Data protection guidelines for IMI users

The new IMI Regulation[1] codifies existing practices regarding the processing of personal data in IMI and its entry into force does not fundamentally change the applicable rules of data protection and security. Nevertheless, some adjustments may be necessary. This note should help IMI users ensure they comply with the new legal framework for IMI.

Basic information about the processing of personal data in IMI (including the legal basis for data processing, system functionalities, workflows and question sets, as well as information on national exceptions or limitations of data subjects' rights) is available at the IMI website: http://ec.europa.eu/internal_market/imi-net/data_protection/index_en.htm

Contact to the Commission IMI Helpdesk: IMI-HELPDESK@ec.europa.eu

1. What is IMI used for? *[Articles 3, 4 and 13]*

IMI may only be used for administrative cooperation in areas listed in the Annex to the IMI Regulation, i.e.: Services Directive[2], Professional Qualifications Directive[3], Patients' Rights Directive[4], Regulation on cross-border transit of euro cash[5], and SOLVIT[6], as well as in the context of the Posting of Workers Directive[7] (on the basis of a pilot project[8]). This list will be amended from time to time (you will find updated information here).

2. Why should I use IMI instead of e-mail or telephone?

Following the privacy-by-design principle, IMI has been developed with the requirements of data protection legislation in mind, in particular by means of restrictions imposed on access to personal data exchanged through the application. Therefore, IMI offers a higher level of data protection and security assurance than other methods of information exchange such as regular mail, telephone, fax or unencrypted e-mail.

Moreover, exchanging information via IMI also provides you with proof of such exchanges on which you may have based your decisions. You can extract a report with a digital signature from IMI about every exchange in which you are involved. This is important in case decisions are contested.

---

[1] Regulation (EU) No 1024/2012 of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation'), OJ L 316, 14.11.2012, p. 1.

[2] 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.

[3] 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, as amended.

[4] Directive 2011/24/EU 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, 4.4.2011, p. 45.

[5] Regulation (EU) No 1214/2011 of the European Parliament and of the Council of 16 November 2011 on the professional cross-border transport of euro cash by road between euro-area Member States, OJ L 31, 29.11.2011, p. 1.

[6] Commission Recommendation of 7 December 2001 on principles for using 'SOLVIT' – the Internal Market Problem Solving Network, OJ L 331, 15.12.2001, p. 79.

[7] Directive 96/71/EC of the European Parliament and of the Council of 16 December 1996 concerning the posting of workers in the framework of the provision of services, OJ L 18, 21.1.97, p. 1.

[8] Further pilot projects are currently under consideration in the areas of electronic commerce and EU certification of train drivers.

3. Can I exchange sensitive information via IMI? *[Article 16]*

Legislation listed under point 1 above often requires competent authorities to exchange information on disciplinary, administrative or criminal sanctions or other information necessary to establish the good repute of an individual or a legal entity. In line with data protection principles, this category of information should only be requested when (i) it is authorised under the relevant legislation and (ii) it is necessary to allow a decision in the case. In practice, it should in many instances be possible to make an informed decision and answer the question(s) asked through IMI without referring specifically to the criminal record of an individual. However, where in a particular case there is genuine need to exchange information of this kind, IMI may and should be used for this purpose in accordance with the IMI Regulation.

4. Do I need the prior consent of the data subjects before responding to questions about them in IMI?

No, with the exception of SOLVIT. Where personal data of citizens are processed in IMI on the basis of specific provisions of EU directives or regulations listed in the Annex to the IMI Regulation (see also point 1 above), it is not necessary to ask for the data subject's consent in order to justify the processing. This is in line with the applicable EU rules on data protection[9].

In the case of SOLVIT, data subjects' consent is obtained through the on-line complaint form[10].

5. Which information should I provide to the data subjects? *[Article 18]*

As with security, all IMI actors (i.e. the competent authorities, the IMI coordinators and the Commission) are jointly responsible for ensuring adequate transparency towards data subjects.

On your side, when you collect personal data directly from an individual (e.g. via an application form), you should provide him/her with *at least* the following information:

- the fact that their personal data may be processed in IMI;
- the identity and contact details of the controller (i.e. those of your competent authority);
- the (categories of) recipients to whom the data may be disclosed (i.e. relevant competent authorities of other Member States);
- the right to access their personal data and to have it corrected.

