2008) 825 final.
[6] Opinion of 18 February 2009 on the Proposal for a Regulation concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) (COM(2008) 825), OJ C 229, 23.9.2009, p. 6.
[7] The Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (COM(2009) 293 final) was adopted on 24 June 2009. An amended proposal was adopted on 19 March 2010: Amended proposal for a Regulation (EU) No …/… of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, COM(2010) 93.
[8] The EDPS issued an opinion on the establishment of the IT Agency (Opinion of 7 December 2009 on the proposal for a Regulation establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and on the proposal for a Council Decision conferring upon the Agency tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty, OJ C 70, 19.3.2010, p. 13).

5. In particular, that proposal introduced a bridging clause to allow access for law enforcement purposes as well as the necessary accompanying provisions and amended the December 2008 proposal. It was presented at the same time as a Proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes [1] (hereafter: the Council Decision), spelling out the exact modalities of such access. The EDPS issued an opinion on this proposal in December 2009 [2].

6. With the entry into force of the Lisbon Treaty and the abolition of the pillar system, the proposal for a Council Decision lapsed; it had to be formally withdrawn and replaced with a new proposal to take account of the new framework of the TFEU.

7. The Explanatory Memorandum to the Proposal states that, with a view to progressing on the negotiations on the asylum package [3] and facilitating the conclusion of an agreement on the Eurodac Regulation, the Commission has found it more appropriate to withdraw from the Eurodac Regulation those provisions referring to the access for law enforcement purposes.

8. The Commission also considers that withdrawing that (rather controversial) part of the proposal and enabling thereby the swifter adoption of the new Eurodac Regulation will also facilitate the timely set up of the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, since that Agency is planned to be also responsible for the management of Eurodac.

9. As a consequence, while the present amended proposal introduces two technical provisions, its main purpose is to amend the previous proposal (i.e. from September 2009) by deleting from it the option of access for law enforcement purposes. It was therefore not considered necessary to conduct a new impact assessment specifically for the present proposal.

[1] COM(2009) 344.

[2] Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, OJ C 92, 10.4.2010, p. 1.

[3] The 'asylum package' aims at improving the way the EU asylum system works and strengthens asylum seekers' rights. It contains amendments to the Reception Conditions Directive (RCD), the Dublin Regulation and Eurodac. It also foresees the creation of a European Asylum Support Office (EASO) accompanied by a decision which facilitates the funding of the EASO by redeploying some of the funds currently allocated to the European Refugee Fund.

II. FOCUS OF THE OPINION OF THE EDPS

10. The EDPS has already contributed several opinions in this area, as mentioned above. The purpose of the present opinion is to recommend improvements to the proposal; these recommendations are either based on new developments or on recommendations previously made and not yet taken on board, in situations where the EDPS finds that his arguments have not been met adequately or that these recommendations are supported by new arguments.

11. The present opinion will focus on the following points:

— the withdrawal of the provisions related to law enforcement access to Eurodac,

— the position of the individual whose fingerprints are not usable,

— information of the data subject,

— use of best available techniques as a way to implement 'Privacy by Design',

— consequences of subcontracting (a part of) the development or management of the system to a third party.

III. WITHDRAWAL OF PROVISIONS ON LAW ENFORCEMENT ACCESS

12. The EDPS welcomes the fact that the possibility to give law enforcement an access to Eurodac has been left out of the current proposal. Indeed, while the EDPS does not dispute that governments need appropriate instruments to guarantee the security of the citizen, he had expressed strong doubts as to the legitimacy of this proposal, based on the following considerations.

13. Measures to combat terrorist offences and other serious offences can be a legitimate ground to allow processing of personal data — even if incompatible with the purposes for which the data were originally collected — provided that the necessity of the intrusion is supported by clear and undeniable elements, and the proportionality of the processing is demonstrated. This is all the more required since the proposals concern a vulnerable group in need of higher protection because they flee from persecution. Their precarious position has to be taken into account in the assessment of the necessity and proportionality of the proposed action. The EDPS emphasised, more concretely, that the necessity should be proven by the demonstration of substantial evidence of a link between asylum applicants and terrorism and/or serious crime. This had not been done in the proposals.

14. On a more general level, the EDPS has advocated the need for assessment of all existing instruments on information exchange before proposing new ones in numerous opinions and comments, and with particular emphasis in the recent opinions on the 'Overview of information management in the area of freedom, security and justice' ([1]) and on 'the EU Counter-Terrorism Policy: main achievements and future challenges' ([2]).

15. Indeed, assessing the effectiveness of existing measures while considering the impact on privacy of new envisaged measures is crucial and should vest an important role in European Union's action in this area, in line with the approach put forward by the Stockholm Programme. In this case, special attention should for instance be devoted to the implementation of exchange of data under the Prüm mechanism. Exchange of fingerprints is foreseen in this context, and it should be demonstrated that the system has severe insufficiencies which justifies the access to a database such as Eurodac.

16. Finally, in these opinions as in many others before, the EDPS recommends that special attention be paid to those proposals resulting in collections of personal data of broad categories of citizens, rather than only suspects. Specific consideration and justification should also be given to those cases where processing of personal data is foreseen for purposes other than those for which they were initially collected, such as in Eurodac.

17. In conclusion, the EDPS welcomes the deletion of this element from the current proposal.

IV. **POSITION OF INDIVIDUALS WHO CANNOT ENROL**

18. The collection and further processing of fingerprints obviously occupy a central place in the Eurodac system. It should be emphasized that the processing of biometric data such as fingerprints poses specific challenges and creates risks which have to be addressed. In the context of the Proposal, the EDPS wants to specifically underline the problem of so-called 'failure to enrol' — the situation in which a person finds him/herself if for some reason, their fingerprints are not usable.

19. Failure to enrol may occur when individuals have temporarily or permanently damaged fingertips or hands. This may be due to various factors, such as illness, disability, wounds and burns. It can also in some cases, be linked to ethnicity or occupation. In particular, it seems that a non-trivial number of agricultural and construction workers have fingerprints which are damaged to the point of being unreadable. In other cases, the frequency of which is difficult to evaluate, it may happen that refugees self-mutilate, in order to avoid being fingerprinted.

20. The EDPS recognises that it can be difficult to distinguish those third country nationals who have voluntarily damaged their fingerprints to frustrate the identification process from those with genuinely unreadable fingerprints.

21. It is however extremely important to ensure that 'failure to enrol' on its own does not lead to a denial of rights for asylum seekers. It would not be acceptable, for instance, that failure to enrol would be construed systematically as an attempt to fraud and would lead to a refusal to examine an asylum application or a withdrawal of assistance to the asylum seeker. If it were the case, it would mean that the possibility to be fingerprinted would be one of the criteria to recognise the status of asylum seeker. The purpose of Eurodac is to facilitate the application of the Dublin Convention, and not to add a criterion ('having usable fingerprints') for granting someone the status of asylum seeker. This would be a violation of the purpose limitation principle, and of at least the spirit of the right to asylum.

22. Finally, the EDPS also insists that the present proposal should be consistent with the other directives relevant in this area. In particular, the 'Qualification Directive' insists that each application shall be considered on its own merit, and does certainly not mention the impossibility to enrol as a criterion for examining the asylum application ([3]).

23. The current proposal already envisages partly the failure to enrol in its Articles 6.1 and 6.2 ([4]).

([1]) EDPS Opinion of 30 September 2010 on the Communication from the Commission to the European Parliament and the Council — 'Overview of information management in the area of freedom, security and justice', available on the website.

([2]) EDPS Opinion of 24 November 2010 on the Communication from the Commission to the European Parliament and the Council concerning the EU Counter-Terrorism Policy: main achievements and future challenges, available on the website.

([3]) See in particular Article 4(3) of the Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted, OJ L 304, 30.9.2004, p. 12.

([4]) '1. Where the condition of the fingertips does not allow to take the fingerprints in a quality ensuring appropriate comparison under Article 18 of this Regulation, the Member State of origin shall retake the fingerprints of the applicant and resend them as soon as possible and no later than 48 hours after they have been successfully taken.' '2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant or the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail'.

24. However, these provisions only envisage the hypothesis of temporary failure to enrol, whereas in a significant number of cases this impossibility will be permanent. Article 1 of the Regulation amending the Common Consular Instructions [1] provides for such cases and stipulates that: '(…) Member States shall ensure that appropriate procedures guaranteeing the dignity of the applicant are in place in the event of there being difficulties in enrolling. The fact that fingerprinting is physically impossible shall not influence the grant or refusal of a visa'.

25. In order to cater for these cases in the context of Eurodac, the EDPS recommends adding to Article 6 a provision inspired by this, along the following line: 'Temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of the individual. In any case, it can not represent sufficient grounds to refuse to examine or to reject an asylum application'.

V. **RIGHT OF INFORMATION TO THE DATA SUBJECT**

26. The EDPS notes that effective implementation of the right to information is crucial for the proper functioning of Eurodac. In particular, it is essential to ensure that information is provided in a way that enables the asylum seeker to fully understand his situation as well as the extent of the rights, including the procedural steps he/she can take as follow-up to the administrative decisions taken in his/her case. The EDPS also reminds that the right of access is a cornerstone of data protection, as mentioned in particular in Article 8 of the EU Charter of Fundamental Rights.

27. The EDPS had already underlined this item in his previous opinion on Eurodac. Since the proposed modification has not been accepted, the EDPS wants to emphasize the importance of this question.

28. Article 24 of the Proposal reads as follows:

'A person covered by this Regulation shall be informed by the Member State of origin in writing, and where appropriate, orally, in a language which he or she understands or may reasonably be presumed to understand of the following:

(…)

(e) the existence of the right of access to data relating to him/her, and the right to request that inaccurate data relating to him/her be corrected or that unlawfully processed data relating to them be erased, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the National Supervisory Authorities referred to in Article 25(1).'

29. The EDPS suggests that the wording of Article 24 should be reformulated to clarify the rights to be given to the applicant. The wording as proposed is unclear, as it can be interpreted as considering 'the right to receive information on the procedures for exercising those rights (…)' apart from the right of access to data and/or the right to request inaccurate data be corrected (…). Moreover, according to the current wording of the above-mentioned provision, the Member States are to inform the person covered by the Regulation not of the content of the rights but of their 'existence'. As the latter seems to be only a stylistic issue, the EDPS suggests that Article 24 be redrafted as follows: 'A person covered by this Regulation shall be informed by the Member State of origin (…) of (…)(g) the right of access to data relating to him/her, and the right to request that inaccurate data relating to him/her be corrected or that unlawfully processed data relating to him/her be deleted'.

VI. **BEST AVAILABLE TECHNIQUES**

30. Article 4(1) of the Proposal stipulates: 'After a transitional period, a Management Authority, funded from the general budget of the European Union, shall be responsible for the operational management of Eurodac. The Management Authority shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for the Central System'. Although the EDPS welcomes the requirement laid down in Article 4(1), he wishes to note that the expression 'best available technology' referred to in the above-mentioned provision, should be replaced with the wording 'best available techniques' which includes both the technology used and the way in which the installation is designed, built, maintained and operated.

31. This is important because the concept of 'best available techniques' is broader and covers various aspects contributing to the application of 'Privacy by Design' which is considered a key principle in the review of the EU data protection legal framework. It underlines that data protection can be implemented through different means, not all of a technological nature. It is indeed important to examine not only the technology but also the way the technology is used as a tool to achieve the purpose of the data processing at hand. Business processes must be oriented toward the achievement of this purpose which is translated into procedures and organisational structures.

[1] Regulation (EC) No 390/2009 of The European Parliament and of The Council of 23 April 2009 amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications, OJ L 131, 28.5.2009, p. 1.

32. In this regard, and on a more general level, the EDPS would like to reiterate the recommendation made in previous opinions [1] regarding the need for the Commission to define and promote together with industry stakeholders 'Best Available Techniques' following the same procedure adopted by the Commission in the environmental field [2]. 'Best Available Techniques' would mean the most effective and advanced stage in the development of technology and their methods of operation which indicate the practical suitability of particular techniques for providing, in compliance with the privacy and data protection EU framework, a defined detection threshold. These BATs will be designed to prevent and, where that is not practicable, to mitigate to an appropriate level the security risks related to this data processing and minimize as much as possible their impact on privacy.

33. This process should also provide reference documents on 'Best Available Techniques' which may offer very useful guidance for the management of other EU large-scale IT systems. It will also enhance the harmonisation of such measures throughout the EU. Last but not least, the definition of privacy and security friendly BATs will facilitate the supervisory role of Data Protection Authorities by providing them privacy and data protection compliant technical references adopted by data controllers.

VII. **SUBCONTRACTING**

34. The EDPS notes that the Proposal does not address the issue of subcontracting parts of the tasks of the Commission [3] to another organisation or entity (such as a private company). Nevertheless, subcontracting is commonly used by the Commission in the development and management both of the system and the communication infrastructure. While subcontracting of activities does not in itself run contrary to data protection requirements, important safeguards should be put in place to ensure that the applicability of Regulation (EC) No 45/2001, including the data protection supervision by the EDPS, remains entirely unaffected by the subcontracting. Furthermore, additional safeguards of a more technical nature should also be adopted.

35. In this regard, the EDPS suggests that similar legal safeguards as envisaged in the SIS II legal instruments should be provided *mutatis mutandis* in the framework of the revision of the Eurodac Regulation, specifying that even when the Commission subcontracts a part of its tasks to another body or organisation, it shall ensure that the EDPS has the right and is able to fully exercise his tasks, including carrying out on-the-spot checks and to exercise any other powers conferred on him by Article 47 of Regulation (EC) No 45/2001.

VIII. **CONCLUSIONS**

36. The EDPS welcomes the fact that he is consulted by the Commission and asks that reference to this consultation is made in the recitals of the Proposal.

37. The EDPS welcomes the fact that the possibility to give law enforcement an access to Eurodac has been left out of the current proposal.

38. The collection and further processing of fingerprints occupy a central place in the Eurodac system. The EDPS emphasizes that the processing of biometric data such as fingerprints poses specific challenges and creates risks which have to be addressed. In particular, the EDPS underlines the problem of so-called 'failure to enrol' — the situation in which a person finds him/herself if for some reason, their fingerprints are not usable. Failure to enrol on its own should not lead to a denial of rights for asylum seekers.

39. The EDPS recommends adding to Article 6a of the proposal a provision along the following line: 'Temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of the individual. In any case, it can not represent sufficient grounds to refuse to examine or to reject an asylum application'.

40. The EDPS notes that effective implementation of the right to information is crucial for the proper functioning of Eurodac, so as to ensure that information is provided in a way that enables the asylum seeker to fully understand his situation, as well as the extent of the rights, including the procedural steps he/she can take as follow-up to the administrative decisions taken in his/her case. The EDPS suggests that the wording of Article 24 of the Proposal should be reformulated to clarify the rights to be given to the asylum applicant.

41. The EDPS recommends amending Article 4(1) of the Proposal, using the expression 'Best Available Techniques' instead of 'Best Available Technologies'. Best Available Techniques include both the technology used and the way in which the installation is designed, built, maintained and operated.

---

[1] EDPS Opinion on Intelligent Transport systems, July 2009; EDPS Opinion on the RFID communication December 2007; EDPS annual Report 2006 p. 48.

[2] http://eippcb.jrc.es/

[3] Or in the future the Management Authority as mentioned above. References to the Commission in this paragraph should be read as references to the EU institution or body who acts as a data controller for Eurodac.

42. The EDPS recommends as regards on the issue of subcontracting a part of the Commission tasks to another organisation or entity (such as a private company) that safeguards should be put in place to ensure that the applicability of Regulation (EC) No 45/2001, including the data protection supervision by the EDPS remains entirely unaffected by the subcontracting of activities. Furthermore, additional safeguards of a more technical nature should also be adopted.

Done at Brussels, 15 December 2010.

Peter HUSTINX

European Data Protection Supervisor

Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)

(2011/C 101/04)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Articles 7 and 8,

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

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

Description of the Proposal

1. On 30 September 2010, the Commission adopted a proposal for a Regulation of the European Parliament and of the Council concerning ENISA, the European Network and Information Security Agency [3].

2. ENISA was established in March 2004 for an initial period of five years by Regulation (EC) No 460/2004 [4]. In 2008, Regulation (EC) No 1007/2008 [5] extended the mandate until March 2012.

3. As follows from Article 1(1) of Regulation (EC) No 460/2004, the Agency was established for the purpose of ensuring a high and effective level of network and information security within the Union and for contributing to the smooth functioning of the internal market.

4. The Commission proposal intends to modernise the Agency, to strengthen its competences, and to establish a new mandate for a five year period that will enable the continuity of the Agency beyond March 2012 [6].

5. The proposed Regulation finds its legal basis in Article 114 of the TFEU [7], which confers competence on the Union to adopt measures with the aim of establishing or ensuring the functioning of the internal market. Article 114 TFEU is the successor of Article 95 of the former EC Treaty on which the previous regulations on ENISA were based [8].

6. The Explanatory Memorandum which accompanies the proposal refers to the fact that preventing and combating crime has become a shared competence following the entry into force of the Lisbon Treaty. This has created an opportunity for ENISA to play a role as a platform on Network Information Security (NIS) aspects of the fight against cybercrime and to exchange views and best practices with cyber defence, law enforcement and data protection authorities.

7. Out of several options the Commission chose to propose an expansion of the tasks of ENISA and to add law enforcement and data protection authorities as fully fledged members of its permanent stakeholders' group. The new list of tasks does not include operational ones, but updates and reformulates the current tasks.

EDPS consultation

8. On 1 October 2010, the proposal was sent to the EDPS for consultation in accordance with Article 28(2) of Regulation (EC) No 45/2001. The EDPS welcomes that he was consulted on this matter and recommends that a reference to this consultation is made in the recitals of the proposal, as is usually done in legislative texts on which the EDPS has been consulted in accordance with Regulation (EC) No 45/2001.

9. Prior to the adoption of the proposal, the EDPS has been informally consulted and provided several informal comments. However, none of these remarks were taken into account in the final version of the proposal.

General assessment

10. The EDPS underlines that security of data processing is a crucial element of data protection [9]. In this respect, he welcomes the proposal's objective to strengthen the

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2010) 521 final.
[4] OJ L 77, 13.3.2004, p. 1.
[5] OJ L 293, 31.10.2008, p. 1.
[6] In order to prevent a legal vacuum, should the legislative procedure in the European Parliament and in the Council last beyond the expiry of the current mandate, the Commission, on 30 September 2010, adopted a second proposal for amendment of Regulation (EC) No 460/2004 which intends only to extend the deadline of the current mandate with 18 months. See COM(2010) 520 final.
[7] Cf. supra.
[8] On 2 May 2006, the Court of Justice dismissed an action for annulment of the previous Regulation (EC) No 460/2004 that challenged its legal basis (Case C-217/04).
[9] Security requirements are contained in Articles 22 and 35 of Regulation (EC) No 45/2001, Articles 16 and 17 of Directive 95/46/EC and Articles 4 and 5 of Directive 2002/58/EC.

competences of the Agency so that it can fulfil more effectively its current tasks and responsibilities and at the same time, expand its field of activity. The EDPS furthermore welcomes the inclusion of data protection authorities and law enforcement bodies as fully fledged stakeholders. He considers the extension of ENISA's mandate a way to encourage at European level professional and streamlined management of security measures for information systems.

11. The overall assessment of the proposal is positive. However, on several points the proposed Regulation is unclear or incomplete which raises concerns from a data protection perspective. These issues will be explained and discussed in the next chapter of this opinion.

II. COMMENTS AND RECOMMENDATIONS

The expanded tasks that will be carried out by ENISA are not sufficiently clear

12. The expanded tasks of the Agency which relate to the involvement of law enforcement bodies and data protection authorities are formulated in a very general way in Article 3 of the proposal. The Explanatory Memorandum is more explicit in that respect. It refers to ENISA as interfacing with cybercrime law enforcement bodies and carrying out of non-operational tasks in the fight against cybercrime. However, these tasks have not been included or have only been mentioned in very general terms in Article 3.

13. In order to avoid any legal uncertainty, the proposed Regulation should be clear and unambiguous about the tasks of ENISA. As stated, security of data processing is a crucial element of data protection. ENISA will play an increasingly important role in that area. It should be clear to citizens, institutions and bodies what kind of activities ENISA could be engaged in. Such dimension is even more important should the expanded tasks of ENISA include the processing of personal data (see pts. 17-20 below).

14. Article 3(1)(k) of the proposal states that the Agency carries out any other task conferred on the Agency by another Union legislative act. The EDPS has concerns about this open ended clause since it creates a potential loophole that may affect the coherence of the legal instrument and could lead to 'function creep' of the Agency.

15. One of the tasks referred to in Article 3(1)(k) of the proposal is contained in Directive 2002/58/EC [1]. It provides that the Commission is required to consult the Agency on any technical implementing measures applicable to notifications in the context of data breaches. The EDPS recommends that this activity of the Agency is described in greater detail while delimiting it to the security area. Given the potential impact ENISA might have on the policy development in this area, this activity should have a clearer and more prominent position within the proposed Regulation.

16. The EDPS furthermore recommends the inclusion of a reference to Directive 1999/5/EC [2] in Recital 21 given the particular task of ENISA referred in Article 3(1)(c) of the current proposal to assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data. This should fuel ENISA promotional exercises in favour of NIS (Network Information Security) best practices and techniques, as it will better illustrate possible constructive interactions between the Agency and the standardisation bodies.

It should be clarified whether personal data will be processed by the Agency

17. The proposal does not specify whether the tasks attributed to the Agency might include the processing of personal data. Therefore, the proposal does not contain a specific legal basis for the processing of personal data, in the meaning of Article 5 of Regulation (EC) No 45/2001.

18. However, some of the tasks attributed to the Agency might involve (at least to a certain extent) the processing of personal data. It is, for instance, not excluded that the analysis of security incidents and data breaches or the execution of non-operational functions in the fight against cybercrime might involve the collection and analysis of personal data.

19. Recital 9 of the proposal refers to the provisions contained in Directive 2002/21/EC [3] which establish that where appropriate, the Agency is notified by the national regulatory authorities in the event of security breaches. The EDPS recommends that the proposal is more detailed about which notifications are meant to be sent to ENISA and about how ENISA should respond to these. Equally, the proposal should address the personal data processing implications that might arise from the analysis of these notifications (if any).

[1] 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, 31.7.2002, p. 37).

[2] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, OJ L 91, 7.4.1999, p. 10 and in particular its Article 3(3)c.

[3] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive, OJ L 108, 24.4.2002, p. 33).

20. The EDPS invites the legislator to clarify whether, and if so which ENISA activities listed in Article 3 will include the processing of personal data.

Internal security rules for ENISA should be specified

21. Although ENISA plays an important role in the discussion on network and information security in Europe, the proposal is almost silent on the establishment of security measures for the Agency itself (either or not related to the processing of personal data).

22. The EDPS is of the opinion that the Agency will be in an even better position to promote good practices in relation to security of data processing if such security measures are strongly applied internally by the agency itself. This will foster that the Agency is recognised not only as centre of expertise but also as a point of reference in the practical implementation of Best Available Techniques (BATs) in the field of security. Striving for excellence in security practices implementation should therefore be embedded within the Regulation governing the working procedures of the Agency. The EDPS therefore suggests adding a provision in this sense to the proposal, for instance by requiring that the Agency applies Best Available Techniques which means the most effective and advanced security procedures and their methods of operation.

23. This approach will allow the Agency to advise on the practical suitability of particular techniques for providing the required security safeguards. Furthermore, the implementation of these BATs should prioritise those ones that allow ensuring the security while at the same time minimising as much as possible the impact on privacy. Techniques which are better in line with the 'privacy by design' concept should be selected.

24. Even with a less ambitious approach, the EDPS recommends, at a minimum, that the Regulation contains the following requirements: (i) the creation of an internal security policy following a comprehensive risk assessment and taking into account international standards and best practices in Member States, (ii) the appointment of a security officer in charge of implementing the policy with the adequate resources and authority, (iii) the approval of this policy after a close examination of the residual risk and the controls proposed by the Management Board, and (iv) a periodic review of the policy with a clear statement of the periodicity timeframe chosen and the objectives of the review.

Cooperation channels with data protection authorities (including the EDPS) and the Article 29 Working Party should be better defined

25. As already stated, the EDPS welcomes the extension of the Agency's mandate and believes that data protection authorities can greatly benefit from the existence of the Agency (and the Agency from the expertise of these authorities). Given the natural and logical convergence between security and data protection, the Agency and data protection authorities are indeed called to collaborate closely.

26. Recitals 24 and 25 contain a reference to the proposed EU Directive on cybercrime and mention that the Agency should liaise with law enforcement bodies and also data protection authorities with respect to the information security aspects of the fight against cybercrime [1].

27. The proposal should also provide concrete channels and collaboration mechanisms that will (i) ensure the *consistency* of the activities of the Agency with those of the data protection authorities and (ii) enable *close cooperation* between the Agency and the data protection authorities.

28. With regards to *consistency*, recital 27 explicitly refers to the fact that Agency tasks should not enter into conflict with Member States' data protection authorities. The EDPS welcomes this reference, but notes that no reference is made to the EDPS and the Article 29 Working Party. The EDPS recommends the legislator to also include a similar non-interference provision in the proposal with regard to these two entities. This will create a clearer working environment for all the parties and should frame the collaboration channels and mechanisms that will enable the Agency to assist the different data protection authorities and the Article 29 Working Party.

29. Accordingly, with regard to *close cooperation*, the EDPS welcomes the inclusion of a representation of data protection authorities in the Permanent Stakeholders' group that will advise the Agency in the performance of its activities. He recommends that it is explicitly mentioned that such representation from national data protection authorities should be appointed by the Agency on the basis of a proposal from the Article 29 Working Party. Also, it would be appreciated if a reference were included that provides for the attendance of the EDPS, as such, to those meetings where issues, which are relevant for the cooperation with the EDPS, are meant to be discussed. Moreover, the EDPS recommends that the Agency (advised by the Permanent Stakeholders' group and with the approval of the Management Board) establishes ad hoc working groups for the different topics where data protection and security overlap to frame this close cooperation effort.

[1] Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, COM(2010) 517 final.

30. Finally, in order to avoid any possible misunderstanding, the EDPS recommends using 'data protection authorities' instead of 'privacy protection authorities' and clarify who those authorities are by including a reference to Article 28 of Directive 95/46/EC and the EDPS as provided in Chapter V of Regulation (EC) No 45/2001.

It is unclear which beneficiaries can request assistance from ENISA

31. The EDPS notes an inconsistency in the proposed Regulation with regard to who can request assistance from ENISA. From recitals 7, 15, 16, 18 and 36 of the proposal, it follows that ENISA has the capacity to assist Member States bodies and the Union as a whole. However, Article 2(1) only refers to the Commission and the Member States, whereas Article 14 restricts the capacity to make requests for assistance to: (i) the European Parliament, (ii) the Council, (iii) the Commission and (iv) any competent body appointed by a Member State leaving out some of the institutions, bodies, agencies and offices of the Union.

32. Article 3 of the proposal is more specific and envisages different types of assistance depending on the type of beneficiaries: (i) collection and analysis information security data (in the case of Member States and the European institutions and bodies), (ii) analysis of the state of network and information security in Europe (in the case of Member States and the European institutions), (iii) promotion of the use of risk management and security good practices (across the Union and the Member States), (iv) develop network and information security detection (in the European institutions and bodies) and (v) collaboration in the dialogue and cooperation with third countries (in the case of the Union).

33. The EDPS invites the legislator to remedy this inconsistency and align the aforementioned provisions. In this respect, the EDPS recommends that Article 14 is amended in a way that it indeed includes all institutions, bodies, offices and agencies of the Union and that it is clear as to the type of assistance that can be required by the different entities within the Union (in case this differentiation is envisaged by the legislator). In the same direction, it is recommended that certain public and private entities could request assistance from the Agency if the support demanded shows a clear potential from an European perspective, and it is aligned with the objectives of the Agency.

Management Board functions

34. The Explanatory Memorandum provides for enhanced competences of the Management Board as regards its supervisory role. The EDPS welcomes this increased role and recommends that several aspects concerning data protection are included among the functions of the Management Board. Additionally, the EDPS recommends that the Regulation specifies unambiguously who is entitled to: (i) establish measures for the application of Regulation (EC) No 45/2001 by the Agency, including those concerning the appointment of a Data Protection Officer, (ii) approve the security policy and the subsequent periodic revisions, and (iii) set the cooperation protocol with data protection authorities and law enforcement bodies.

Applicability of Regulation (EC) No 45/2001

35. Although this is already required by Regulation (EC) No 45/2001, the EDPS suggests to include in Article 27 the appointment of the Data Protection Officer since this is of particular importance and should be accompanied by the prompt establishment of the implementing rules regarding the scope of powers and tasks to be entrusted to the Data Protection Officer in accordance with Article 24(8) of Regulation (EC) No 45/2001. More concretely, Article 27 could read as follows:

1. The information processed by the Agency in accordance with this Regulation shall be subject 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. The Management Board shall establish measures for the application of Regulation (EC) No 45/2001 by the Agency, including those concerning the Data Protection Officer of the Agency.

36. In case a specific legal basis for the processing of personal data is required, as discussed in pts. 17-20 above, it should also provide for specification as to the necessary and appropriate safeguards, limitations and conditions under which such a processing would take place.

III. **CONCLUSIONS**

37. The overall assessment of the proposal is positive and the EDPS welcomes the extension of the Agency's mandate and the expansion of its tasks by the inclusion of data protection authorities and law enforcement bodies as fully fledged stakeholders. The EDPS considers that the continuity of the Agency will encourage at European level professional and streamlined management of security measures for information systems.

38. The EDPS recommends that in order to avoid any legal uncertainty, the proposal should be clarified with regard to the expansion of the Agency's tasks and in particular those that relate to the involvement of law enforcement bodies and data protection authorities. Also, the EDPS draws the attention to the potential loophole created by the inclusion of a provision in the proposal that allows the addition of new tasks to the Agency by any other Union legislative Act without any additional restriction.

39. The EDPS invites the legislator to clarify whether, and if so which of ENISA's activities will include the processing of personal data.

40. The EDPS recommends including provisions on the establishment of a security policy for the Agency itself, in order to reinforce the role of the Agency as enabler of excellence in security practices, and as promoter of privacy by design by integrating the use of best available techniques in security with the respect to personal data protection rights.

41. The cooperation channels with data protection authorities, including the EDPS and the Article 29 Working Party, should be better defined with the aim of ensuring consistency and close cooperation.

42. The EDPS invites the legislator to solve some inconsistencies with regard to the restrictions expressed on Article 14 concerning the capacity to request the assistance of the Agency. In particular, the EDPS recommends that these restrictions are waived and all institutions, bodies, agencies and offices of the Union are empowered to request assistance from the Agency.

43. Finally, the EDPS recommends that the extended capacities of the Management Board include some concrete aspects that could enhance the assurance that good practices are followed within the Agency with regard to security and data protection. Among others, it is proposed to include the appointment of a data protection officer and the approval of the measures aimed at the correct application of Regulation (EC) No 45/2001.

Done at Brussels, 20 December 2010.

Giovanni BUTTARELLI

Assistant European Data Protection Supervisor

II

(Information)

INFORMATION FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

EUROPEAN COMMISSION

Non-opposition to a notified concentration

(Case COMP/M.6076 — Orangina Schweppes/Européenne d'Embouteillage)

(Text with EEA relevance)

(2011/C 101/05)

On 22 March 2011, the Commission decided not to oppose the above notified concentration and to declare it compatible with the common market. This decision is based on Article 6(1)(b) of Council Regulation (EC) No 139/2004. The full text of the decision is available only in French and will be made public after it is cleared of any business secrets it may contain. It will be available:

— in the merger section of the Competition website of the Commission (http://ec.europa.eu/competition/mergers/cases/). This website provides various facilities to help locate individual merger decisions, including company, case number, date and sectoral indexes,

— in electronic form on the EUR-Lex website (http://eur-lex.europa.eu/en/index.htm) under document number 32011M6076. EUR-Lex is the on-line access to the European law.

IV

(Notices)

NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

EUROPEAN COMMISSION

Euro exchange rates [1]

31 March 2011

(2011/C 101/06)

1 euro =

	Currency	Exchange rate		Currency	Exchange rate
USD	US dollar	1,4207	AUD	Australian dollar	1,3736
JPY	Japanese yen	117,61	CAD	Canadian dollar	1,3785
DKK	Danish krone	7,4567	HKD	Hong Kong dollar	11,0559
GBP	Pound sterling	0,88370	NZD	New Zealand dollar	1,8598
SEK	Swedish krona	8,9329	SGD	Singapore dollar	1,7902
CHF	Swiss franc	1,3005	KRW	South Korean won	1 554,51
ISK	Iceland króna		ZAR	South African rand	9,6507
NOK	Norwegian krone	7,8330	CNY	Chinese yuan renminbi	9,3036
BGN	Bulgarian lev	1,9558	HRK	Croatian kuna	7,3778
CZK	Czech koruna	24,543	IDR	Indonesian rupiah	12 366,75
HUF	Hungarian forint	265,72	MYR	Malaysian ringgit	4,2983
LTL	Lithuanian litas	3,4528	PHP	Philippine peso	61,559
LVL	Latvian lats	0,7095	RUB	Russian rouble	40,2850
PLN	Polish zloty	4,0106	THB	Thai baht	42,976
RON	Romanian leu	4,1221	BRL	Brazilian real	2,3058
TRY	Turkish lira	2,1947	MXN	Mexican peso	16,9276
			INR	Indian rupee	63,3450

[1] *Source*: reference exchange rate published by the ECB.

COURT OF AUDITORS

Special Report No 1/2011 'Has the devolution of the Commission's management of external assistance from its headquarters to its delegations led to improved aid delivery?'

(2011/C 101/07)

The European Court of Auditors hereby informs you that Special Report No 1/2011 'Has the devolution of the Commission's management of external assistance from its headquarters to its delegations led to improved aid delivery?' has just been published.

The report can be accessed for consultation or downloading on the European Court of Auditors' website: http://www.eca.europa.eu

A hard copy version of the report may be obtained free of charge on request to the Court of Auditors:

European Court of Auditors
Communication and Reports Unit
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1
E-mail: euraud@eca.europa.eu

or by filling in an electronic order form on EU-Bookshop.

NOTICES FROM MEMBER STATES

Belgian national procedure for allocating limited air traffic rights

(2011/C 101/08)

In accordance with Article 6 of Regulation (EC) No 847/2004 on the negotiation and implementation of air service agreements between Member States and third countries, the European Commission is publishing the following national procedure for the distribution of traffic rights among eligible Community air carriers where these rights are limited by aviation agreements with third countries.

KINGDOM OF BELGIUM

FEDERAL PUBLIC SERVICE FOR MOBILITY AND TRANSPORT

AIR TRANSPORT

Royal Decree on the designation of Community air carriers and the allocation of traffic rights in respect of the operation of scheduled air services between Belgium and non-Community countries

ALBERT II, King of the Belgians,

To all, present and to come, greetings.

Having regard to Regulation (EC) No 847/2004 of the European Parliament and of the Council of 29 April 2004 on the negotiation and implementation of air service agreements between Member States and third countries,

Having regard to the Law of 27 June 1937 revising the Law of 16 November 1919 laying down rules for air navigation, in particular Article 5, §2, incorporated by the Law of 2 January 2001,

Having regard to the Law of 3 May 1999 on scheduled air carriers,

Having regard to the involvement of the governments of the regions in drafting this Decree,

Having regard to Opinion No 47.574/4 of the Council of State, given on 6 January 2010, in application of Article 84, §1, paragraph 1, 1, of the laws of the Council of State, as coordinated on 12 January 1973,

On a proposal from our Prime Minister and the State Secretary for Mobility,

WE HAVE DECIDED AS FOLLOWS:

Article 1

This Decree lays down the detailed arrangements for the designation of Community air carriers and for allocating traffic rights with a view to the operation of scheduled air services between Belgium and non-Community countries.

Article 2

For the purposes of this Decree, the following definitions apply:

1. 'Community air carrier' means any air carrier with a valid operating licence issued in accordance with Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community;

2. 'traffic right' means the right for an air carrier, in return for payment, to carry passengers, freight and/or mail on a given air link;

3. 'Director-General' means the Director-General of the Directorate-General for Air Transport;

4. 'Directorate-General for Air Transport' means the directorate responsible for air transport within the Federal Public Service for Mobility and Transport;

5. 'scheduled air services' means a series of flights accessible to the public and intended to ensure, either combined or individually, the transportation of passengers, mail and/or freight in return for payment. This series of flights is operated:

   (a) either according to a published timetable;

   (b) or with flights which are so regular and frequent as to constitute a recognisably systematic series;

6. 'bilateral aviation agreement' means an aviation agreement concluded between Belgium and a non-Community country and any other aviation agreement between the European Union and a non-Community country;

7. 'designation' means the right granted to an air carrier to operate scheduled air services in the framework of a bilateral aviation agreement. Such designation may be granted to a single air carrier (single designation) or to several air carriers (multiple designation) in accordance with the provisions of the bilateral aviation agreement concerned;

8. 'accessibility' means the possibility, under a bilateral aviation agreement, to be designated and/or to operate the desired number of flights on a given route;

9. 'Minister' means the Minister responsible for aviation;

10. 'IATA season' means the summer or winter season as defined by the International Air Transport Association (IATA).

Article 3

This Decree and the timetable for the bilateral negotiation of aviation agreements between Belgium and non-Community countries will be published on the website of the Federal Public Service for Mobility and Transport. All other information about the aviation agreements, the traffic rights and designation can be obtained from the Directorate-General for Air Transport.

Article 4

1. Only Community air carriers established in Belgium in accordance with Community law may be designated and allocated traffic rights.

To this end, a carrier must submit an application in one of the national languages or in English to the Director-General by registered letter.

Such an application must be accompanied by a file containing:

1. the operating licence and the air operator certificate (AOC), unless those documents were issued by Belgium;

2. the insurance certificate;

3. evidence that the Community air carrier is established in Belgium in conformity with Community law;

4. proof of operational capacity and financial fitness within the meaning of Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community;

5. the following information on the scheduled air services proposed:

   (a) the proposed air link (route, weekly frequency, timetables, stop-over points, whether or not seasonal);

   (b) the type of transport (freight, passengers, mail);

(c) the passenger traffic (traffic forecasts, customer breakdown, main actual origins and destinations);

(d) the type of aircraft, its class configuration and its capacity;

(e) the date on which it is proposed to start the service, its foreseeable duration and information about any earlier operation of the air link concerned by the applicant;

(f) information about the size of the market and in particular about any capacity already offered on the air link concerned or foreseeable in the short term;

(g) how the flights proposed will be operated:

(i) whether the aircraft entered in the applicant's air operator certificate (AOC) will be used;

(ii) recourse to a code-sharing agreement with another air carrier (Community or otherwise);

(iii) leasing of an aircraft or aircraft capacity;

(iv) any other form of cooperation with one or more other air carriers;

(h) how the flights will be offered to the public and marketed (fares planned, public access to services, distribution channels);

(i) the acoustic emissions categories and other environmental characteristics of the aircraft which it is planned to use;

6. whether the applicant agrees to make available any necessary capacity to meet Belgium's national or international needs in exceptional circumstances.

2. By way of derogation from the third paragraph of §1, an application from a Community air carrier who, following the entry into force of this Decree, has already submitted a file containing all the elements referred to in points 1 to 4 of the third paragraph of §1 need only be accompanied by the information referred to in point 5 of the third paragraph of §1 and, if applicable, details of any changes made to the information referred to in points 1 to 4 of the third paragraph of §1.

Article 5

Only applications which comply with Article 4 will be considered by the Director-General and published on the website of the Federal Public Service for Mobility and Transport.

At any time during the consideration of an application, the Director-General may:

1. ask the Community air carrier for additional information; and/or

2. hold hearings to which all applicants will be called.

Article 6

All Community air carriers will automatically be granted designation and/or allocated the requested traffic rights by the Minister provided that the bilateral aviation agreement between Belgium and the non-Community country concerned does not limit:

1. the number of Community air carriers that may be designated; or

2. the number of flights which may be operated on specific routes.

Allocation will be notified to the air carrier.

Article 7

In cases where the bilateral aviation agreements limit:

1. the number of Community air carriers which may be designated; or

2. the frequency of operations on specific routes,

the application is first considered with regard to accessibility to designation and/or the traffic rights requested.

Article 8

If there is no more accessibility to enable the applicant to operate scheduled air services on the routes concerned, the applicant will be notified by registered letter within 15 working days of receipt of the application. The notification is also published on the website of the Federal Public Service for Mobility and Transport.

If there is still sufficient accessibility to enable the applicant to operate scheduled air services on the routes concerned, the Director-General will notify the applicant within 15 working days in writing and via the website of the Federal Public Service for Mobility and Transport.

Community air carriers established in Belgium will be informed in writing that they have 15 working days from the date of notification referred to in the second paragraph to apply for designation and/or the allocation of traffic rights.

The competing applications will be published on the website of the Federal Public Service for Mobility and Transport.

Article 9

If there are no competing applications or if all applications can be accepted, the Minister will accept the application(s) concerned and provide notification of his decision within 15 working days by registered letter and by publishing the decision on the website of the Federal Public Service for Mobility and Transport.

Article 10

If several Community air carriers express their desire to be designated or allocated traffic rights on a given route and it is impossible to accept all the applications, the competing applications will be examined by the Director-General on the basis of the complete file of applications as defined in Article 4.

The Director-General will send a draft decision on the allocation of traffic rights and/or designation to the competing applicants by registered letter within 30 working days. The date on which the draft decision is sent will be published on the website of the Federal Public Service for Mobility and Transport.

Community air carriers which have submitted an application may submit their comments to the Director-General by registered letter within 10 working days following the date on which the draft decision is sent:

1. if comments are expressed, the Minister will take a final decision on the allocation of traffic rights and/or designation within 15 working days following the receipt of such comments; that decision will be notified to applicants by registered letter and published on the website of the Federal Public Service for Mobility and Transport;

2. if no comments are expressed, the draft decision will become the Minister's final decision on the allocation of traffic rights and/or designation; that decision will be notified to the applicant(s) by registered letter and published on the website of the Federal Public Service for Mobility and Transport.

Article 11

The applications referred to in this Decree will be considered on a transparent, non-discriminatory basis.

Any decision or draft decision on the allocation of traffic rights and/or designation will take account, with no particular order of priority or importance, of:

1. the information referred to in Article 4 as submitted by the Community air carrier;

2. the guarantees provided as regards operational continuity and its inclusion in a coherent business plan;

3. whether optimum use is made of the limited traffic rights;

4. the priority nature of the operations performed by a Community air carrier using its own (owned or leased) aircraft as compared with operations where the Community air carrier is satisfied to market flights operated by another air carrier by means of code-sharing arrangements;

5. the interests of all categories of users;

6. the ease of access to new routes, markets and regions, whether by means of new links or departures from or arrivals at different Belgian airports;

7. the contribution towards ensuring a satisfactory level of competition;

8. any effects of the operation on the creation of jobs, either directly or indirectly, in the air transport sector;

9. as a secondary consideration, how long the Community air carrier has been actively and repeatedly expressing the desire to obtain the traffic rights which are the subject of its application.

The Minister will give details of the criteria referred to above in order to guarantee that they are objective and transparent.

Article 12

Any Community air carrier which is granted designation and/or obtains traffic rights under a bilateral aviation agreement between Belgium and a non-Community country is obliged:

1. to start operating the air services concerned at the latest at the end of the IATA season following that during which the decision granting designation and/or allocating traffic rights was notified;

2. to operate the air services concerned in accordance with the file referred to in Article 4. The difference between the original project and actual operations must not be so great that it might have led to another air carrier being chosen when designation was originally granted;

3. to comply with any conditions laid down by the Director-General, the decisions made by the aviation authorities of the non-Community countries affected by the operation of the air services concerned and the permits issued by them as well as with all relevant international regulations;

4. to notify the Director-General immediately of the cessation of, or any interruption in, the operation of the air services concerned. If any such interruption continues for more than two seasons, the decision to allocate traffic rights and/or grant designation will be automatically withdrawn at the end of the second season unless the Community air carrier can claim there were exceptional circumstances beyond its control.

The Directorate-General for Air Transport will monitor compliance with the obligations set out in paragraph 1.

Article 13

Designation and/or the allocation of traffic rights is personal and is not transferrable. It is of unlimited duration unless the decision is withdrawn.

Article 14

If an air carrier does not comply with the obligations set out in the first paragraph of Article 12 or seriously jeopardises air safety, the Minister may suspend or withdraw the decision granting designation and/or allocating traffic rights.

Article 15

1. All Community air carriers established in Belgium in accordance with Community law are entitled to contest the use of traffic rights made by any other air carrier on a given route and to apply to make better use of them.

To this end, it must send the Director-General a duly substantiated file which may be consulted by the air carrier whose traffic rights' use is contested.

However, the right to contest this use may not be exercised until after two years of operation following the allocation of the original traffic rights.

2. In such an event, the Minister will re-consider, on the basis of the file and any possible hearings, the original allocation and the use made thereof and will decide:

1. either to take no further action on the application;

2. or to launch a new allocation procedure.

However, if a Community air carrier uses its traffic rights only in the form of cooperation with another air carrier and without using its own aircraft, the Minister will re-consider the original allocation immediately if a competing air carrier submits a formal application to operate the air services concerned using its own aircraft.

Any change in the allocation of traffic rights and/or in designation, either in full or in part, will not take effect at the earliest until the first day of the second IATA season following that during which the decision was taken.

Article 16

In order to allow a proper assessment to be made of Community air carriers' markets, links and applications, the carriers will regularly send the Directorate-General for Air Transport figures concerning the operations for which they have been designated.

The Minister will specify the level of detail and the frequency with which these figures must be submitted.

Article 17

1. Traffic rights which were allocated on a particular route prior to the entry into force of this Decree and which were already limited or have been limited may be contested in accordance with the procedure set out in Article 15.

In such an event, the Directorate-General for Air Transport will ensure that a solution can be found before any procedure is launched by renegotiating the limited traffic rights agreed in the aviation agreement concluded with the non-Community country concerned.

2. The procedure referred to in §1 also applies to designation.

Article 18

The Law of 3 May 1999 on scheduled air carriers is hereby repealed.

Article 19

This Decree enters into force two months after its publication in the *Belgian Official Gazette*.

Article 20

Our Minister responsible for aviation is instructed to implement this Decree.

Done at Brussels, 18 August 2010.

For the King

The Prime Minister
Yves LETERME

State Secretary for Mobility
Etienne SCHOUPPE

Information communicated by Member States regarding State aid granted under Commission Regulation (EC) No 1628/2006 on the application of Articles 87 and 88 of the Treaty to national regional investment aid

(Text with EEA relevance)

(2011/C 101/09)

Aid No	XR 194/07
Member State	Spain
Region	Galicia
Title of aid scheme or the name of the undertaking receiving ad hoc aid supplement	Ayudas regionales a la inversión en la Comunidad Autónoma de Galicia en aplicación del Reglamento (CE) nº 1628/2006
Legal basis	Proyecto de Decreto por el que se regulan las ayudas regionales a la inversión en la Comunidad Autónoma de Galicia en aplicación del Reglamento (CE) nº 1628/2006
Type of measure	Aid scheme
Annual budget	EUR 100 million
Maximum aid intensity	30 %
	In conformity with Article 4 of the Regulation
Date of implementation	1.1.2007
Duration	31.12.2013
Economic sectors	All sectors eligible for regional investment aid
Name and address of the granting authority	Xunta de Galicia Consellería de Economía y Hacienda Edificio Administrativo San Caetano s/n 15781 Santiago de Compostela ESPAÑA
Internet address of the publication of the aid scheme	http://www.econmiaefacenda.org/
Other information	—

Aid No	XR 67/08
Member State	Spain
Region	—
Title of aid scheme or the name of the undertaking receiving ad hoc aid supplement	Ayudas derivadas del Plan de Seguridad Minera para la consecución de una minera sostenible en los aspectos de prevención y seguridad minera.
Legal basis	Orden ITC/732/2008, de 13 de marzo, punto Tercero, apartado 5.1. letra b), inversiones regionales (BOE nº 67 de 18.3.2008)

Type of measure	Aid scheme
Annual budget	EUR 1,4 million
Overall budget	—
Maximum aid intensity	48 %
	In conformity with Article 4 of the Regulation
Date of implementation	19.3.2008
Duration	31.12.2013
Economic sectors	Limited to specific sectors:
	NACE: 13, 14
Name and address of the granting authority	Dirección General de Politica Energética y Minas Jorge Sanz Oliva Paseo de la Castellana, 160 28071 Madrid ESPAÑA Tel. +34 913497475 E-mail: jcsanz@mytic.es
Internet address of the publication of the aid scheme	http://www.mityc.es/seguridadminera
Other information	—

V

(Announcements)

PROCEDURES RELATING TO THE IMPLEMENTATION OF COMPETITION POLICY

EUROPEAN COMMISSION

Prior notification of a concentration

(Case COMP/M.6144 — Giesecke & Devrient/Wincor Nixdorf International/BEB Industrie-Elektronik)

Candidate case for simplified procedure

(Text with EEA relevance)

(2011/C 101/10)

1. On 23 March 2011, the Commission received notification of a proposed concentration pursuant to Article 4 of Council Regulation (EC) No 139/2004 [1] by which the undertakings Giesecke & Devrient GmbH ('G&D', Germany) and BEB Industrie-Elektronik AG ('BEB', Switzerland), which is controlled by Wincor Nixdorf International GmbH ('WNI', Germany), belonging to the Wincor Nixdorf Aktiengesellschaft group (Germany), acquire within the meaning of Article 3(1)(b) of the Merger Regulation joint control of the undertaking CI Tech Components AG (Switzerland) by way of transfer of assets and purchase of shares in a newly created company constituting a joint venture.

2. The business activities of the undertakings concerned are:

— G&D: Banknote management, ID documents, smart cards, card system solutions and security solutions in the IT environment,

— WNI: IT solutions for process optimisation in retail banking and trade,

— BEB: Equipment for identifying and checking bank notes.

3. On preliminary examination, the Commission finds that the notified transaction could fall within the scope of the EC Merger Regulation. However, the final decision on this point is reserved. Pursuant to the Commission Notice on a simplified procedure for treatment of certain concentrations under the EC Merger Regulation [2] it should be noted that this case is a candidate for treatment under the procedure set out in the Notice.

4. The Commission invites interested third parties to submit their possible observations on the proposed operation to the Commission.

---

[1] OJ L 24, 29.1.2004, p. 1 (the 'EC Merger Regulation').
[2] OJ C 56, 5.3.2005, p. 32 ('Notice on a simplified procedure').

Observations must reach the Commission not later than 10 days following the date of this publication. Observations can be sent to the Commission by fax (+32 22964301), by email to COMP-MERGER-REGISTRY@ec.europa.eu or by post, under reference number COMP/M.6144 — Giesecke & Devrient/ Wincor Nixdorf International/BEB Industrie-Elektronik, to the following address:

European Commission
Directorate-General for Competition
Merger Registry
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

Prior notification of a concentration

(Case COMP/M.6182 — MAN/MAN Camions et Bus/MAN Truck & Bus Belgium)

Candidate case for simplified procedure

(Text with EEA relevance)

(2011/C 101/11)

1. On 21 March 2011, the Commission received a notification of a proposed concentration pursuant to Article 4 of Council Regulation (EC) No 139/2004 ([1]) by which the undertaking MAN Truck & Bus AG ('MAN Truck & Bus', Germany), controlled by MAN SE ('MAN', Germany) acquires within the meaning of Article 3(1)(b) of the Merger Regulation sole control of the whole of MAN Camions et Bus S.A.S. ('MAN Camions et Bus', France) and MAN Truck and Bus N.V./S.A. ('MAN Truck and Bus Belgium', Belgium) by way of purchase of shares.

2. The business activities of the undertakings concerned are:

— MAN: development, manufacture and sale of trucks, buses and coaches, chassis and floor assemblies for buses, industrial and marine engines, diesel engines, turbo-machines and industrial services,

— MAN Camions et Bus: sale and after sale services of trucks, buses and coaches and the sale of chassis for coaches and (as a genuine agent) the sale of truck (diesel) engines and spare parts thereof,

— MAN Truck & Bus Belgium: sale and after sale services of trucks, buses and coaches and (as a genuine agent) the sale of truck (diesel) engines and spare parts thereof.

3. On preliminary examination, the Commission finds that the notified transaction could fall within the scope of the EC Merger Regulation. However, the final decision on this point is reserved. Pursuant to the Commission Notice on a simplified procedure for treatment of certain concentrations under the EC Merger Regulation ([2]) it should be noted that this case is a candidate for treatment under the procedure set out in the Notice.

4. The Commission invites interested third parties to submit their possible observations on the proposed operation to the Commission.

Observations must reach the Commission not later than 10 days following the date of this publication. Observations can be sent to the Commission by fax (+32 22964301), by email to COMP-MERGER-REGISTRY@ec.europa.eu or by post, under reference number COMP/M.6182 — MAN/MAN Camions et Bus/MAN Truck & Bus Belgium, to the following address:

European Commission
Directorate-General for Competition
Merger Registry
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

([1]) OJ L 24, 29.1.2004, p. 1 (the 'EC Merger Regulation').
([2]) OJ C 56, 5.3.2005, p. 32 ('Notice on a simplified procedure').

OTHER ACTS

EUROPEAN COMMISSION

Notice for the attention of Ibrahim Hassan Tali Al-Asiri who was added to the list referred to in Articles 2, 3 and 7 of Council Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, by virtue of Commission Regulation (EU) No 317/2011

(2011/C 101/12)

1. Common Position 2002/402/CFSP [1] calls upon the Union to freeze the funds and economic resources of Usama bin Laden, members of the Al-Qaida organisation and the Taliban and other individuals, groups, undertakings and entities associated with them, as referred to in the list drawn up pursuant to UNSCR 1267(1999) and 1333(2000) to be updated regularly by the UN Committee established pursuant to UNSCR 1267(1999).

The list drawn up by this UN Committee comprises:

— Al Qaida, the Taliban and Usama bin Laden,

— natural or legal persons, entities, bodies and groups associated with Al Qaida, the Taliban and Usama bin Laden, and

— legal persons, entities and bodies owned or controlled by, or otherwise supporting, any of these associated persons, entities, bodies and groups.

Acts or activities indicating that an individual, group, undertaking, or entity is 'associated with' Al-Qaida, Usama bin Laden or the Taliban include:

(a) participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of, Al Qaida, the Taliban or Usama bin Laden, or any cell, affiliate, splinter group or derivative thereof;

(b) supplying, selling or transferring arms and related materiel to any of them;

(c) recruiting for any of them; or

(d) otherwise supporting acts or activities of any of them.

2. The UN Committee decided on 23 March 2011 to add Ibrahim Hassan Tali Al-Asiri to the relevant list. He may submit at any time a request to the UN Ombudsperson, together with any supporting documentation, for the decision to include him in the UN list referred to above, to be reconsidered. Such request should be sent to the following address:

United Nations — Office of the Ombudsperson
Room TB-08041D
New York, NY 10017
UNITED STATES OF AMERICA

Tel. +1 2129632671
Fax +1 2129631300 / 3778
E-mail: ombudsperson@un.org

[1] OJ L 139, 29.5.2002, p. 4.

See for more information at http://www.un.org/sc/committees/1267/delisting.shtml

3. Further to the UN decision referred to in paragraph 2, the Commission has adopted Regulation (EU) No 317/2011 ([1]), which amends Annex I to Council Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban ([2]). The amendment, made pursuant to Articles 7(1)(a) and 7a(1) of Regulation (EC) No 881/2002, adds Ibrahim Hassan Tali Al-Asiri to the list in Annex I of that Regulation ('Annex I').

The following measures of Regulation (EC) No 881/2002 apply to the individuals and entities included in Annex I:

1. the freezing of all funds and economic resources belonging to the individuals and entities concerned, or owned or held by them, and the prohibition (on everyone) on making funds and economic resources available to any of the individuals and entities concerned or for their benefit, whether directly or indirectly (Articles 2 and 2a ([3])); and

2. the prohibition on granting, selling, supplying or transferring technical advice, assistance or training related to military activities to any of the individuals and entities concerned, whether directly or indirectly (Article 3).

4. Article 7a of Regulation (EC) No 881/2002 ([4]) provides for a review process where observations on the grounds for listing are submitted by those listed. Individuals and entities added to Annex I by Regulation (EU) No 317/2011 may make a request for the grounds for their listing to the Commission. This request should be sent to:

European Commission
'Restrictive measures'
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

5. The attention of the individuals and entities concerned is also drawn to the possibility of challenging Regulation (EU) No 317/2011 before the General Court of the European Union, in accordance with the conditions laid down in the fourth and sixth paragraphs of Article 263 of the Treaty on the Functioning of the European Union.

6. Personal data of the individuals concerned will be handled in accordance with the rules of Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community (now Union) institutions and bodies and on the free movement of such data ([5]). Any request, e.g. for further information or in order to exercise the rights under Regulation (EC) No 45/2001 (e.g. access or rectification of personal data), should be sent to the Commission, at the address mentioned under point 4 above.

7. For good order, the attention of the individuals and entities included in Annex I is drawn to the possibility of making an application to the competent authorities in the relevant Member State(s), as listed in Annex II to Regulation (EC) No 881/2002, in order to obtain an authorisation to use frozen funds and economic resources for essential needs or specific payments in accordance with Article 2a of that Regulation.

([1]) OJ L 86, 1.4.2011, p. 63.
([2]) OJ L 139, 29.5.2002, p. 9.
([3]) Article 2a was inserted by Council Regulation (EC) No 561/2003 (OJ L 82, 29.3.2003, p. 1).
([4]) Article 7a was inserted by Council Regulation (EU) No 1286/2009 (OJ L 346, 23.12.2009, p. 42).
([5]) OJ L 8, 12.1.2001, p. 1.

V *Announcements*

EN

[1] Text with EEA relevance

2011 SUBSCRIPTION PRICES (excluding VAT, including normal transport charges)

EU Official Journal, L + C series, paper edition only	22 official EU languages	EUR 1 100 per year
EU Official Journal, L + C series, paper + annual DVD	22 official EU languages	EUR 1 200 per year
EU Official Journal, L series, paper edition only	22 official EU languages	EUR 770 per year
EU Official Journal, L + C series, monthly DVD (cumulative)	22 official EU languages	EUR 400 per year
Supplement to the Official Journal (S series), tendering procedures for public contracts, DVD, one edition per week	multilingual: 23 official EU languages	EUR 300 per year
EU Official Journal, C series — recruitment competitions	Language(s) according to competition(s)	EUR 50 per year

Subscriptions to the *Official Journal of the European Union*, which is published in the official languages of the European Union, are available for 22 language versions. The Official Journal comprises two series, L (Legislation) and C (Information and Notices).

A separate subscription must be taken out for each language version.

In accordance with Council Regulation (EC) No 920/2005, published in Official Journal L 156 of 18 June 2005, the institutions of the European Union are temporarily not bound by the obligation to draft all acts in Irish and publish them in that language. Irish editions of the Official Journal are therefore sold separately.

Subscriptions to the Supplement to the Official Journal (S Series — tendering procedures for public contracts) cover all 23 official language versions on a single multilingual DVD.

On request, subscribers to the *Official Journal of the European Union* can receive the various Annexes to the Official Journal. Subscribers are informed of the publication of Annexes by notices inserted in the *Official Journal of the European Union*.

Sales and subscriptions

Subscriptions to various priced periodicals, such as the subscription to the *Official Journal of the European Union*, are available from our sales agents. The list of sales agents is available at:

http://publications.europa.eu/others/agents/index_en.htm

EUR-Lex (http://eur-lex.europa.eu) offers direct access to European Union legislation free of charge. The *Official Journal of the European Union* can be consulted on this website, as can the Treaties, legislation, case-law and preparatory acts.

For further information on the European Union, see: http://europa.eu

Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN