Opinion of the European Data Protection Supervisor

on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI')

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2],

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

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 29 August 2011, the Commission adopted a Proposal for a Regulation ('the Proposal' or 'the proposed Regulation') of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI').[3] The Proposal was sent to the EDPS for consultation on the same day.

2. Before the adoption of the Proposal, the EDPS was given the possibility to give informal comments on the Proposal, and prior to that, on the Commission

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2011) 522 final.

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

Communication 'Better governance of the Single Market through greater administrative cooperation: A strategy for expanding and developing the Internal Market Information System ("IMI")' ('the IMI Strategy Communication')[4] that preceded the Proposal. Many of these comments have been taken into account in the Proposal, and - as a result - the data protections safeguards in the Proposal have been strengthened.

3. The EDPS welcomes the fact that the Commission formally consulted him and that a reference to this Opinion is included in the preamble of the Proposal.

1.2. Objectives and scope of the Proposal

4. IMI is an information technology tool that allows competent authorities in Member States to exchange information with each other when applying the Internal Market legislation. IMI allows national, regional and local authorities in EU Member States to communicate quickly and easily with their counterparts in other European countries. This also involves the processing of relevant personal data, including sensitive data.

5. IMI has initially been built as a communication tool for one-to-one exchanges under the Professional Qualification Directive[5] and the Services Directive[6]. IMI helps users to find the right authority to contact in another country and communicate with it using pre-translated sets of standard questions and answers.[7]

6. IMI, however, is meant to be a flexible, horizontal system that can support multiple areas of internal market legislation. It is envisaged that its use will be gradually expanded to support additional legislative areas in the future.

7. The functionalities of IMI are also planned to be expanded. In addition to one-to-one information exchanges, other functionalities are also foreseen, or already implemented, such as 'notification procedures, alert mechanisms, mutual assistance arrangements and problem solving'[8] as well as 'repositories of information for future reference by IMI actors'[9]. Many, but not all, of these functionalities may also include the processing of personal data.

8. The Proposal aims to provide a clear legal basis and a comprehensive data protection framework for IMI.

1.3. Background of the Proposal: a step-by-step approach to establish a comprehensive data protection framework for IMI

9. During the spring of 2007, the Commission requested the Opinion of the Article 29 Data Protection Working Party ('WP29') to review the data protection implications of

[4] COM(2011) 75.
[5] Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications, OJ L 255, 30.9.2005, p. 22.
[6] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, OJ L 376, 27.12.2006, p. 36.
[7] To illustrate, a typical question containing sensitive data would be, for example: 'Does the attached document lawfully justify the absence of suspension or prohibition of the pursuit of the relevant professional activities for serious professional misconduct or criminal offence with regard to [the migrant professional]?'
[8] See recital 10.
[9] See Article 13(2).

IMI. The WP29 issued its Opinion on 20 September 2007.[10] The Opinion recommended the Commission to provide a clearer legal basis and specific data protections safeguards for the exchange of data within IMI. The EDPS actively participated in the work of the subgroup dealing with IMI and supported the conclusions of the Opinion of the WP29.

10. Subsequently, the EDPS continued to provide further guidance to the Commission on how to ensure, step by step, a more comprehensive data protection framework for IMI.[11] In the framework of this cooperation, and since the issue on 22 February 2008 of his Opinion on the implementation of IMI[12], the EDPS has been consistently advocating the need for a new legal instrument under the ordinary legislative procedure, in order to establish a more comprehensive data protection framework for IMI and to provide legal certainty. The Proposal for such a legal instrument has now been put forward.[13]

2. ANALYSIS OF THE PROPOSAL

2.1. Overall views of the EDPS on the Proposal and on the key challenges regulating IMI

11. The overall views of the EDPS on IMI are positive. The EDPS supports the aims of the Commission in establishing an electronic system for the exchange of information and regulating its data protection aspects. Such a streamlined system will not only enhance efficiency of cooperation, but may also help ensure consistent compliance with applicable data protection laws. It may do so by providing a clear framework on what information can be exchanged, with whom, and under what conditions.

12. The EDPS also welcomes the fact that the Commission proposes a horizontal legal instrument for IMI in the form of a Council and Parliament Regulation. He is pleased that the Proposal comprehensively highlights the most relevant data protection issues for IMI. His comments must be read against this positive background.

13. Nevertheless, the EDPS cautions that establishment of a single centralized electronic system for multiple areas of administrative cooperation also creates risks. These include, most importantly, that more data might be shared, and more broadly than strictly necessary for the purposes of efficient cooperation, and that data, including potentially outdated and inaccurate data, might remain in the electronic system longer than necessary. The security of the information system accessible in 27 Member States is also a sensitive issue, as the whole system will be only as secure as the weakest link in the chain permits it to be.