It is for each competent authority to decide how to convey this information (e.g. in the correspondence with data subjects or through privacy statements on websites, etc.). For more details on this, look at national rules and guidelines in place. In case of doubt,

[9] See Article 7 of the data protection Directive 95/46/EC.

[10] See SOLVIT Privacy Statement.

competent authorities should seek advice from their national IMI coordinators (see also point 7 below).

National law may lay down specific exceptions or limitations regarding the obligation of transparency (e.g. exempting certain types of public authorities or procedures from the requirement to provide information). The Commission will liaise with national IMI coordinators in order to identify the relevant national rules and will make them publicly available[11].

Please refer to http://ec.europa.eu/internal_market/imi-net/data_protection/index_en.htm for up-to-date information and consider including this link in the information materials for data subjects.

6. Does information concerning legal persons also require protection? *[Article 10]*

Not all information exchanged through IMI is personal data, for example when it concerns legal entities[12] or where the question and answer do not relate to any given individual[13]. Such information should be treated in accordance with the applicable national rules of professional secrecy or confidentiality. It is also possible to specifically request confidential handling of non-personal data in the system. Such requests should be respected by IMI users.

7. What should I do if a data subject requests access to information about him/her exchanged in IMI? *[Article 19]*

In addition to the right to be informed, data subjects have the right to access his/her personal data. As a general rule, data subjects should be able to request access from any of the competent authorities involved in the administrative cooperation procedure concerning him/her. A request for access to data should in principle always be granted. You can print a report from the IMI database for this purpose if the case is still open or if it was closed less than 6 months ago. For requests concerning older cases, you will need to contact the Commission IMI Helpdesk. They can still retrieve data up to three years after closure of the exchange of information. After that period, all personal data will be erased.

8. What if a data subject wants to have their data corrected or deleted? *[Articles 19 and 20]*

A request for rectification or deletion of data should be examined on the basis of its merits and the provisions of your national data protection law. If necessary, before taking a decision you may contact the data protection officer of your authority, or other competent authorities.

Once the decision to grant a request has been made, the necessary action (correction or deletion, as appropriate) in IMI will be performed by the relevant IMI actor, depending on the circumstances of the case:

---

[11] E.g. through publication on the IMI website: http://ec.europa.eu/internal_market/imi-net/data_protection_en.html.

[12] Although in some Member States the scope of data protection legislation also covers legal persons to a certain extent.

[13] E.g. a general question as to whether a profession is regulated in a given Member State.

(a) if the request for rectification or deletion concerns an administrative cooperation procedure which is still *open* (i.e. ongoing) and it was addressed to the competent authority which initiated the procedure in IMI, that competent authority can and should perform the necessary action(s) in the system.

(b) if the request for rectification or deletion was received and granted by a competent authority which was involved in a workflow *but did not initiate the information exchange*, that competent authority will not be able to perform any actions on the personal data in IMI itself for security reasons. It should therefore contact the Commission IMI Helpdesk which will work together with the other competent authority to make sure that the necessary is done.

(c) for technical reasons, the rectification or deletion of personal data contained in information exchanges which have been *closed* in IMI can only be performed by the Commission. The competent authority that granted such a request should therefore contact the Commission IMI Helpdesk without delay to agree on the appropriate course of action.

In accordance with the IMI Regulation, the correction or deletion of data must be done *as soon as possible* and not later than 30 days after the request was received by the responsible competent authority. This time limit would normally prevail over generally applicable time limits set in national law (if any). Please keep in mind that in cases (b) and (c) above sufficient time must be granted for the necessary technical intervention of the Commission. You should therefore inform the Commission IMI Helpdesk about such requests without delay.

In cases where a request for rectification or deletion concerns personal data which have already been *blocked* in IMI (6 months after formal closure of a case), the competent authority should contact the Commission IMI Helpdesk to verify whether the request meets the requirements set out in the IMI Regulation and to agree on the appropriate course of action. As a rule, blocked data will not be deleted or corrected, but the fact that their accuracy or lawfulness is contested by the data subject will be recorded, along with the corrected information. For technical reasons, such recording will need to be done by the Commission.

Where national law provides for exceptions or limitations on the data subjects' rights, such exceptions or limitations continue to be fully applicable in the context of IMI and the Commission should be informed and will make them public to ensure transparency.

9. How long will personal data be stored in IMI? *[Article 14]*

As a general rule, personal data processed in IMI is blocked six months[14] after the administrative cooperation procedure[15] was formally closed in the system. Blocked data is

[14] For SOLVIT, this period is set at 18 months. In the case of the Services Directive, the rules for handling alerts remain unchanged, i.e. information, including personal data, contained in an alert which has been closed becomes invisible to IMI users.

[15] The IMI Regulation uses the term "administrative cooperation procedure" to describe the workflows in IMI.

inaccessible to IMI users via the normal IMI interface[16]. All personal data is automatically deleted in IMI 3 years after the formal closure of the administrative cooperation procedure.

IMI uses a number of technical features (e.g. reminders) which encourage you as a user to formally close the procedure in the system as soon as possible.

In addition, it is possible to delete personal data in IMI before the expiry of the retention period, on a case-by-case basis, at the express request of a competent authority and provided that the individual concerned has given his/her consent. It is important to remember that IMI only provides for a possibility of early deletion. Before you decide to request early deletion (e.g. in response to a demand from the individual concerned), please make sure that there are sufficient legal grounds for such a request on the basis of the applicable national law, including data protection legislation, and/or the applicable rules on administrative procedure.

10. How about personal data of IMI users? *[Article 15]*

Your personal data (i.e. contact details of IMI users) are kept in the system as long as you are a user of IMI. They may be processed for such purposes as monitoring the use of the system by IMI coordinators and the Commission, communication, training and awareness raising initiatives, and gathering information on administrative cooperation or mutual assistance in the internal market, e.g. through user surveys. Once using IMI ceases to be part of your responsibilities, your personal data will be blocked, but will remain in the system for three years before they are finally deleted[17]. It is therefore very important to keep user lists up to date. For this purpose, users or their supervisors should communicate the changes to the relevant IMI coordinator.

11. Who is responsible for the security of IMI? *[Article 17]*

All IMI actors (i.e., the Commission, the IMI coordinators and the competent authorities) share responsibility for ensuring security of IMI and its operations.

The Commission ensures that IMI complies with the requirements applicable to all IT systems at EU level set out in Commission Decision C(2006)3602 on Security of Information Systems and its implementing rules. This means that an analysis of the risks was performed and appropriate technical and organisational security measures were defined and integrated in the IMI system. For example, authentication (a PIN/password combination) and access control mechanisms ensure confidentiality and integrity of the IMI system and the information it contains. Personal data is transmitted encrypted through use of the https protocol and, thanks to logical data partitioning, a user has access only to the specific data they need.

In addition, each competent authority is a data controller and is therefore responsible for ensuring the security of personal data it handles. Consequently, each IMI user must

[16] In exceptional circumstances, the Commission will be able to retrieve the blocked data on specific request from a competent authority and with consent of the individual concerned, for purposes of proof of an information exchange or for overriding reasons in the public interest.

[17] The blocked data can only be retrieved in exceptional cases for purposes of proof of and information exchange in IMI.

implement organizational security measures applicable to the processing of personal data in accordance with national legislation. In general, security measures for IMI users will not be different from those measures your authority applies to other IT tools used for personal data processing[18]. Basic precautions which you should always take include: keeping your password and security code safe, and (for those involved in user management) making sure that IMI user lists are kept up to date, and that access rights of those who moved on to another job or whose responsibilities no longer involve using IMI are promptly revoked.

It is also important to apply appropriate security measures to personal data which you extract from and further process outside IMI (e.g. in a printed report or otherwise archived outside IMI). They will typically not be different from those applicable to other data processing operations of your authority. In case of doubt, you should check what these rules are with the data protection officer of your authority or with your IMI coordinator.

12. Where should I go with questions about data protection & IMI?

In case of doubts concerning the rules on the protection of personal data in IMI and/or their application in practice, the national IMI coordinator (NIMIC) is your main contact point for IMI users. The NIMIC will provide you with relevant information and will also act as the main interlocutor of the Commission in respect of data protection and security.

[18] Please note that specific security measure may apply to the processing of sensitive data in your organisation.