

EN

EN

EN



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 26.3.2009  
C(2009) 2041 final

**COMMISSION RECOMMENDATION**

**of 26.3.2009**

**Commission Recommendation on data protection guidelines for the Internal Market  
Information System (IMI)**

## COMMISSION RECOMMENDATION

of 26.3.2009

### Commission Recommendation on data protection guidelines for the Internal Market Information System (IMI)

(Text with EEA relevance)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community, and in particular Article 211, second indent, thereof,

After consulting the European Data Protection Supervisor,

Whereas:

- (1) Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC)<sup>1</sup>, and in particular Article 4 thereof, provides for the implementation of projects of common interest, in order to enable the efficient, effective and secure interchange of information between public administrations at all appropriate levels, as well as between such administrations and the Community institutions or other entities as appropriate.
- (2) On 17 March 2006, Member States representatives in the Internal Market Advisory Committee<sup>2</sup> approved the Global Implementation Plan for the Internal Market Information System, hereinafter: "IMI", and its development aimed at improving communication among Member State administrations.
- (3) Further to this approval, the Commission decided on the financing and setting up of the Internal Market Information System as a project of common interest in Decisions C/2006/3606 of 14 August 2006, C/2007/3514 of 25 July 2007 and C/2008/1881 of 14 May 2008.
- (4) The aim of IMI is to give support to relevant Community acts that require the exchange of information between Member States administrations, including Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications<sup>3</sup> and Directive 2006/123/EC of the

---

<sup>1</sup> OJ L 144, 30.4.2004, as corrected by OJ L 181, 18.5.2004, p. 25.

<sup>2</sup> Set up by Commission Decision 93/72/EEC (OJ L 26, 3.2.1993, p. 18).

<sup>3</sup> OJ L 255, 30.9.2005, p. 22. Directive as last amended by Commission Regulation (EC) No 1137/2008 (OJ L 311, 21.11.2008, p. 1-54)

European Parliament and of the Council of 12 December 2006 on services in the internal market<sup>4</sup>.

- (5) The exchange of information by electronic means between Member States and between Member States and the Commission should comply with the rules on the protection of personal data laid down in 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<sup>5</sup> and in 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<sup>6</sup>.
- (6) The right to data protection is recognised by the Charter of Fundamental Rights of the European Union, in particular in Article 8 thereof; information systems such as IMI should ensure that the different responsibilities and obligations shared between the Commission and the Member States as regards data protection rules are clear and that data subjects are provided with simple and easily available mechanisms to assert their rights.
- (7) The Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (COM 2008/49/EC) laid down the functions, rights and obligations of the IMI actors and IMI users. This Commission decision took into account the opinion of the Article 29 Working Party<sup>7</sup>.
- (8) Further to the adoption of this Decision, the European Data Protection Supervisor (EDPS) adopted an opinion<sup>8</sup> where it called for the adoption of a legal instrument, preferably in the form of a Council and Parliament Regulation in view of the fact that IMI is expected to gradually broaden its scope to additional areas of internal market legislation with increased complexity and an increasing number of participating authorities and data exchanges. In several meetings and in an exchange of letters between the EDPS and the Commission services<sup>9</sup> it was agreed to follow a step by step approach which would start with the adoption of data protection guidelines, to be drawn up in close consultation with the EDPS.
- (9) These guidelines complement Commission Decision 2008/49/EC and take into account both the recommendations of the Article 29 Working Party and the EDPS.

---

<sup>4</sup> OJ L 376, 27.12.2006, p. 36.

<sup>5</sup> OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

<sup>6</sup> OJ L 8, 12.1.2001, p. 1.

<sup>7</sup> Opinion 01911/07/EN, WP 140.

<sup>8</sup> Opinion of the European Data Protection Supervisor ("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 of 22 February 2008, OJ C 270, 25.10.2008, p. 1.

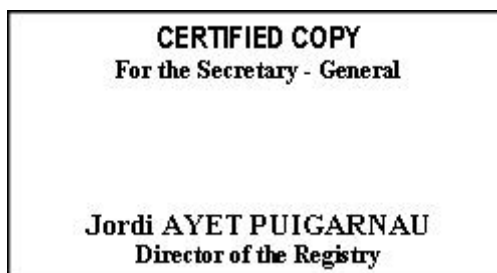
<sup>9</sup> <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/87>

HEREBY RECOMMENDS THAT MEMBER STATES SHOULD:

- (1) Take steps to ensure the implementation of the guidelines in the Annex among actors and users of IMI.
- (2) Encourage national IMI coordinators to make contacts with their national Data Protection Authorities for guidance and assistance on the best way to implement these guidelines under national law.
- (3) Provide feedback to the European Commission on the implementation of the guidelines in the Annex, not later than nine months after the adoption of this Recommendation and with the assistance of the national IMI coordinators. This feedback will be taken into account by the European Commission in a report it will draw up not later than one year after the adoption of this Recommendation in which it will assess the data protection situation in IMI as well as the content and timeliness of any future measures including the possible adoption of a legal instrument.

Done at Brussels, 26.3.2009

*For the Commission*  
*Charlie McCreevy*  
*Member of the Commission*

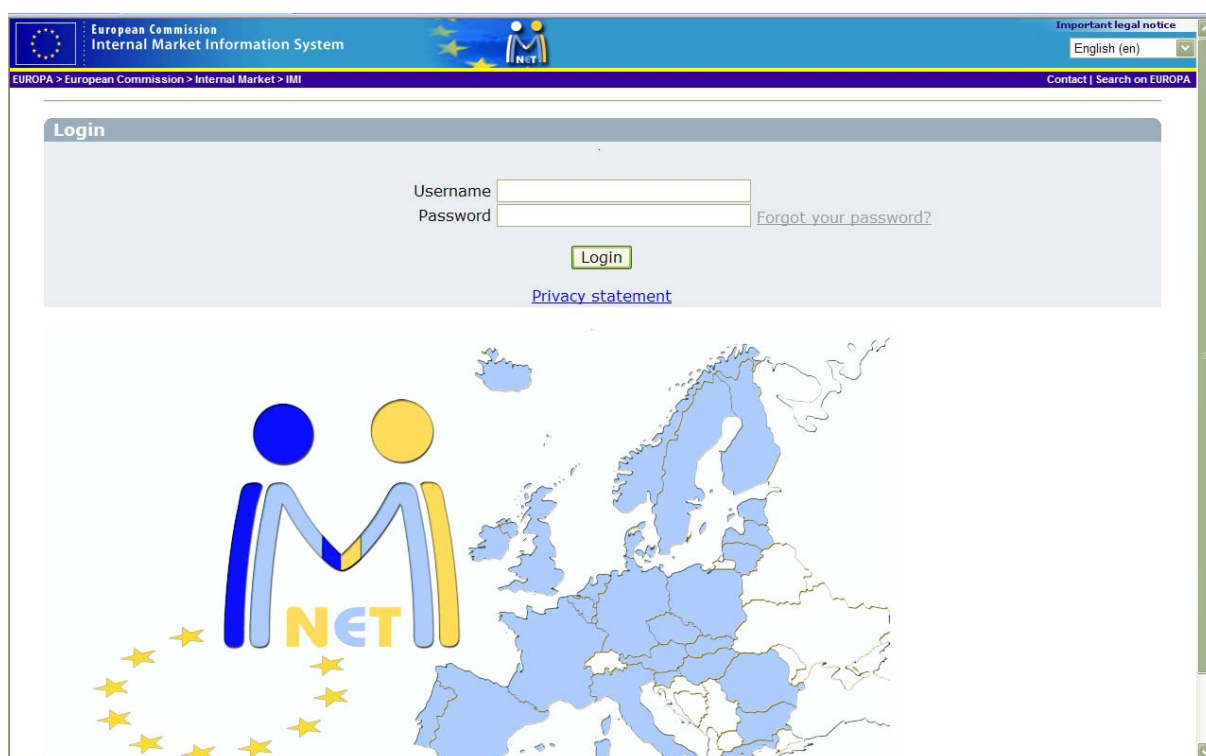


## ANNEX

### **Guidelines for the implementation of data protection rules in IMI**

#### **1. IMI - a tool for administrative cooperation**

IMI is a software application accessible via the Internet designed by the European Commission in cooperation with the Member States. Its main goal is to assist Member States with the practical implementation of EU legislation that provides for mutual assistance and administrative cooperation. IMI is not a database aimed at storing information for long periods of time but rather a centralised mechanism to allow national administrations of the EEA Member States to exchange information, with limited data retention periods.



*IMI login page*

IMI currently supports exchanges of information under the Professional Qualifications Directive and it will also support exchanges of information under the Services Directive from the end of 2009. In the future it may support exchanges of information for additional legislative areas of the Internal Market. At all times you will be able to find an updated list of these legislative areas in the annex to Commission Decision 2008/49/EC. This annex will be amended from time to time. IMI cannot be used for information exchanges in legislative areas not specifically listed in this annex.

The screenshot shows the 'Settings for Professional Qualifications' interface. It has a navigation bar at the top with tabs: Country and Languages, Address, Areas of competence, User Details, Legislative areas, and Settings for Professional Qualifications. Below this is the 'Legislative area Professional Qualifications' header. The main content is split into two sections: 'Profession' and 'Keywords'. Each section contains a search bar, a list of available keywords, and a list of selected keywords. In the 'Profession' section, available keywords include Accountant, Architect, Dentist, Doctor, Midwife, and Nurse. In the 'Keywords' section, available keywords include Diploma, Local, National, Recognition, Regional, and Supervision. Navigation buttons (>, <, >>, <<) are used to move keywords between the lists.

*Example of the view of the application concerning competent authorities dealing with professional qualifications*

Cooperation between national administrations is vital for the Internal Market to function well. European citizens cannot benefit from basic internal market rights such as the freedom of establishment in another Member State or the freedom to provide services cross border without practical arrangements for administrative cooperation in place.

#### A couple of examples

A German doctor resident in Berlin marries a French man and decides to start a new life in Paris. The German doctor wants to practice her profession in France and therefore submits titles and diplomas to the Order of Doctors in France. The person dealing with the file has doubts about the authenticity of one of the diplomas and uses IMI to check with the competent authority in Berlin.

A French industrial cleaning company operating in France also provides cleaning services across the border in the Catalan region (Spain). A Spanish NGO lodges a complaint with the Catalan environmental department stating that the French company does not have the specialised work force required to handle certain cleaning substances. The Catalan competent authority uses IMI to find out whether the cleaning company is operating legally in France.

Administrative cooperation in the EU is not an easy task. There are language barriers (the EU has 23 official languages), lack of administrative procedures for cross-border cooperation, different administrative structures and cultures and lack of clearly identified partners in other Member States.

Although it is up to Member States to ensure that Internal Market laws work effectively on their territories, the Commission believes that Member States need the tools to work together. IMI has been designed with this idea in mind: to identify the appropriate competent authority in another Member State (search function), to manage the exchanges of information on the basis of simple and unified procedures and to remove the linguistic barriers on the basis of pre-defined and pre-translated question sets.

**Questions** Hide translations

When entering free text please indicate the language you are using in the dropdown next to the text box. If possible use a language which is understood by the Requesting Authority. The Requesting Authority has indicated that it understands the following languages: English (en), français (fr), Deutsch (de), español (es)

Questions to identify the profession  
 Identification of the profession

1. Is the profession [pharmacist] regulated in your territory? [Link](#)

Answer:  en

Answer comments:

2. Which are the professional activities covered by the profession [pharmacist] in your territory? [Link](#)

Answer:

Answer comments:  en

Professional Title

3. What is the professional title for the exercise of the profession of [pharmacist] in your territory? [Link](#)

Answer:  en

Answer comments:  en

Questions to identify the qualification  
 Holder of qualification

4. What is the professional qualification delivered in your territory to [Mr. Philippe BOULANGER]?

Answer:  en

Answer comments:  en

**Questions** Cacher les traductions

Lorsque vous rédigez un texte libre, veuillez indiquer la langue que vous utilisez dans le menu déroulant situé à côté de l'encadré. Utilisez si possible une langue comprise par l'autorité requérante. L'autorité requérante a indiqué qu'elle comprenait les langues suivantes: English (en), français (fr), Deutsch (de), español (es)

Questions concernant la profession  
 Identification de la profession

1. La profession de/d' [pharmacien] est-elle réglementée sur votre territoire? [Lien](#)

Réponse:  fr

Commentaires concernant la réponse:

2. Quelles activités professionnelles recouvre la profession de/d' [pharmacien] sur votre territoire? [Lien](#)

Réponse:  fr

Commentaires concernant la réponse:  fr

Titre professionnel

3. Quel titre professionnel doit-on détenir pour exercer la profession de/d' [pharmacien] sur votre territoire? [Lien](#)

Réponse:  fr

Commentaires concernant la réponse:  fr

Questions concernant les qualifications professionnelles  
 Titulaire du titre de formation

4. Quelles qualifications professionnelles [M. Philippe BOULANGER] a-t-il/elle reçues sur votre territoire?

Réponse:  fr

Commentaires concernant la réponse:  fr

*Screenshots showing questions in the languages of two competent authorities involved in an information exchange*



## 2. Scope and objective of these guidelines

IMI users are experts in their respective fields of competence, whether it is the rules governing a profession or the regulations in place for the provision of services. However, they are not data protection experts and they may not always be sufficiently aware of the data protection requirements imposed by their own national data protection legislation.

Therefore it is advisable to provide IMI users with guidelines in which the functioning of IMI is explained from the data protection perspective as well as the safeguards built into the system and the possible risks associated with its use<sup>10</sup>.

These guidelines are not intended to be a comprehensive review of all data protection issues in connection with IMI but a user-friendly explanation, a compliance framework that all IMI users can understand. In case of need, IMI users can always obtain further guidance and assistance from the data protection authorities in the Member States. A list of these authorities with contact details and websites can be found here:

[http://ec.europa.eu/justice\\_home/fsj/privacy/nationalcomm/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm)

## 3. A data protection friendly environment

IMI has been developed with the requirements of data protection legislation in mind and is data protection friendly from its conception.

IMI users can be reassured that IMI is a reliable software application from the data protection point of view and some simple examples may easily illustrate this point:

- a) IMI is only used by competent authorities inside the European Economic Area (EU Member States plus Norway, Iceland and Lichtenstein) and there are no transfers of personal data outside the EEA.
- b) The European Commission and the IMI coordinators<sup>11</sup> have no access to the personal data of professionals or service providers exchanged in the system.
- c) Only the competent authorities involved in a request for information are allowed to see the personal data of the service provider<sup>12</sup>. In fact, the protection goes so far as to prevent the addressee of a request from seeing the personal information on the service provider until the addressee has formally accepted it.

---

<sup>10</sup> Members States should consider including information on data protection in their training actions on IMI.

<sup>11</sup> See Article 12 of Decision 2008/49/EC.

<sup>12</sup> Competent authorities may have other authorities "linked" for supervision (e.g. a regional authority links a federal authority). These "linked authorities" can in this way be made aware of the number and the nature of the requests but they have no access to the personal data of the service providers or the migrant professionals.

Details of the professional		Hide translations
Profession	pharmacist	
Title	*****	
First Name	*****	
Surname	*****	
Nationality	French	
Place of birth	*****	
Date of birth (dd/mm/yyyy)	*****	
Country	France	
Region / Area	Paris	
Town	Paris	
Postcode	*****	
Street and number	*****	
E-mail		
Justification for the request	Reasonable and justified doubts about the authenticity of the document	

Questions		Hide translations
When entering free text please indicate the language you are using in the dropdown next to the text box. If possible use a language which is understood by the Requesting Authority. The Requesting Authority has indicated that it understands the following languages: español (es), čeština (cs)		
<ul style="list-style-type: none"> <li>☐ Questions to identify the profession               <ul style="list-style-type: none"> <li>☐ Identification of the profession                   <ul style="list-style-type: none"> <li>1. Is the profession [pharmacist] regulated in your territory? <a href="#">Link</a></li> <li>2. Which are the professional activities covered by the profession [pharmacist] in your territory? <a href="#">Link</a></li> </ul> </li> <li>☐ Questions related to the professional                   <ul style="list-style-type: none"> <li>☐ Nationality                       <ul style="list-style-type: none"> <li>3. Is [*****] a national of your Member State? <a href="#">Link</a></li> </ul> </li> </ul> </li> <li>☐ Questions regarding the exercise of the profession                   <ul style="list-style-type: none"> <li>☐ Legal establishment within the EU                       <ul style="list-style-type: none"> <li>4. For the exercise of which profession is [*****] legally established in your territory? <a href="#">Link</a></li> </ul> </li> <li>☐ File for recognition                       <ul style="list-style-type: none"> <li>5. According to the national legislation applicable in your territory, are you able to formally issue a document concerning the good character or repute with regard to [*****]? <a href="#">Link</a></li> <li>6. According to the national legislation applicable in your territory, are you able to formally issue a document concerning the absence of bankruptcy with regard to [*****]? <a href="#">Link</a></li> <li>7. According to the national legislation applicable in your territory, are you able to formally issue a document concerning the absence of suspension or prohibition of the pursuit of the relevant professional activities for serious professional misconduct or criminal offence with regard to [*****]? <a href="#">Link</a></li> <li>8. According to the national legislation applicable in your territory, are you able to formally issue a document concerning the physical health of [*****]? <a href="#">Link</a></li> </ul> </li> </ul> </li> </ul> </li> </ul>		

*Example of the view of a request before acceptance by the recipient*

d) All personal data relating to requests are automatically deleted from the system six months after the closure of a request or even before if requested by the competent authorities involved (for more details, see chapter 12 on retention period).

#### 4. Who is who in IMI? The issue of joint controllership

IMI is a clear example of joint processing operations and joint controllership. For example, whilst only the competent authorities in the Member States exchange personal data, the storage of these data on its servers is the responsibility of the European Commission. Whilst the European Commission is not allowed to see this personal data it is the operator of the system who physically processes the deletion and rectification of the data.

In other words and as a result of the allocation of different responsibilities between the Commission and the Member States:

a) Each competent authority and each IMI coordinator is a controller with respect to its own data processing activities,

b) The Commission is not a user, but the operator of the system, responsible, primarily, for maintenance and security of the system,<sup>13</sup>

---

<sup>13</sup> As provided for in Article 10.3 of Commission Decision 2008/49/EC, the Commission may participate in information exchanges only in specific cases where the relevant Community act provides for information to be exchanged between Member States and the Commission. In these cases the Commission has similar obligations as if it were a competent authority. For example, it needs to provide appropriate notice to the data subjects as well as access to their data if they so request.

c) The IMI actors share responsibility with respect to notice provisions and rights of access, objection and rectification.

In complex scenarios of joint controllership like IMI, it seems most efficient from the perspective of compliance to embed data protection in the system from the beginning (see section: "Work in Progress" under chapter 13: "Cooperation with data protection authorities and the EDPS") and to define a compliance framework as provided in these guidelines. Compliance with the framework is the responsibility of all IMI actors and users.

## **5. Actors and users in IMI**

All actors which use IMI are validated by IMI coordinators. Actors and users as well as their functions, rights and obligations are described in detail in Articles 6 to 12 of Commission Decision 2008/49/EC. There is therefore no need for these guidelines to repeat these.

It is important to understand that IMI is a very flexible system whereby Member States may allocate responsibilities and functions to competent authorities and coordinators in many different ways in order to fit their particular administrative structure and the legislative areas to be covered by administrative cooperation.

It is also important to bear in mind that IMI users in the Member States are responsible for many other processing operations. Data protection compliance in IMI does not need to be unduly complicated or pose an excessive administrative burden. Neither does it have to be a one-size fits all system.

In most cases competent authorities simply need to carry out the processing operations inside IMI under the same rules and good practices that they normally have in place as data controllers according to their own particular needs and the data protection laws of their Member States.

They should also take advantage of the data protection-friendly environment offered within IMI. For example, they are encouraged to request that the personal data exchanged will be deleted from IMI even before the six months retention period lapses, if they no longer need to keep the information exchange in IMI.

## **6. Legal grounds for the exchanges of personal information in IMI**

The Commission has adopted Decision 2008/49/EC which sets out the functions, rights and obligations of IMI actors and users concerning the implementation of IMI as regards the protection of personal data.

Not all information exchanged in IMI is personal data. For example, the information exchanged may concern legal persons<sup>14</sup> or the question and answer may not relate to any given individual (e.g. a general question as to whether a profession is regulated in a given Member State).

In many cases, however, the exchanges of information do concern individuals and therefore there must be legal grounds for the processing of personal data. The use of IMI is often in the

---

<sup>14</sup> Although in some Member States such as Italy, Luxembourg, Austria and Denmark the scope of data protection legislation also covers legal persons to a certain extent.

interest of the data subject. Nevertheless, even if the exchange of information is not necessarily in the interest of the data subject, it may be exchanged using IMI by competent authorities, provided that such exchange is required by a specific legal basis.

Article 7 of Directive 95/46/EC lists the legal grounds for the processing of personal data. Of these, Article 7 c and Article 7 e are the most relevant for exchanges of data within IMI.

#### I) Compliance with a legal obligation (Article 7 c)

As a general principle, EU Member States have the duty to cooperate with each other and with the Community Institutions. The duty of administrative cooperation is explicit and specific in Directive 2005/36/EC (Recognition of Professional Qualifications) and Directive 2006/123/EC (Services Directive).

Article 56 of the Professional Qualifications Directive provides as follows:

*“1. The competent authorities of the host Member State and of the home Member State shall work in close collaboration and shall provide mutual assistance in order to facilitate application of this Directive. They shall ensure the confidentiality of the information which they exchange.*

*“2. The competent authorities of the host and home Member States shall exchange information regarding disciplinary action or criminal sanctions taken or any other serious, specific circumstances which are likely to have consequences for the pursuit of activities under this Directive, respecting personal data protection legislation provided for in Directives 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) and 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.)”*

Article 28 of the Services Directive provides as follows:

*“1. Member States shall give each other mutual assistance, and shall put in place measures for effective cooperation with one another, in order to ensure the supervision of providers and the services they provide...*

*“6. Member States shall supply the information requested by other Member States or the Commission by electronic means and within the shortest possible period of time.”*

Article 34 of the Services Directive provides as follows:

*“1. The Commission, in cooperation with Member States, shall establish an electronic system for the exchange of information between Member States, taking into account existing information systems”.*

II) The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 7 e).

IMI actors and users carry out tasks in the public interest or in the exercise of official authority vested in them. All registrations in IMI are validated by the IMI Coordinator after

making sure that the competent authority in question does carry out tasks either in the public interest (for example doctors or veterinary bodies ensuring that their members conform to ethical or sanitary rules) or in the exercise of official authority vested in them (e.g. Ministries of Education ensuring that secondary education teachers have the correct qualifications).

Based on the foregoing, you may use IMI to exchange personal data under the Professional Qualifications and Services Directives for the purposes set out in their provisions. Information in relation to other internal market legislation cannot be exchanged in IMI. If the scope of IMI is at any stage widened to include additional legislation, appropriate reference to the relevant Community acts will be added to the annex of Commission Decision 2008/49/EC.

## **7. The issue of the applicable law and the appropriate supervision**

The applicable data protection law depends on who the IMI actor or user is. For the European Commission, for example, the Data Protection Regulation 45/2001/EC applies. For a national user (e.g. a competent authority) the applicable law is its national data protection law which must be in conformity with Directive 95/46/EC.

The European Union has a solid data protection legal framework provided by this Directive and by Regulation 45/2001/EC<sup>15</sup>. The Data Protection Directive leaves some flexibility for Member States. IMI national coordinators are therefore advised to discuss these guidelines with their data protection authorities, for example as regards the details of information to be provided to individuals (see chapter 9 on this matter) or the duty to notify certain data processing operations to data protection authorities.

Directive 95/46/EC (Data Protection) is an Internal Market Directive which has a dual purpose. The harmonisation of national data protection legislation is intended both to ensure a high level of data protection and to safeguard the fundamental rights of individuals and thus to allow the free flow of personal data between Member States. Therefore, national specificities should not have any practical or significant impact on the use of IMI and the exchange of information required by other Community acts.

One of the most significant features of the EU data protection legal framework is its supervision by public independent data protection authorities. As a result, citizens may lodge complaints before these authorities to get their data protection problems dealt with promptly and outside the courts. The processing of personal data at national level is supervised by the national data protection authorities and the processing of personal data by the European Institutions is supervised by the European Data Protection Supervisor (EDPS). Consequently, the European Commission is subject to the supervision of the EDPS and other users of IMI, to the supervision of the national data protection authorities involved. For more details on how to deal with complaints or data subjects' requests, see chapter 10 on the rights of access and rectification and chapter 13 on the issue of cooperation with data protection authorities and the EDPS.

---

<sup>15</sup> Directive 95/46/EC applies to the Member States whilst Regulation 45/2001/EC applies to the European Institutions.

## 8. Data protection principles applicable to exchanges of information

The processing of personal data under EC Law may only take place under certain conditions (see chapter 6: "Legal grounds for the exchanges of personal information in IMI") and in accordance with some principles that the Data Protection Directive calls "principles relating to data quality" (see Article 6 thereof).

Data controllers should only collect personal data for legitimate and specific purposes and not process it for other purposes incompatible with those stated at the time of the collection. A classical example of incompatible purposes would be a competent authority selling on to private companies for marketing purposes the address data that it collected for purposes of handling the case of migrant professionals under the Services Directive.

Furthermore, processing of personal data needs to be proportionate (adequate, relevant and not excessive) to the purposes of the collection and the controller must also take reasonable steps to ensure that the data is kept up to date and that it is destroyed or rendered anonymous once the identification of the data subject is no longer necessary. Data quality principles are good information management principles because a good information system is not one that keeps gigabytes of data for no particular reason and that soon becomes out of date and unreliable. A good electronic information system should collect only the data that is necessary for the purposes set out in advance and these data should be kept up to date so that they can be relied on fully.

Applying these data quality principles to the functioning of IMI, leads to the following recommendations:

- (1) The use of IMI should be strictly limited to the purposes set out in the applicable legislation (e.g. in case of justified doubt or for any other reasons set out in the applicable legislation). Therefore, while it is expected that IMI will become the routine way to exchange information between competent authorities, it must be absolutely clear that IMI should not be used systematically to carry out background checks on migrant professionals or service providers.
- (2) The requesting competent authority should provide only the personal data that the responding competent authority needs to be able to unambiguously identify the person in question or to answer the questions. For example, if a migrant professional can be identified by his name and registration number in a professional registry, there should be no need to also provide his personal identification number.
- (3) IMI users should carefully select the questions and not ask more than is absolutely necessary. This is not only a matter of respecting data quality principles, but also a matter of reducing administrative burden. For transparency purposes, the pre-defined question sets are published on the IMI website<sup>16</sup>.

---

<sup>16</sup> [http://ec.europa.eu/internal\\_market/imi-net/docs/questions\\_and\\_data\\_fields\\_en.pdf](http://ec.europa.eu/internal_market/imi-net/docs/questions_and_data_fields_en.pdf)

What is sensitive data<sup>17</sup>?

It is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, offences, criminal convictions or security measures. Some Member States may also consider as sensitive data information concerning administrative sanctions or judgements.

(4) Competent authorities must be particularly vigilant when the exchanges of information concern *sensitive data*. Exchange of sensitive data is only possible in very limited circumstances. The most relevant requirements for the processing of sensitive data in IMI are the following:

(a) The processing of sensitive data is necessary for the establishment, exercise or defence of legal claims (see Article 8.2.e of the Data Protection Directive and corresponding provisions in national law).

This may apply to those data exchanges in IMI where a migrant professional or a service provider is claiming his right to exercise his profession or to be established in another Member State. Competent authorities, in each case, must carefully assess whether use of the sensitive data is indeed absolutely necessary to establish the right.

With regard to certain specific sensitive data exchanged within IMI, Member States adopted specific provisions in the Professional Qualifications Directive and the Services Directive:

4.a.1. Article 56.2 of the Professional Qualifications Directive states that "The competent authorities of the host and home Member States shall exchange information regarding disciplinary action or criminal sanctions taken or any other serious, specific circumstances which are likely to have consequences for the pursuit of activities under this Directive, respecting personal data protection legislation..."

4.a.2. Article 33 of the Services Directive foresees specific rules for the exchange of information regarding the good repute of the migrant service provider: "*Member States shall, at the request of a competent authority in another Member State, supply information, in conformity with their national law, on disciplinary or administrative actions or criminal sanctions and decisions concerning insolvency or bankruptcy...*"

(b) The data subject gives his explicit consent. If the administrative cooperation is in the data subject's interest, it may not be difficult to obtain the data subject's explicit consent for the processing of personal data.

(5) Precaution must be extreme as regards information on criminal records whose accuracy and up-to-date status are paramount. Therefore, besides compliance with other principles of the Data Protection Directive and Regulation referred to in this Recommendation<sup>18</sup> this category of information should only be requested when it is authorised under the relevant Community acts and is absolutely necessary to allow a

<sup>17</sup> For a legal definition see Article 8 of Directive 95/46/EC and Article 10 of Regulation 45/2001/EC.

<sup>18</sup> i.e. appropriate information should be provided to the data subjects, processing should be proportionate, and data should not be further processed for purposes incompatible with its collection.

decision in the particular case which is directly linked to the request. In other words, the processing must be directly related to the exercise of the professional activity or the provision of a service and necessary for the purpose of verifying compliance with the provisions of the relevant Directive. IMI users should always bear in mind that in many cases, the information necessary to take a decision does not need to refer specifically to the criminal record of the migrant professional or service provider.

In fact, there are only a few questions in the IMI question set that concern criminal records or other sensitive data<sup>19</sup>. Beyond these limited cases, the exchange of sensitive data should only occur in those exceptional cases where the concrete circumstances of the case are such that the sensitive data are directly related to the pursuit of the activity in question and are absolutely necessary for the establishment of the legal claims.

Competent authorities must not use IMI for routine checks of the criminal history of migrant professionals as this would not be compliant with the purpose for which IMI has been established. Any enquires about offences or disciplinary measures must also relate to the profession or the service concerned and not to any other offences or disciplinary measures that the migrant professional may have committed in the country of origin. For example, in order to determine if a doctor is legally registered and in good standing with the order of doctors, the requesting competent authority does not need to know whether the doctor has a road traffic offence on his criminal record, because such an offence would not prevent him from working as a doctor in his home country.

#### The issue of further processing and storage outside IMI

The use of IMI will often be associated with providing input to another processing operation that takes place in the Member State (for example to deal with an application to perform a service or to license a given activity). It is therefore normal that competent authorities will further process the data obtained for these purposes. When data is obtained through IMI and is further processed beyond the system, national data protection legislation still applies. You would therefore need to make sure that:

- This further processing is not incompatible with the purposes of collection and exchange that took place in IMI.
- This further processing is necessary and proportionate (adequate, relevant and not excessive) with the original purposes of collection in IMI.
- Take reasonable steps to keep the data up to date and to delete once no longer required.
- When data are extracted from IMI for disclosure to a third party, the data subject needs to be informed of this circumstance to guarantee fair processing, unless it would be impossible or involve disproportionate effort or if disclosure is expressly laid down by law (see Article 11.2 of the Data Protection Directive 95/46/EC). Considering that the disclosure may be required by the laws of only one of the Member States involved, and therefore, may not be widely

---

<sup>19</sup> A specific list of these questions is available on the IMI website:  
[http://ec.europa.eu/internal\\_market/imi-net/docs/questions\\_and\\_data\\_fields\\_en.pdf](http://ec.europa.eu/internal_market/imi-net/docs/questions_and_data_fields_en.pdf)



known elsewhere, the Commission suggests that efforts be made to provide information even when the disclosure is expressly laid down by law.

## **9. The provision of information to data subjects**

One of the pillars of any data protection scheme is that data controllers provide information to data subjects about the processing operations that they intend to carry out on their personal data.

Article 10 of the Data Protection Directive provides that at the time of the collection at least information concerning the identity of the controller, the purposes of the processing, the recipients or categories of recipients of the data, whether the replies to the questions are obligatory and the possible consequences of failure to reply, as well as the right of access and rectification must be provided to the data subject.

Therefore, when collecting personal data from an individual, the competent authority must inform the data subject that the data may be introduced in IMI in order to correspond with other public administrations in other Member States for the purposes of his or her request and that, in case of need, he or she could request access to or rectification of the data being exchanged from any of the competent authorities involved in the request (for more details in this regard, see chapter 10 on rights of access and rectification).

It is for each competent authority to decide how to convey this information to data subjects. As most (if not all) competent authorities will carry out processing operations other than exchanges of information in IMI, the way they inform individuals may, if appropriate, be the same way chosen for conveying similar information for other processing operations under national law (e.g. with signs, in the correspondence with data subjects and/or on websites).

### **The provision of information in the Data Protection Directive**

Article 10 of the Data Protection Directive contains a list with a minimum set of information that needs to be provided to individuals, except when they already have it:

- a) Identity of the controller or controllers (competent authority collecting the data and similar authorities in other Member States)
- b) The purpose of the processing (corresponding with other authorities in connection with the request of the migrant professional or service provider)
- c) Any further information in so far as such information is necessary to guarantee fair processing or if the provision of further information is required by national law such as:
  - c.1) recipients or categories of recipients
  - c.2) the existence of the right of access to and the right to rectify the data concerning them, how these rights can be exercised in practice and any exceptions to these rights under national law
  - c.3) right of redress (e.g. access to Courts and right to claim damages)
  - c.4) storage and retention period

c.5) security measures

c.6) links to relevant documents and websites, including the Commission IMI website

The Data Protection Directive foresees two cases in which information must be provided to data subjects: when the data is collected directly from them and when the data has been obtained from someone else. In this latter case, however, Article 11 of the Directive contains a rule of reason by which the provision of such information would not be necessary if it would involve a disproportionate effort or if the recording or disclosure was expressly laid down by law (as is the case for exchanges of information in IMI) although the Directive goes on to say that in these cases, "Member States shall provide for appropriate safeguards".

Therefore, competent authorities may need to fine-tune the provision of information to data subjects on the basis of their respective national data protection laws, possibly in consultation with the national IMI coordinators and the national data protection authorities. It is recommended to follow a layered approach, with the provision of basic information upon collection (e.g. in application forms to competent authorities) along with indication as to where data subjects may get more comprehensive information if they are interested.

For this second, more detailed layer of information, one efficient way to provide information to data subjects is by means of privacy policies or privacy statements on websites.

If competent authorities already have these privacy statements, they should update or complement them to refer specifically to exchanges of personal data in IMI. If that is not the case, competent authorities should decide whether the use of IMI and the amount of collection of personal data justifies the drafting of an on-line privacy statement.

In those cases where the use of IMI is very sporadic, it may suffice to inform individuals about IMI only briefly upon collection and also later when the need arises. In these cases, where no specific privacy statement about IMI is provided to the data subject by the competent authority, the competent authority should clearly indicate where data subjects may get more comprehensive information, for example, on the website of the national IMI coordinator and on the Commission's IMI website.

The data protection section of the Commission IMI website<sup>20</sup> contains the Commission's IMI privacy statement. It also contains additional information for data subjects on how to exercise their rights and to get assistance from national competent authorities or data protection authorities if necessary:

*"If you think that your personal data is in IMI and you would like to have access to it or have it deleted or rectified, you may do so by contacting the administration or the professional body with which you had contacts or any other IMI user that was involved in the request. If you were not satisfied with the answer received, you may either contact another IMI user involved or lodge a complaint with the data protection authority of one of the IMI users involved in the request which will assist you at no charge. A list of data protection authorities is available at the following address:*

---

<sup>20</sup> The data protection section of the IMI website contains all the IMI specific data protection documents as well as a link to a list of all legislative documents on data protection at EU level:

[http://ec.europa.eu/internal\\_market/imi-net/data\\_protection\\_en.html](http://ec.europa.eu/internal_market/imi-net/data_protection_en.html)

[http://ec.europa.eu/justice\\_home/fsj/privacy/nationalcomm/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm)

*Please be aware that in some cases, national law may contain exceptions to your right to have access to your personal data."*

It is strongly recommended that important actors in IMI dealing with a high volume of requests should publish their privacy policies on their websites. These privacy policies should contain a link to the data protection site of the Commission IMI website. Other competent authorities dealing with a low volume of requests may primarily rely on a link to the Commission IMI website.

National IMI Coordinators should provide assistance to competent authorities. This may include assistance in drafting sample privacy notices that may be used as a template by the national competent authorities. Alternatively, a common, national privacy notice could be drafted and published on the internet by the national coordinator, and each competent authority could simply provide the link to this notice when dealing with data subjects (e.g. in application forms or any other documents provided to the data subjects).

## **European Commission Privacy Statement Internal Market Information System - IMI**

### **1. Aim and actors of IMI**

The objective of IMI is to facilitate administrative cooperation and mutual assistance between Member States in order to ensure the proper functioning of the Internal Market and the free movement of persons and services. It does so by providing a tool for the exchange of information (including certain personal data) between national administrations of the EEA Member States.

This privacy statement covers the part of IMI for which the Commission is responsible, i.e. the collection, registration, storage and deletion of personal data of the first users in National IMI Coordinators and the storage and deletion, but not the collection, retrieval or viewing, of personal data of other IMI users and of persons who are the subject of an information exchange. Thus it does not concern those data processing acts which fall under the responsibility of Member States.

### **2. What is the applicable law?**

All processing acts within the responsibility of the European Commission are governed by Regulation 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.

The Decision of the European Commission of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data also applies.

### **3. Which data are processed by the Commission in IMI?**

The Commission collects the necessary contact details of the first users in the National IMI Coordinators such as name, professional telephone, fax numbers and e-mail addresses. These personal data as well as those of users in Delegated IMI Coordinators and in Competent Authorities are stored on a Commission server.

The personal data of persons who are the subject of an information exchange will for technical reasons be stored on a Commission server.

### **4. What is the purpose of processing data in IMI?**

The contact details of the National IMI Coordinators are essential in order to set up and run IMI. The Commission needs to have access to these data in order to cooperate effectively with the Member States on the management of IMI.

With regard to the temporary storage of personal data of persons who are the subject of an information exchange between national authorities, the purpose of data processing in IMI is to improve and facilitate cooperation amongst Member State competent authorities on the basis of Community legislation adopted to achieve the Internal Market in cases when there is a need for additional information from another Member State in relation to temporary cross-border provision of services or establishment of a service provider in another Member State.

### **5. Who has access to the data?**

Within the limits of Article 12 paragraph 7 of the European Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data the local data administrators of the Commission have access to the personal data of the local data administrators of the National IMI Coordinators. In no case are Commission staff able to access personal data of the person who is the subject of an information exchange.

## **6. How long will your data be stored?**

Personal data of users in Competent Authorities and Coordinators will be stored as long as they are IMI users.

All personal data exchanged between Competent Authorities and processed in IMI will be deleted automatically by the Commission 6 months after the formal closure of an information exchange. For statistical reasons the information exchange will continue to be kept in IMI, but all personal data will be rendered anonymous. A Competent Authority involved in a specific information exchange may at any time after the closure of that information exchange instruct the Commission to delete specific personal data. The Commission will honour any such request within 10 working days subject to the agreement of the other Competent Authority involved.

## **7. Which security measures are in place against unauthorised access?**

IMI is protected by a number of technical measures. Different levels of access to the database are secured by a normal password system and an additional digital code similar to that used in some personal computer banking systems. Access to the personal data in IMI is only allowed to a restricted group as described above under point 5 "Who has access to the data?" The system is also protected by https, a special, secure internet protocol.

## **8. Access to your personal data**

Access to your personal data as National IMI Coordinator is possible via the contact address below in point 10.

## **9. Additional information**

In addition to these Privacy Statements the "important legal notice" ([http://europa.eu/geninfo/legal\\_notices\\_en.htm](http://europa.eu/geninfo/legal_notices_en.htm)) applies.

## **10. Contact**

IMI is managed by the European Commission's Directorate General for Internal Market and Services, unit E.3. The responsible person (controller) is Mr Nicholas Leapman, Head of Unit. The contact address for IMI is:

European Commission  
Internal Market and Services Directorate General  
Unit E.3  
B-1049 Brussels  
Belgium  
[markt-imidataprotection@ec.europa.eu](mailto:markt-imidataprotection@ec.europa.eu)

If you want to file a complaint against any data processing act executed under the Commission's responsibility you may contact the European Data Protection Supervisor:

European Data Protection Supervisor (EDPS)  
60Rue Wiertz (MO 63)  
B-1047 Brussels  
Belgium  
phone: +32 2 283 19 00  
fax: +32 2 283 19 50  
[edps@edps.europa.eu](mailto:edps@edps.europa.eu)

## 10. Right of access and rectification

Transparency with the data subject is paramount. This is achieved both by first providing him or her with the information discussed in the previous chapter and second by granting him or her the right to access his or her personal data and, where appropriate, the right to have it deleted or rectified or blocked if they are inaccurate or have been unlawfully processed.

The complexity of the IMI system with many actors and users involved in joint-processing and joint-controller operations require a straight-forward approach towards the data subject. Data subjects are not familiar with the technicalities of joint processing operations or the functioning of IMI and they do not need to be.

A clear and simple approach therefore needs to be in place: as a general rule subject only to justified exceptions agreed between the data subject and all other parties concerned, data subjects will be able to exercise their rights of access, rectification and deletion by addressing any competent authority involved in a request. No competent authority should refuse access, rectification or deletion on the ground that it did not introduce the data in the system or that the data subject should contact another competent authority. The competent authority receiving the request will examine it and grant or refuse it in accordance with the merits of the request and the provisions of its own national data protection law. If necessary and appropriate, the competent authority may contact other competent authorities before taking a decision. In case of disagreement between competent authorities, they should involve their respective data protection authorities to reach an agreement in a timely and efficient way.

If the data subject is not happy with the decision taken, it may contact another competent authority involved in the information exchange or contact the national data protection authority of one of these competent authorities that suits him or her best: for example, the authority of the country where he or she is established, or his or her own national data protection authority, or the authority of the country where he or she is working. If necessary and appropriate, data protection authorities should cooperate with each other to deal with the complaint (see Article 28 of the Data Protection Directive).

It must be highlighted that data subjects always have the right to commence at any moment legal proceedings and to obtain redress where appropriate (see Articles 22 and 23 of the Data Protection Directive and corresponding provisions in national laws).

Article 12 c of the Data Protection Directive provides that the controller will notify any rectification, erasure or blocking to third parties to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort. This also applies to information further processed outside IMI.

Further to the recommendations of the Article 29 Working Party and the EDPS, the Commission is currently working on a feature within the IMI system (along the lines of the procedure already in place for early deletion of data at the request of competent authorities, see chapter 12) that would allow online data rectifications and with automatic notifications to those competent authorities involved. This has some technical complexity, so it is proposed that until the functionality can be implemented, if there was a need to rectify personal data, the competent authority should address such request for rectification directly to the IMI data controller at the European Commission (see the previous section "European Commission Privacy Statement").

The Data Protection Directive and the national laws implementing it also give data subjects the right to object to the processing of data relating to them and to have processing stopped when there is a justified objection. If you are contacted by a data subject who objects to the processing of data relating to him or her, please contact your national data protection authority to get more information about how this right to object works in your Member State.

## **11. Data security**

A number of organisational and technical measures, similar to those used in some personal computer banking systems, are used to ensure the security of IMI. Communication with IMI across the Internet is protected by https, a special, secure, Internet protocol. The technical measures to protect IMI have to be interoperable across the European Union. The technical protection of the system will be further developed with regard to the state of the art and the cost of implementation (see Article 17 of Directive 95/46/EC and Article 22 of Regulation 45/2001)

To obtain more information about the rules concerning the security of information systems used by the European Commission, please consult Commission Decision C (2006) 3602 available on the data protection section of the IMI website:

[http://ec.europa.eu/internal\\_market/imi-net/data\\_protection\\_en.html](http://ec.europa.eu/internal_market/imi-net/data_protection_en.html)

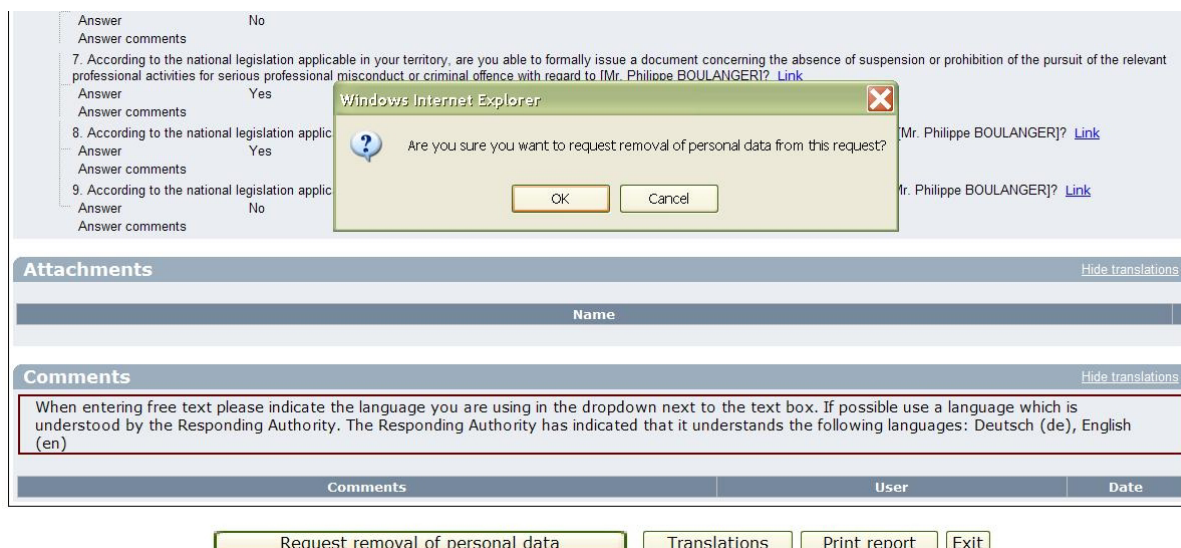
## **12. Retention period**

The rules as regards the retention period are laid down in Articles 4 and 5 of Decision 2008/49/EC.

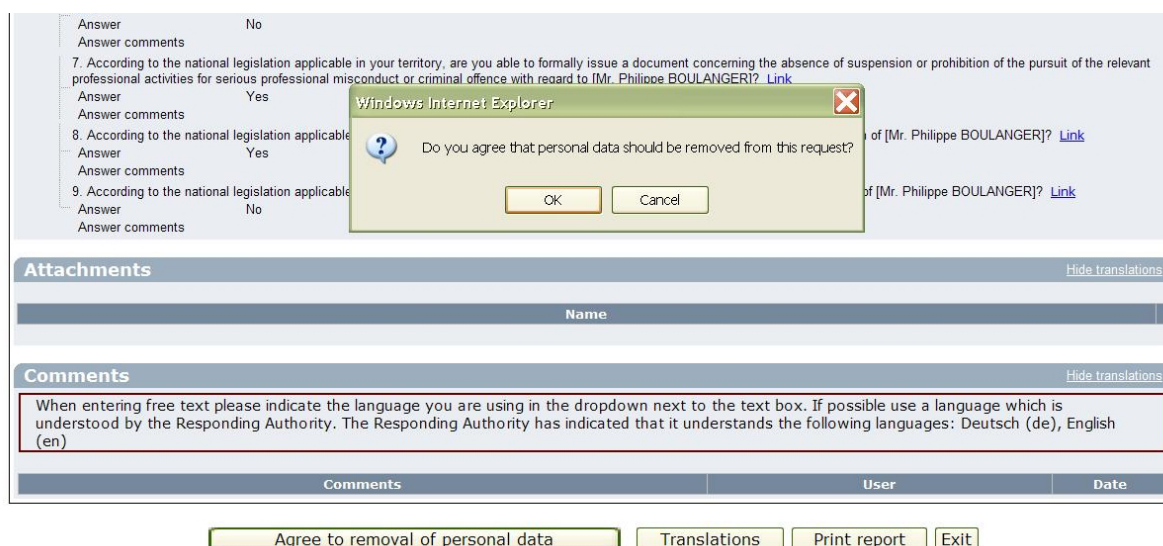
As a general rule, all personal data contained in information exchanges will be automatically erased six months after the formal closure of an information exchange. The Commission is currently implementing some modifications in the system (reminders and urgency lists) aimed at achieving the formal closure of requests as soon as possible.

There is also the possibility that a competent authority requests the deletion of personal data before the end of the six month period. Provided that the other competent authority agrees, the Commission shall act upon such requests within ten working days.

Competent authorities should be aware that requests for deletion of personal data can be made online simply by accessing the appropriate closed request and clicking on the "Request removal of personal data" button.



*Screenshot of a competent authority requesting an early removal of personal data*



*Screenshot of a competent authority being consulted on early removal of personal data*

The Commission will also implement some improvements to the system, such as automatic reminders to accept replies or to formally close requests in cases where there has been a satisfactory answer.

It is also important to recall that the national data protection rules apply to the storage of any personal data outside IMI by competent authorities.

### 13. Cooperation with national data protection authorities and the EDPS

The network of national data protection authorities and the EDPS is one of the most robust guarantees of the good functioning of our data protection system. Competent authorities can rely on them to seek advice any time they are confronted with a difficult issue that is not covered by these guidelines. National IMI coordinators are called upon to play a significant role in this respect. A list of contacts in the data protection authorities is available on the data protection section of the IMI website.



Competent authorities must also be aware that it might be necessary for them to notify their respective national data protection authorities before participating in IMI. In some Member States a prior authorisation might be necessary. IMI coordinators should play an active coordinating role in contacting data protection authorities, when necessary.

### **Work in progress**

The following data protection-friendly improvements will be included in a future version of IMI during 2009:

- a) Where the exchanges of information concern sensitive data (e.g. health data or criminal records or disciplinary measures), there will be a reminder that the information exchanged is sensitive and that the case handler should only request this information if absolutely necessary and directly related to the exercise of the professional activity or the performance of a given service.
- b) An online procedure will be set up (along the lines of the one already in place for early deletion of data at the request of the competent authorities) for the rectification erasure or blocking of data which have been unlawfully processed or are inaccurate.
- c) There will be automated reminders and urgency lists to accept a response so that requests do not remain open longer than necessary.
- d) Appropriate measures to deal with new flows of information under the Services Directive - that is the alert mechanism and the case by case derogations. As a general rule, these measures will follow the same approach designed for general exchanges of information, for example: reminders about the sensitive nature of these information flows, reminders to close alerts as soon as feasible and possible ways of informing individuals about the exchange of information and their rights to have access to the data and, if appropriate, to have it blocked, deleted or rectified. It is possible that additional data protection safeguards may be necessary. These will be drawn up in consultation with the EDPS.

### **14. Review clause**

IMI is a pioneer information system and is still being developed. The Commission is continuously gathering input from coordinators and competent authorities to improve the system and it is therefore likely that changes will be implemented in the coming months. Some of them may have no data protection consequences - others may do so.

These guidelines, therefore, are not set in stone and will need to be updated on the basis of the experience with the daily work of IMI. Not later than one year after the adoption of this Recommendation, the Commission will draw up a report in which it will assess the situation, including the possibility of adopting another legal measure.