[10] WP29 Opinion No 7/2007 on data protection issues related to the Internal Market Information System (IMI), WP140. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140_en.pdf.

[11] The key documents concerning this cooperation are available on the Commission's IMI website at http://ec.europa.eu/internal_market/imi-net/data_protection_en.html as well as on the EDPS website at http://www.edps.europa.eu.

[12] Opinion of the EDPS on the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC, OJ C 270, 25.10.2008, p. 1).

[13] The WP29 also plans to comment on the Proposal. The EDPS has been following these developments in the relevant WP29 subgroup and contributed comments.

Key challenges

14. With regard to the legal framework for IMI to be established in the proposed Regulation, the EDPS calls attention to two key challenges:

    - the need to ensure consistency, while respecting diversity, and
    - the need to balance flexibility and legal certainty.

15. These key challenges serve as important points of reference and determine, to a large part, the approach that the EDPS takes in this Opinion.

Consistency, while respecting diversity

16. First, IMI is a system that is used in 27 Member States. At the current state of harmonization of European laws, there are considerable differences among national administrative procedures, as well as national data protection laws. IMI needs to be built in such a way that users in each of these 27 Member States would be able to comply with their national laws, including national data protection laws, when exchanging personal data via IMI. At the same time, the data subjects must also be reassured that their data will be consistently protected irrespective of transfer of data via IMI to another Member State. Consistency, while at the same time respecting diversity, is a key challenge for building both the technical and the legal infrastructure for IMI. Undue complexity and fragmentation should be avoided. The data processing operations within IMI must be transparent, responsibilities for making decisions regarding the design of the system, its day-day maintenance and use, and also of its supervision, must be clearly allocated.

Balancing flexibility and legal certainty

17. Second, unlike some other large-scale IT systems, such as the Schengen Information System, the Visa Information System, the Customs Information System, or EURODAC, which are all focused on cooperation in specific, clearly defined areas, IMI is a horizontal tool for information exchange, and can be used to facilitate information exchange in many different policy areas. It is also foreseen that the scope of IMI will gradually expand to additional policy areas and its functionalities may also change to include hitherto unspecified types of administrative cooperation. These distinguishing features of IMI make it more difficult to clearly define the functionalities of the system, and the data exchanges that may take place in the system. Therefore, it is also more challenging to clearly define the appropriate data protection safeguards.

18. The EDPS acknowledges that there is a need for flexibility and takes note of the Commission's desire to make the Regulation 'future-proof'. However, this should not lead to lack of clarity or legal certainty in terms of the functionalities of the system and the data protection safeguards that are to be implemented. For this reason, whenever possible, the Proposal should be more specific and go beyond reiterating the main data protection principles set forth in Directive 95/46/EC and Regulation 45/2001.[14]

[14] In this respect, see also our comments in Section 2.2 regarding the foreseen expansion of IMI.

2.2. Scope of IMI and its foreseen expansion (Articles 3 and 4)

2.2.1. Introduction

19. The EDPS welcomes the Proposal's clear definition of the current scope of IMI, with Annex I listing the relevant Union acts on the basis of which information can be exchanged. These include cooperation under specific provisions of the Professional Qualifications Directive, the Services Directive and the Directive on the application of patients' rights in cross-border healthcare[15].

20. As the scope of IMI is expected to expand, potential targets for expansion are listed in Annex II. Items from Annex II can be moved to Annex I via a delegated act to be adopted by the Commission following an impact assessment.[16]

21. The EDPS welcomes this technique as it (i) clearly delimits the scope of IMI and (ii) ensures transparency, while at the same time (iii) allowing flexibility in cases where IMI will be used for additional information exchanges in the future. It also ensures that no information exchange can be carried out through IMI without (i) having an appropriate legal basis in specific internal market legislation allowing or mandating information exchange[17], and (ii) including a reference to that legal basis in Annex I to the Regulation.

22. That said, uncertainties still exist regarding the scope of IMI, with regard to the policy areas where IMI may be expanded to, and with regard to the functionalities that are or may be included in IMI.

23. First, it cannot be excluded that the scope of IMI may be extended beyond the policy areas listed in Annex I and Annex II. This may happen if the use of IMI is provided for certain types of information exchanges not in a Commission delegated act but in an act adopted by the Parliament and the Council in a case where this was not foreseen in Annex II.[18]

24. Second, while the extension of scope to new policy areas in some cases may require little or no change in the existing functionalities of the system,[19] other extensions may require new and different functionalities, or important changes to existing functionalities:

---

[15] Directive 2011/24/EC of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88/45, 4.04.2011, p. 45).

[16] The draft Regulation itself does not refer to an impact assessment. However, page 7 of the Explanatory Memorandum to the Proposal explains that the Commission will be empowered to move items from Annex II to Annex I, by adopting a delegated act and 'following an assessment of technical feasibility, cost-efficiency, user-friendliness and overall impact of the system, as well as the result of a possible test phase'.

[17] This is with the exception of SOLVIT (see Annex II, I(1)), where only 'soft law', a Commission Recommendation is available. From the data protection point of view, in the view of the EDPS, in the specific case of SOLVIT, the legal basis of the processing may be 'consent' of the data subjects.

[18] This may happen upon initiative of the Commission, but it can also not be excluded that the idea to use IMI in a specific policy area may arise later in the legislative process, and may be proposed by the Parliament or by the Council. This has already happened in the past with regard to the Directive on patients' rights in cross-border health-care. More clarity would be required for such a case with regard to the 'procedure' for expansion which appears to have been focusing only on the case of expansion via delegated acts (see provisions on impact assessment, delegated acts, updating of Annex I).

[19] For example, one-to-one information exchanges under the Professional Qualifications Directive and the Directive on patients' rights in cross-border healthcare follow essentially the same structure and can be accommodated using similar functionalities subject to similar data protection safeguards.

- although the Proposal refers to several existing or planned functionalities, these references are often not sufficiently clear, or sufficiently detailed. This applies, to varying degrees, to references to alerts, external actors, repositories, mutual assistance arrangements, and problem solving.[20] To illustrate, the word 'alert', which refers to a key existing functionality is only mentioned a single time, in recital (10);

- Under the proposed Regulation it is possible to adopt new types of functionalities that are not mentioned in the Proposal at all;

- IMI has thus far been described as an IT tool for information exchange: in other words, a communication tool (see, e.g. Article 3 of the Proposal). Some of the functionalities referred to in the Proposal, including the 'information repository' function, however, appear to go beyond this. The proposed extension of retention periods to five years also suggests a move towards a 'database'. These developments would fundamentally change the character of IMI.[21]

2.2.2. Recommendations

25. To address these uncertainties, the EDPS recommends a two-pronged approach. He proposes, first, that functionalities that are already foreseeable should be clarified and more specifically addressed, and second, that adequate procedural safeguards should be applied to ensure that data protection will also be carefully considered during the future development of IMI.

    Clarification of functionalities already available or foreseeable (e.g. one-to-one exchanges, alerts, repositories, problem solving and external actors)

26. The EDPS recommends that the Regulation should be more specific with respect to functionalities where these are already known, as in the case of the information exchanges referred to in Annexes I and II.

27. For example, more specific and clear measures could be foreseen for the integration of SOLVIT[22] into IMI (provisions for 'external actors' and 'problem-solving') and for the directories of professionals and service providers (provisions for 'repositories').

28. Additional clarifications should also be made regarding 'alerts', which are already in use under the Services Directive and may also be introduced to additional policy areas. In particular, 'alert' as functionality should be clearly defined in Article 5 (along with other functionalities, such as one-to-one information exchanges and repositories). Access rights and retention periods for alerts should also be clarified.[23]

    Procedural safeguards (data protection impact assessment and consultation of data protection authorities)

[20] See recitals (2), (10), (12), (13), (15), and Articles 5(b), 5(i), 10(7) and 13(2).
[21] Incidentally, if there is an intention to have IMI replace/complement existing file handling and archiving systems, and/or to use IMI as a database, this should be made clearer in Article 3.
[22] See Annex II, I(1)).
[23] See Sections 2.4 and 2.5.5 below.

29. If the intention is to keep the Regulation 'future-proof' in terms of additional functionalities that may be necessary in the longer term, and thus, to allow additional functionalities not yet defined in the Regulation, this should be accompanied by adequate procedural safeguards to ensure that appropriate provisions will be made to implement the necessary data protection safeguards before the roll-out of the new functionality. The same should apply to expansions into new policy areas where this has an impact on data protection.

30. The EDPS recommends a clear mechanism that ensures that before each extension of functionalities, or expansions into new policy areas, data protection concerns are carefully evaluated, and, if necessary, additional safeguards or technical measures will be implemented in the architecture of IMI. In particular:

- the impact assessment referred to on page 7 of the Explanatory Memorandum should be specifically required in the Regulation itself, and should also include a data protection impact assessment, which should specifically address what, if any, changes in the design of IMI are necessary to ensure that it continues to contain adequate data protection safeguards covering also the new policy areas and/or functionalities;

- the Regulation should specifically provide that the consultation of the EDPS and national data protection authorities is required before each expansion of IMI. This consultation can take place via the mechanism foreseen for coordinated supervision in Article 20.

31. These procedural safeguards (data protection impact assessment and consultation) should apply to the expansion both via a Commission delegated act (moving an item from Annex II to Annex I), and via a Parliament and Council Regulation including an item that has not been listed in Annex II.

32. Finally, the EDPS recommends that the Regulation should clarify whether the scope of the delegated acts that the Commission will be empowered to adopt pursuant to Article 23 will include any other matters beyond moving items from Annex II to Annex I. If feasible, the Commission should be empowered in the Regulation to adopt specific implementing or delegated acts to further define any additional functionalities of the system, or address any data protection concerns that may arise in the future.

2.3. Roles, competences and responsibilities (Articles 7-9)

33. The EDPS welcomes the dedication of a full chapter (Chapter II) to clarify the functions and responsibilities of the different actors involved in IMI. The provisions could be further strengthened as follows.

34. Article 9 describes the responsibilities that derive from the Commission's role as a controller. The EDPS further recommends the inclusion of an additional provision referring to the Commission's role in ensuring that the system is designed applying the principles of 'privacy by design' as well as its coordinating role with respect to data protection issues.

35. The EDPS is pleased to see that the tasks of IMI coordinators listed in Article 7 now specifically include coordinating tasks relating to data protection, including acting as a

contact person for the Commission. He recommends further clarifying that these coordinating tasks also include contacts with the national data protection authorities.

2.4. Access rights (Article 10)

36. Article 10 provides safeguards with regard to access rights. The EDPS welcomes the fact that following his comments these provisions have been significantly strengthened.

37. Considering the horizontal and expanding nature of IMI, it is important to ensure that the system should guarantee the application of 'Chinese walls' that confine the information processed in one policy area only to that policy area: IMI users should (i) only access information on a need-to-know basis and (ii) confined to a single policy area.

38. If it is unavoidable that an IMI user would be entitled to access information for several policy areas (which may be the case, for example, in some local government offices), at the minimum, the system should not allow the combination of information coming from different policy areas. Exceptions, if necessary, should be set forth in implementing legislation or a Union act, strictly observing the principle of purpose limitation.

39. These principles are now outlined in the text of the Regulation, but could be further strengthened and operationalized.

40. With regard to access rights by the Commission, the EDPS welcomes the fact that Articles 9(2), (4) and 10(6) of the Proposal, taken together, specify that the Commission will have no access to the personal data exchanged among Member States, except in cases where the Commission is designated as a participant to an administrative cooperation procedure.

41. Access rights by external actors, and access right to alerts should also be further specified.[24] With respect to alerts, the EDPS recommends that the Regulation should provide that alerts should not, by default, be sent to all relevant competent authorities in all Member States, but only to those concerned, on a need-to-know basis. This does not exclude sending alerts to all Member States in specific cases or in specific policy areas, if all are concerned. Similarly, a case-by-case analysis is necessary to decide whether the Commission should have access to alerts.

2.5. Retention of personal data (Articles 13 and 14)

2.5.1. Introduction

42. Article 13 of the Proposal extends the length of data storage within IMI from the current six months (to be counted from case closure) to five years, with the data being 'blocked' after 18 months. During the period of 'blockage', data are only accessible following a specific procedure for retrieval, which can only be initiated at the request of the data subject or in case the data are needed 'for purposes of proof of an information exchange by means of IMI'.

[24] See also Section 2.2.2.

43. In effect, thus, data are stored in IMI during three distinct periods:

- from the moment of upload to the moment of case closure;
- from case closure for a period of 18 months[25];
- from the lapse of the period of 18 months, in a blocked form, for a further period of three years and six months (in other words, until the lapse of five years as of case closure).

44. Beyond these general rules, Article 13(2) allows retention of data in a 'repository of information' as long as it is needed for this purpose, with the consent of the data subject or when 'this is necessary to comply with a Union act'. Further, Article 14 provides for a similar blocking mechanism for the retention of personal data of IMI users, for five years, as of the date when they cease to be IMI users.

45. There are no other specific provisions. Therefore, presumably, the general rules are intended to apply not only to one-to-one exchanges, but also to alerts, resolution of problems (as in SOLVIT[26]) and to all other functionalities involving processing of personal data.

46. The EDPS has several concerns regarding the retention periods, in light of Article 6(1)(e) of Directive 95/46/EC and Article 4(1)(e) of Regulation 45/2011, which both require that personal data must be kept no longer than is necessary for the purposes for which the data were collected or are further processed.

2.5.2. From upload to case closure: the need for timely case closure

47. With respect to the first period, from upload of information to case closure, the EDPS is concerned about the risk that some cases might never close, or will be closed only after a disproportionately long period of time. This may lead to some personal data remaining in the database longer than necessary, or even indefinitely.

48. The EDPS understands that the Commission has made progress, on the practical level, to reduce the backlog in IMI and there is a system in place for one-to-one exchanges to monitor timely case closures and to periodically remind those who are lagging behind. In addition, a new change in the functionalities of the system, following a 'privacy by design' approach allows, with the push of a single button, to accept a reply, and to also, at the same time, close the case. Previously this has required two separate steps and may have led to some of the dormant cases that remained in the system.

49. The EDPS welcomes these efforts made at the practical level. However, he recommends that the text of the Regulation itself should provide guarantees that cases will be closed in a timely manner in IMI and that dormant cases (cases without any recent activity) will be deleted from the database.

2.5.3. From case closure to 18 months: is extension of the six months period justified?

50. The EDPS invites reconsidering whether there is an adequate justification for the extension of the current six months period to 18 months following case closure, and if

[25] Article 13(1) suggests that 18 months is a 'maximum' time limit, thus, a shorter period can also be established. This, however, would not have an effect on the total length of retention, which would last, in any event, until the end of five years as of case closure.
[26] See Annex II, I(1)).

so, whether this justification applies to one-to-one information exchanges only, or also to other types of functionalities. IMI has now been in existence for several years, and the practical experience accumulated in this regard should be taken advantage of.

51. If IMI remains a tool for information exchange (as opposed to a file handling system, database, or archiving system), and further provided that the competent authorities are provided with means to retrieve from the system the information they received (either electronically or on a paper form, but in any case in a way that they can use the retrieved information as evidence[27]), there appears to be little need to keep the data in IMI after case closure at all.

52. In one-to-one exchanges of information the potential need to ask follow-up questions even after an answer has been accepted, and thus, a case has been closed, may perhaps justify a (reasonably short) period of retention following case closure. The current six-month period *prima facie* appears to be generous enough for this purpose.

2.5.4. From 18 months to five years: 'blocked' data

53. The EDPS considers that the Commission has also not provided sufficient justification for the necessity and proportionality of retention of 'blocked data' up to a period of five years.

54. The Explanatory Memorandum, on page 8, refers to the Court of Justice ruling in *Rijkeboer*[28]. The EDPS recommends that the Commission should reconsider the implications of this case on data retention in IMI. In his view, *Rijkeboer* does not require IMI to be configured to retain data for five years after case closure.

55. The EDPS does not consider reference to the *Rijkeboer* judgment or to the rights of data subjects to have access to their data as a sufficient and adequate justification for retaining data in IMI for five years after case closure. Retention of merely 'log data' (strictly defined to exclude any content, among others, any attachments or sensitive data) may be a less intrusive option, which might deserve some further consideration. However, the EDPS, at this stage, is not convinced that even this would be either necessary or proportionate.

56. In addition, lack of clarity as to who can access the 'blocked data' and for what purposes is also problematic. Simply referring to use 'for purposes of proof of an information exchange' (as in Article 13(3)) is not sufficient. If the provision regarding 'blocking' is retained, in any event, it should be better specified who can ask for a proof of the information exchange and in what context. In addition to the data subject, would others be entitled to request access? If so, would these be solely the competent authorities, and solely in order to prove that a particular information exchange with a particular content took place (in case such an exchange is contested by the competent authorities who sent or received the message)? Are other possible uses 'for purposes of proof of an information exchange' foreseen? [29]

[27] We understand that efforts have been made to ensure this at the practical level.
[28] C-553/07 *Rijkeboer* [2009] ECR I-3889.
[29] Although retention of personal poses comparatively less risks to privacy, the EDPS nevertheless considers that retention of personal data of IMI users for a period of five years once they no longer have access to IMI has also not been sufficiently justified.

2.5.5. Alerts

57. The EDPS recommends that a more clear distinction should be made between alerts and repositories of information. It is one thing to use an alert as a communication tool to alert competent authorities of a particular wrongdoing or suspicion, and quite another to store this alert in a database for an extended or even undefined period of time. Storing alert information would raise additional concerns and would require specific rules and additional data protection safeguards.

58. Therefore, the EDPS recommends that the Regulation should provide, as a default rule that (i) -unless otherwise specified in vertical legislation, and subject to adequate additional safeguards- a six month retention period should apply to alerts and, importantly, that (ii) this period should be counted as of the time of sending the alert.

59. Alternatively, the EDPS recommends that detailed safeguards, with respect to alerts, would be specifically set forth in the proposed Regulation. The EDPS is ready to assist the Commission and the legislators with further advice in this respect, should this second approach be followed.

2.6. Special categories of data (Article 15)

60. The EDPS welcomes the distinction made between the personal data referred to in Article 8(1) of Directive 95/46/EC on one hand, and the personal data referred to in Article 8(5) on the other hand. He also welcomes that the Regulation clearly specifies that special categories of data may only be processed on the basis of a specific ground mentioned in Article 8 of Directive 95/46/EC.

61. In this regard, the understanding of the EDPS is that IMI will process a significant amount of sensitive data falling under Article 8(2) of Directive 95/46/EC. Indeed, IMI, from the very beginning, when it was first rolled out to support administrative cooperation under the Services and Professional Qualifications Directives, was designed to process such data, in particular, data relating to records of criminal and administrative infringements that may have an effect on a professional's or service provider's right to perform work/services in another Member State.

62. Additionally, a significant amount of sensitive data under Article 8(1) (mainly health-related data) will also likely be processed in IMI once IMI will expand to include a module for SOLVIT[30]. Finally, it cannot be excluded that additional sensitive data may also be collected through IMI in the future, on an *ad hoc* or systematic basis.

2.7. Security (Article 16 and recital 16)

63. The EDPS is pleased to see that Article 16 specifically refers to the obligation of the Commission to follow its own internal rules adopted to comply with Article 22 of Regulation 45/2001 and to adopt and keep up-to-date a security plan for IMI.

64. To further strengthen these provisions, the EDPS recommends that the Regulation requires a risk assessment and a review of the security plan before each expansion of IMI to a new policy area or before adding a new functionality with an impact on personal data.[31]

[30] See Annex II, I(1)).
[31] Please also see Section 12 on recommendations regarding audits.

65. In addition, the EDPS also notes that Article 16 and recital 16 refer only to the obligations of the Commission and the supervisory role of the EDPS. This reference may be misleading. While it is true that the Commission is the operator of the system, and as such, is responsible for a predominant part of the maintenance of the security in IMI, competent authorities also have obligations, which are, in turn, supervised by national data protection authorities. Therefore, Article 16 and recital 16 should also refer to the obligations on security applicable to the rest of the IMI actors pursuant to Directive 95/46/EC and to the supervisory powers of national data protection authorities.

2.8. Information to data subjects and transparency (Article 17)

2.8.1. Information provided in Member States

66. With regard to Article 17(1), the EDPS recommends more specific provisions in the Regulation to ensure that data subjects will be fully informed of the processing of their data in IMI. Considering that IMI is used by multiple competent authorities, including many small local government offices without sufficient resources, it is strongly recommended that notice provision be coordinated at the national level.

2.8.2. Information provided by the Commission

67. Article 17(2)(a) requires the Commission to provide a privacy notice regarding its own data processing activities, under Articles 10 and 11 of Regulation 45/2001. In addition, Article 17(2) (b) requires the Commission to also provide information on 'the data protection aspects of administrative cooperation procedures in IMI as referred to in Article 12'. Finally, Article 17(2)(c) requires the Commission to provide information on 'exceptions to or limitations of data subjects' rights as referred to in Article 19'.

68. The EDPS is pleased to see these provisions that help contributing to transparency of the data processing operations in IMI. As noted in Section 2.1 above, in case of an IT system used in 27 different Member States, it is crucial to ensure consistency regarding the operation of the system, the data protection safeguards applied, and the information that is provided to the data subjects. [32]

69. That said, the provisions of Article 17(2) should be further strengthened. The Commission, as the operator of the system, is best positioned to take a proactive role in providing a first 'layer' of data protection notice and other relevant information to data subjects on its multilingual website, also 'on behalf of' competent authorities, that is, covering the information required under Articles 10 or 11 of Directive 95/46/EC. It would then often be sufficient for notices provided by competent authorities in Member States to simply refer to the notice provided by the Commission, only complementing it as necessary to comply with any specific additional information specifically required under national law.

70. In addition, Article 17(2)(b) should clarify that information provided by the Commission will comprehensively cover all policy areas, all types of administrative cooperation procedures and all functionalities within IMI and will also specifically include the categories of data that may be processed. This should also include the

[32] This approach to ensure consistency should, of course, take duly into account any national divergences when necessary and justified.

publication of the question sets used in one-to-one cooperation on the IMI website as is currently done in practice.

2.9. Rights of access, rectification and erasure (Article 18)

71. The EDPS would like to refer again, as noted in Section 2.1 above, to the fact that it is crucial to ensure consistency regarding the operation of the system and the data protection safeguards applied. For this reason, the EDPS would further specify the provisions on the rights of access, correction and erasure.

72. Article 18 should specify whom data subjects should turn to with an access request. This should be clear with respect to access to data during the different time periods:

    - prior to case closure,
    - after case closure but before the lapse of the 18 months retention period,
    - and finally, during the period of time while data are 'blocked'.

73. The Regulation should also require competent authorities to cooperate with respect to access requests as necessary. Correction and deletion should be carried out 'as soon as possible but within 60 days at the latest' rather than 'within 60 days'. Reference should also be made to the possibility for building a data protection module and the possibility of 'privacy by design' solutions for cooperation among authorities regarding access rights, as well as 'empowerment of data subjects', for example, by providing them direct access to their data, where relevant and feasible.

2.10. Supervision (Article 20)

74. In recent years the model of 'coordinated supervision' has been developed. This model of supervision, as now operational in EURODAC and parts of the Customs Information System, has also been adopted for the Visa Information System (VIS) and the second generation Schengen Information System (SIS-II).

75. This model has three layers:

    - supervision at national level is ensured by national data protection authorities;
    - supervision at EU level is ensured by the EDPS;
    - coordination is ensured by way of regular meetings and other coordinated activities supported by the EDPS acting as the secretariat of this coordination mechanism.

76. This model has proven to be successful and effective and should be envisaged in the future for other information systems.

77. The EDPS welcomes the fact that Article 20 of the Proposal specifically provides for coordinated supervision among national data protection authorities and the EDPS following - in broad terms - the model established in the VIS and SIS II Regulations[33].

[33] See Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4) and Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

78. The EDPS would strengthen the provisions on coordinated supervision at certain points and would for that purpose support similar provisions as those in place for example in the context of the Visa Information System (Articles 41-43 of the VIS Regulation), Schengen II (Articles 44-46 of the SIS-II Regulation) and envisaged for EURODAC[34]. In particular, it would be helpful if the Regulation would:

- in Article 20(1) and (2) set out and divide more clearly the respective supervision tasks of national data protection authorities and the EDPS[35];

- in Article 20(3) specify that the national data protection authorities and the EDPS, each acting within the scope of their competences, 'shall cooperate actively' and 'shall ensure coordinated supervision of IMI' (rather than simply referring to coordinated supervision without mentioning active cooperation)[36]; and

- specify, in more detail, what cooperation may include, for example, by requiring that the national data protection authorities and the EDPS 'each acting within the scope of their respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of the IMI Regulation, study problems with the exercise of independent supervision or with the exercise of the rights of data subjects, draw up harmonized proposals for joint solutions to any problems and promote awareness of data protection rights as necessary'.[37]

79. This being said, the EDPS is conscious of the present smaller size, the different nature of the data processed, as well as the evolving nature of IMI. Therefore, he acknowledges that regarding the frequency of meetings and audits, more flexibility may be advisable. In short, the EDPS recommends that the Regulation should provide the necessary minimal rules to ensure effective cooperation, but not create unnecessary administrative burdens.

80. Article 20(3) of the Proposal does not require regular meetings but simply provides that the EDPS may 'invite the National Supervisory Authorities to meet ... when necessary'. The EDPS welcomes the fact that these provisions leave it up to the parties concerned to decide on the frequency and modalities of the meetings, and other procedural details regarding their cooperation. These can be agreed upon in the rules of procedures, which are already referred to in the Proposal.

81. With regard to regular audits, it may also be more effective to leave it to the cooperating authorities to determine, in their rules of procedures, when, and with what frequency, such audits should be held. This may depend on a number of factors and may also change over time. Therefore, the EDPS supports the Commission's approach, which allows for more flexibility also in this regard.

[34] Council Regulation 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000, currently under revision. In this context, similar provisions are considered as in the VIS and SIS II Regulations.
[35] See, for example, Articles 41 and 42 of the VIS Regulation.
[36] See, for example, Article 43(1) of the VIS Regulation.
[37] See, for example, Article 43(2) of the VIS Regulation.

2.11. National use of IMI

82. The EDPS welcomes the fact that the Proposal provides a clear legal basis for the national use of IMI and that such use is subject to several conditions, including the fact that the national data protection authority must be consulted and that the use must be in accordance with national law.

2.12. Information exchange with third countries (Article 22)

83. The EDPS welcomes the requirements set in Article 22(1) for information exchanges, as well as the fact that Article 22(3) ensures the transparency of the expansion via publication in the Official Journal of an updated list of third countries using IMI (Article 22(3)).

84. The EDPS further recommends that the Commission should narrow the reference made to the derogations under Article 26 of Directive 95/46/EC to include only Article 26(2). In other words: competent authorities or other external actors in a third country that does not afford adequate protection should not be able to have direct access to IMI unless there are appropriate contractual clauses in place. These clauses should be negotiated at the EU level.

85. The EDPS emphasises that other derogations such as 'transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims', should not be used to justify data transfers to third countries using direct access to IMI.[38]

2.13. Accountability (Article 26)

86. In line with the expected strengthening of arrangements for greater accountability during the review of the EU data protection framework[39], the EDPS recommends that the Regulation should establish a clear framework for adequate internal control mechanisms that ensures data protection compliance and provides evidence thereof, containing at least the elements noted below.

87. In this context, the EDPS welcomes the requirement in Article 26(2) of the Regulation that the Commission should report, every three years, to the EDPS on data protection aspects, including on security. It would be advisable if the Regulation would clarify that the EDPS, in turn, would be required to share the Commission's report with the national data protection authorities, in the framework of the coordinated supervision referred to in Article 20. It would also be helpful to clarify that the report should discuss, with respect to each policy area and each functionality, how the key data protection principles and concerns (e.g. information to data subjects, access rights, security) have been addressed in practice.

88. In addition, the Regulation should clarify that the framework for internal control mechanisms should also include privacy assessments (also including a security risk

[38] A similar approach has been followed in Article 22(2) for the Commission as an IMI actor.

[39] See Section 2.2.4 of the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - 'A comprehensive approach on personal data protection in the European Union', COM(2010) 609 final. See also Section 7 of the EDPS opinion issued on this Commission Communication on 14 January 2011.

analysis), a data protection policy (including a security plan) adopted based on the results of these, as well as periodic reviews and auditing.

2.14. Privacy by design

89. The EDPS welcomes the reference in recital (6) of the Regulation to this principle.[40] He recommends that beyond this reference, the Regulation should also introduce specific privacy by design safeguards such as:

    - a data protection module to allow data subjects to more effectively exercise their rights[41];
    - clear isolation of the different policy areas included in IMI ('Chinese walls')[42];
    - specific technical solutions to limit search capabilities in directories, alert information and elsewhere, to ensure purpose limitation;
    - specific measures to ensure that cases with no activity will be closed[43];
    - adequate procedural safeguards in the context of future developments.[44]

3. CONCLUSIONS

90. The overall views of the EDPS on IMI are positive. The EDPS supports the aims of the Commission in establishing an electronic system for the exchange of information and regulating its data protection aspects. The EDPS also welcomes the fact that the Commission proposes a horizontal legal instrument for IMI in the form of a Parliament and Council Regulation. He is pleased that the Proposal comprehensively highlights the most relevant data protection issues for IMI.

91. With regard to the legal framework for IMI to be established in the proposed Regulation, the EDPS calls attention to two key challenges:

    - the need to ensure consistency, while respecting diversity, and
    - the need to balance flexibility and legal certainty.

92. Functionalities of IMI that are already foreseeable should be clarified and more specifically addressed.

93. Adequate procedural safeguards should be applied to ensure that data protection will be carefully considered during the future development of IMI. This should include an impact assessment and consultation of the EDPS and national data protection authorities before each expansion of IMI's scope to a new policy area and/or to new functionalities.

94. Access rights by external actors and access right to alerts should be further specified.

95. With regard to retention periods:

[40] *Idem.*
[41] See Section 2.9 above.
[42] See Section 2.4 above.
[43] See Section 2.5.2 above.
[44] See Section 2.2.2 above.

- the Regulation should provide guarantees that cases will be closed in a timely manner in IMI and that dormant cases (cases without any recent activity) will be deleted from the database;

- it should be reconsidered whether there is an adequate justification for the extension of the current six months period to 18 months following case closure;

- the Commission has not provided sufficient justification for the necessity and proportionality of retention of 'blocked data' up to a period of five years, and therefore, this proposal should be reconsidered;

- a more clear distinction should be made between alerts and repositories of information: The Regulation should provide, as a default rule that (i) - unless otherwise specified in vertical legislation, subject to adequate additional safeguards - a six month retention period should apply to alerts and that (ii) this period should be counted as of the time of sending the alert.

96. The Regulation should require a risk assessment and a review of the security plan before each expansion of IMI to a new policy area or before adding a new functionality with an impact on personal data.

97. The provisions on information to data subjects and access rights should be strengthened and should encourage a more consistent approach.

98. The EDPS would strengthen the provisions on coordinated supervision at certain points and would for that purpose support similar provisions as those in place for example in the context of the Visa Information System, Schengen II and envisaged for EURODAC. With regard to the frequency of meetings and audits, the EDPS supports the Proposal in its flexible approach aimed to ensure that the Regulation provides the necessary minimal rules to ensure effective cooperation without creating unnecessary administrative burdens.

99. The Regulation should ensure that competent authorities or other external actors in a third country that does not afford adequate protection should not be able to have direct access to IMI unless there are appropriate contractual clauses in place. These clauses should be negotiated at the EU level.

100. The Regulation should establish a clear framework for adequate internal control mechanisms that ensures data protection compliance and provides evidence thereof, including privacy assessments (also including a security risk analysis), a data protection policy (including a security plan) adopted based on the results of these, as well as periodic reviews and auditing.

101. The Regulation should also introduce specific privacy by design safeguards.

Done in Brussels, 22 November 2011

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor