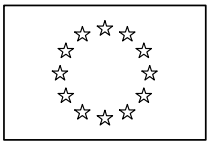


EUROPEAN COMMISSION

Brussels, 22.4.2010
COM(2010)170 final

COMMISSION REPORT

on the state of data protection in the Internal Market Information System

COMMISSION REPORT

on the state of data protection in the Internal Market Information System

1. EXECUTIVE SUMMARY

The Commission is satisfied with the way personal rights and freedoms with regard to personal data (hereafter "data protection") are ensured in the Internal Market Information (IMI) System. IMI is an internet-based, secure and multilingual information exchange system that assists Member States to carry out their duties of administrative cooperation. The Commission is also satisfied with the implementation of the Recommendation on data protection guidelines for IMI.

Member States have not reported any data protection problems. This justifies the step-by-step approach agreed with the European Data Protection Supervisor to building the legal framework for IMI in response to technical developments and the extension of the system to other areas of Internal Market legislation.

In 2010, the Commission will explore the possibility of extending IMI to other areas of the Internal Market and gain more experience with the practical use of the system in the area of services. In the first quarter of 2011, it will publish a staff working paper on the functioning and development of the IMI system in 2010, which will also cover data protection.

2. OBJECT OF THIS REPORT

This report, announced in the Commission Recommendation on data protection guidelines for the Internal Market Information System[1] ('the Recommendation'), reviews the Recommendation's implementation by the Member States and by the Commission and assesses the state of data protection in IMI. It also covers new issues which were not addressed in the Recommendation — in particular, coverage of the new Services Directive.

In drafting the report, the Commission took into account feedback provided by the Member States both via an *ad hoc* consultation launched in November 2009[2] and

---

1 C(2009) 2041final. OJ L 100, 18.4.2009, p. 12–28.

2 Seventeen Member States replied to the consultation, which asked the following questions:
- Have you contacted your national data protection authority? Have they expressed any views on the national implementation of the guidelines?
- Have you set up a general privacy policy statement for all IMI users or is this being arranged locally by your competent authorities (CAs)?
- Have your CAs experienced any problems in relation to data protection when sending or responding to requests in IMI?
- Have your CAs reported any issues in dealing with questions about criminal records?
- Have your CAs received any access, deletion or rectification requests from data subjects?
- Are your CAs aware of the possibility of early deletion of personal data in the system? Are they using

through regular contacts with IMI coordinators and Member States' representatives in IMAC-IMI (Internal Market — IMI Committee) meetings.

3. THE DEVELOPMENT OF IMI DURING 2009

The year 2009 was crucial for the development of IMI. The use of IMI for legislation concerning professional qualifications was extended to 20 new professions and most resources were devoted to extending IMI to cover the Services Directive[3].

National IMI coordinators participated in the pilot project to exchange information on the Services Directive (on the basis of real and fictional cases) and the training sessions that took place in Brussels[4]. The Commission released a new version of the software (1.7) to allow competent authorities to self-register. At the end of the year it also released an interim version 2.0 which included a separate IT application for the alert mechanism[5]. This new software release became fully operational during the first quarter of 2010.

Thanks to these joint efforts by the Commission and the Member States, by the end of January 2010, 4 508 competent authorities had been registered in IMI, of which 3 698 had access to the new Services area, although it is expected that this number will increase substantially over the next few months. The average number of different daily users logged on increased from 40 in January 2009 to 180 in December.

---

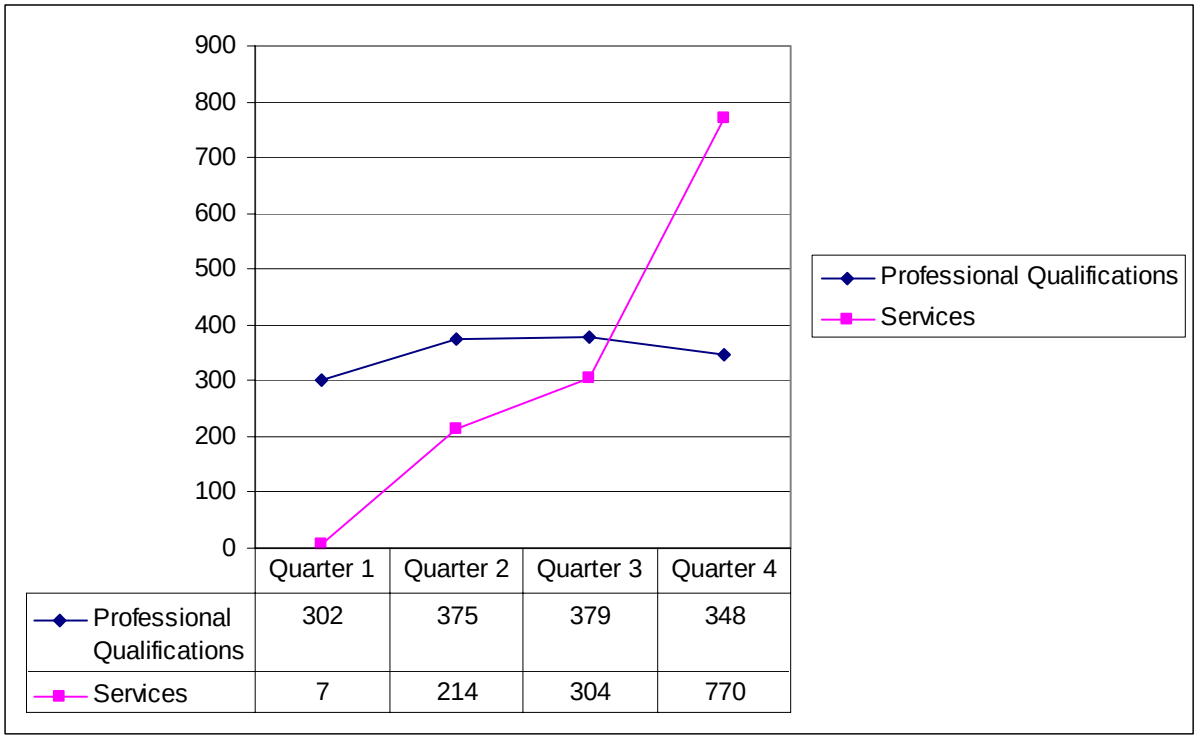
this possibility?
- Have you included data protection in your IMI training sessions?

[3] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the Internal Market, OJ 376, 27.12.2006, p. 36–68.

[4] In 2009, the Commission held three one-day training sessions for IMI coordinators in Brussels, catering for around 60 participants each. During the same period, Member States held more than 100 training events altogether for competent authorities at local, regional and national levels.

[5] See Article 32 of the Services Directive.

Total number of requests sent per quarter and by legislative area for 2009



	Quarter 1	Quarter 2	Quarter 3	Quarter 4
Professional Qualifications	302	375	379	348
Services	7	214	304	770

In the professional qualifications field, the system has gained maturity and its unequivocal success illustrates the potential of IMI as a tool for administrative cooperation in the EU. An average of 350 requests per quarter was sent. More than 90% of all requests concerning professional qualifications sent in 2009 came from the EU-15, the Member States who joined before 2004, which reflects the direction of labour migration. Poland and Romania were the recipients of 32% of all requests.

When looking at these numbers, it is important to note that 56% of the requests were answered within one week.

Time needed to deal with a request under the Professional Qualifications Directive in 2009

	Requests accepted	**Cumulative %**	**Requests answered**	**Cumulative %**
Within 3 days	**741**	**57.0%**	**518**	**43.0%**
Within 1 week	**216**	**73.7%**	**167**	**56.8%**
Within 2 weeks	**166**	**86.5%**	**170**	**71.0%**
Within 4 weeks	**120**	**95.7%**	**164**	**84.6%**
Within 8 weeks	**35**	**98.4%**	**106**	**93.4%**

More than 8 weeks	**21**	**100.0 %**	**80**	**100.0 %**
Total:	**1299**		**1205**	

(* The discrepancy between requests accepted and answered is due to requests that were withdrawn or still open at the end of December 2009)

4. IMPROVING DATA PROTECTION IN IMI, A STEP-BY-STEP APPROACH

IMI follows the so-called 'Privacy by design' approach whereby data protection compliance is designed into systems holding information right from the start. Data protection considerations are also part of the daily use of the system and are included in the training materials, an approach that goes beyond formalistic or theoretical protection. This seems to be paying off as no Member State reported a single data protection incident in IMI and no complaints were received from data subjects.

The Commission has been engaged in a dialogue with the data protection authorities and the European Data Protection Supervisor (EDPS) over the past two years. The main principle guiding the step-by-step approach is that, given that the system guarantees a high level of technical and procedural data protection and the Commission is clearly committed to continuing to improve it, the legal framework for IMI should follow technical development and the extension of the system to other areas of Internal Market legislation.

The step-by-step approach, on the basis of limited experience with the system, has allowed the Commission to address all the concerns expressed by the EDPS in an opinion of 12 December 2007 and to adopt three legal texts which deal with data protection issues for IMI:

a) 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[6]

b) The European Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI)[7]

c) The European Commission Decision of 2 October 2009 setting out the practical arrangements for the exchange of information by electronic means between Member States under Chapter VI of Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market[8].

Section 6 of this report will discuss any remaining issues as well as the content and timeliness of future measures, including the possible adoption of a legal instrument.

---

6 C(2007) 6306, OJ L 13, 16.1.2008, p. 13-23.
7 C(2009) 2041 final, OJ L 100, 18.4.2009, p. 12-28.
8 C(2009) 7493, OJ L 263, 7.10.2009, p. 32-34.

5. THE IMPLEMENTATION OF THE COMMISSION RECOMMENDATION

5.1. Improvements made by the Member States

5.1.1. Contacts with the data protection authorities

The Recommendation *'encouraged IMI coordinators to make contacts with their national data protection authorities for guidance and assistance on the best way to implement the guidelines under national law'*. In their reports to the Commission, most Member States stated that they had consulted their national data protection authorities. These consultations have reassured IMI users that personal data can be exchanged through IMI in compliance with data protection legislation and, at the same time, they have allowed national regulators to establish working relations with representatives of public administrations who value data protection highly and are committed to making this truly European project a success.

5.1.2. Privacy statements

Following a suggestion from the EDPS, the Recommendation also encouraged IMI coordinators to discuss the content of privacy statements with local data protection authorities. It was not possible for the Recommendation to be very specific on this issue because although the Data Protection Directive harmonised in full, Member States have a margin of discretion in the implementation of some provisions. Reports from the Member States confirm that there are different national practices on the content and format of privacy statements. A small majority of Member States have taken the view that the right format and content of the information to be provided to individuals should be decided locally by each competent authority in compliance with local laws. In some Member States, by contrast, adaptable models are proposed for the whole Member State[9].

5.1.3. Awareness and training

One of the most important achievements of the Recommendation is that it has increased data protection awareness among IMI actors and users who are now acquainted with general data protection principles and also given practical suggestions to guarantee a high level of data protection in IMI. Thanks to the Recommendation, references to the data protection guidelines have also been incorporated in the IMI training materials drafted for competent authorities.

5.2. Improvements made by the Commission

5.2.1. The IMI Security Plan

Data security and confidentiality are regulated by the Commission Decision of 16 August 2006 concerning the security of information systems used by the

---

[9] A good example of a national model drawn up with technical assistance from the national data protection authority is the privacy statement (*cláusula de privacidad*) made available by the Spanish IMI team: http://www.mpt.es/documentacion/sistema_IMI/documentos/protec_datos/ClausulaIMI_ES/documentos/Clausula_IMI.pdf.

European Commission[10]. This Decision has been updated with implementing rules adopted in 2009 and recent guidelines and standards which are broadly the same as international standards. The security measures in IMI have been revised and updated accordingly and a comprehensive Security Plan was drawn up in 2009 that will be reviewed in 2010.

5.2.2. Technical improvements

Where exchanges of information concern sensitive data, there is now a reminder on screen that the information 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. Data protection considerations have also been fully taken into account in the design and implementation of the new alert mechanism (see section 5.2.3.2 below).

The IMI website has also been improved to make it more intuitive for users to find the relevant documents. The section on data protection[11] has been updated with all legal texts relating to data protection, correspondence with the EDPS and questions sets used in the system. For transparency purposes, further to a suggestion from the European Supervisor, the questions concerning sensitive data have been identified.

5.2.3. The new legislative area of the Services Directive

5.2.3.1. The use of IMI for the Services Directive

The Services Directive did not specifically refer to IMI (but only more generally to an electronic system for the exchange of information). Therefore, it was necessary to formally determine that IMI would be used for that purpose. This was done by a Decision[12] adopted by the Commission according to the procedure provided for in the Services Directive ("the comitology decision").

This comitology Decision lays down practical arrangements for exchanging information in the Services field in IMI. It contributes to the system's high level of data protection and brings additional transparency and precision to the general rules resulting from Decision 2008/49/EC and the data protection guidelines contained in the Recommendation. It leaves any additional data protection safeguards to be decided later, if necessary, in the light of experience with the system[13].

5.2.3.2. A data-protection-friendly design for the alert mechanism

The alert mechanism is a warning mechanism set up under Articles 29(3) and 32 of the Services Directive which complements the RAPEX system for products. It helps to prevent the risk for recipients resulting from services.

---

10 C(2006)3602.

11 http://ec.europa.eu/internal_market/imi-net/data_protection_en.html

12 Commission Decision of 2 October 2009 setting out the practical arrangements for the exchange of information by electronic means between Member States under Chapter VI of Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

13 See Chapter 13 of the Recommendation, subsection 'Work in progress', point (d).

The alert mechanism allows Member States to comply with a legal obligation to exchange information and is thus fully lawful from the data protection perspective. However, the Commission is conscious of the data protection implications of such a system. It has therefore taken great care in its design, ensuring that it is data-protection-friendly, and it urges Member States, who are responsible for data protection when sending or receiving alerts, to be vigilant in applying the rules correctly.

The alert mechanism contains a good number of data protection safeguards which are general features of the IMI system, plus some specific safeguards aimed at making sure that:

a) **Access to the data is limited to specific competent authorities/users**

In line with the overall approach in IMI, access to information under the alert mechanism is strictly limited on a need-to-know basis. Competent authorities and IMI users have access to alerts only if they have been granted specific access by Member States not only to IMI in general but to the specific application for alerts. By default, competent authorities and IMI users cannot send or receive alerts. This function has to be activated separately.

b) **No unnecessary alerts are sent**

No alert can be sent without completing a check list to ensure the criteria are met; for instance, that there are serious specific acts or circumstances relating to a service activity that could cause serious damage. If the initiating authority does not check off all the relevant criteria, the system does not allow it to proceed with sending an alert.

Moreover, the alert is not directly sent to other Member States but is first submitted to an alert coordinator in the same Member State. This alert coordinator should, once again, take a view on whether or not the alert should be broadcast to other Member States.

c) **Alerts are not distributed to more recipients than necessary to comply with the information requirements set out in the legislation**

When alerts are sent to other Member States, the initiating authority and the alert coordinator need to assess which Member States need to receive the alert. If the Member State where a service is provided wants to send an alert, by default only the Member State of establishment of the service provider and the Commission will receive the alert. This default configuration makes sure that the addition of other Member States to the list of recipients is subject to a case-by-case decision on a need-to-know basis.

Moreover, when the alert is broadcast to other Member States, it is not sent to all competent authorities in the receiving Member States but only to an incoming alert post-box (usually the national alert coordinator). The recipient will take the decision on which competent authorities in its Member State are concerned and need to be involved.

d) **The Commission, while receiving alerts as provided for in the Services Directive, does not have access to personal data**

The Services Directive provides for all alerts to be sent to the Commission but, unlike the Member States, the Commission does not need access to personal data. The Commission thus receives alerts without personal data.

e) **Should unfounded alerts be sent, despite the precautions, these can quickly be withdrawn or incorrect data can be rectified or deleted**

The IMI system allows a competent authority that has sent an unfounded alert to withdraw it immediately, rendering it invisible to all IMI users. If the alert was justified but it is necessary to rectify some information, the initiating competent authority can do that at any time. In addition, the IMI system also allows other competent authorities who have received the alert to indicate that certain information provided in an alert is incorrect.

f) **Alerts are closed as soon as there is no longer a risk; the data immediately becomes invisible to all users, and the personal data is deleted six months after closure**

Once the risk that triggered the alert has disappeared, the alert needs to be closed. The IMI system thus allows the Member State of establishment to close the alert and the responsible authorities are sent reminders by email. Once an alert has been closed, it becomes invisible. Six months after closure, at the latest, all personal data is automatically deleted and removed from the system.

6. ISSUES FOR FURTHER CONSIDERATION

Although most Member States have expressed positive views of data protection in IMI, a few Member States have raised some issues which are reviewed in this section of the report.

6.1. Applicable rules on data security and confidentiality

Processing personal data in IMI involves joint processing (between the Commission and the Member States), joint controllership (between the different users and actors) and joint supervision (by the national data protection authorities and the EDPS). In such a complex scenario, it is not always easy to allocate responsibilities.

The Danish and German data protection authorities have taken the view that since the competent authorities located in their territories must comply with certain national requirements (e.g. a stronger authentication mechanism, as referred to in the following section), they should insist that IMI meet these national requirements or else stop using the system. The competent authorities forwarded these requests to the Commission, which is responsible for the security of the system.

The Commission believes that IMI is a secure system and that a truly European network like IMI simply could not work if every Member State insisted that their national security standards had to be complied with. The adoption of the Data Protection Directive almost twenty years ago had the twofold purpose of protecting the fundamental right to data protection, on the one hand, and guaranteeing the free

flow of personal data between Member States and between the Member States and the EU institutions[14] on the other hand.

On this basis, the Commission insists that in view of the high level of guarantees with regard to data protection in the IMI system and the principle of sincere cooperation of Article 4.3 of the Treaty on the European Union, national data protection authorities should not create obstacles to using the system for national competent authorities.

6.2. Towards stronger authentication in IMI

The IMI authentication system is an advanced version of single factor authentication as it combines a user name and password with a PIN. When attempting to access the system, the user is asked to provide a randomly-chosen combination of characters from the PIN code.

German and Danish data protection authorities have expressed some concerns about the IMI authentication system. The Commission believes that the current authentication mechanism is appropriate, bearing in mind the state of the art and the implementation cost, but agrees that stronger authentication is desirable in the long term. As Member States have introduced different authentication systems that are not always interoperable, the preferred solution for stronger authentication in IMI seems to be e-identities managed at Member State level that would become interoperable by means of 'middleware'.

One of the options is the STORK project, which is currently being developed by a consortium in which some Member States participate and it is financed under the Competitiveness and Innovation - ICT Policy Support Programme. The Commission will closely monitor its progress over the following months, which are critical to determining whether to use it in IMI.

Further references to data security are made in section 7.2.

6.3. Data retention

The data retention policy in IMI is very strict[15] and some actors and users have indicated that it should be reviewed. Quick deletion of personal data in the system is not always in the interest of the data subject, who might prefer storage of his or her data in IMI for a longer period, for example in connection with legal proceedings.

In a recent ruling[16], the European Court of Justice stated that the right of access to information[17] applies not only to present data but also to data held in the past.

---

14 This principle is clearly set out in Article 1.2 of the Data Protection Directive, and Article 1.1. and Recital 13 of the Data Protection Regulation: 'The aim is to ensure both effective compliance with the rules governing the protection of individuals' fundamental rights and freedoms and the free flow of personal data between Member States and the Community institutions and bodies or between the Community institutions and bodies for purposes connected with the exercise of their respective competences'.

15 Early deletion of personal data is possible just with a couple of clicks and in any case all personal data are automatically deleted six months after the closure of the information requests.

16 C-553/07, Rotterdam v Rijkeboer.

Therefore, the Court considers that limiting access by deleting the data may be against the law unless it can be demonstrated that longer storage of the information would constitute an excessive burden on the controller. The Commission does not consider that storing personal information in IMI for a longer period would be an excessive burden and therefore it intends to reflect on a longer storage period, which might also include a transitional phase of blockage of the data, rendering the data invisible for all users before it is ultimately deleted. The possible implications of a blocking policy, including who could have accessed to the blocked data and for what purposes, will be carefully analysed.

This is a good example of the need to reflect very carefully before deciding on a set of rules governing the functioning of IMI in a legally binding instrument. It is essential that the Commission and the Member States, while guaranteeing good data protection and the involvement of the data protection authorities in the process, can benefit from sufficient experience with the system to avoid laying down ineffective or even counter-productive rules on data protection.

6.4. National use of IMI

The transposition of the Services Directive in the Netherlands provides for IMI to be used for national purposes, that is, to exchange information between Dutch administrations as well. The European Commission commends this approach, which illustrates the potential of IMI for use across administrations. However, national use of IMI by the Member States is subject to three conditions:

a) that the processing of personal data and the storage of information on Commission servers are considered lawful under national law,

b) that the system is used as it is, with the same question sets and functionalities, and

c) that the Member State takes full responsibility for any issues (data protection or other issues) in connection with the use of the system for national purposes.

Therefore, should Member States be interested in national use of IMI, it is recommended that they consult with their national data protection authorities first and then contact the Commission to discuss this issue and make sure that it does not create any problems from the perspective of data protection laws.

6.5. Specific data protection safeguards in legally binding Community legislation

In its opinion of 12 December 2007 and in the exchange of letters with the Commission, the EDPS has called for specific, legally binding data protection safeguards to be laid down in EU legislation as IMI broadens its scope beyond the Services and Professional Qualifications Directives. German data protection authorities have expressed similar views.

In 2010, the new Commission will take a fresh look at the functioning of the Single Market and the possibility of enhancing IMI's contribution to improving Member

---

[17] See Article 12 a) of Directive 95/46/EC.

States' implementation of Internal Market legislation. It will thus consider which other policy areas could benefit from the use of IMI.

There is a solid package of data protection measures already in place and the feedback received from the Member States has been positive. Therefore, the Commission believes that it would be unwise to proceed with a legislative proposal before defining the scope of IMI and before benefiting from the experience with the practical use of the system for services. Any future proposal needs to fit well with these developments in order to ensure a solid, future-proof basis for IMI and data protection.

In the meantime, the Commission will continue to improve data protection in IMI in close cooperation with the Member States and the EDPS as set out below.

7. FUTURE IMPROVEMENTS

7.1. Technical improvements

Automatic reminders and urgency lists to accept a response (so that requests remain open no longer than necessary) will be included in a future software release. As regards an online procedure for rectifying, blocking or erasing data, since there have been no requests so far and it is very unlikely that there will be many in the future, the Commission believes that it would be more appropriate to introduce a lighter procedure which will be properly documented with the help of the Commission's data protection officer and the EDPS.

7.2. Data security

In accordance with the new guidelines and standards recently adopted by the Commission, the Commission will conduct a new risk assessment for IMI in 2010 and will update the security plan accordingly, identifying the parts of the system that need to be considered, the possible threats and the necessary infrastructure and software measures. If the risk assessment reveals the need to introduce additional security measures, these measures will be gradually incorporated in future software releases.

In early 2011 there will also be an external audit, which will focus mainly on the performance and stability of the system but may also cover some data protection and security issues.

7.3. Review of the Professional Qualifications Directive

An evaluation of the Professional Qualifications Directive will be carried out in 2010-2011; this will include an assessment of administrative cooperation and the use of IMI, including data protection concerns.

8. CONCLUSIONS

The Commission is satisfied with the implementation of the Recommendation and the state of data protection in IMI. Nevertheless, it will continue to work on further improvements to the system, particularly technical and data security improvements.

The Commission also intends to explore the possibility of extending IMI to other areas of the Internal Market while benefitting from further practical experience with its use in the area of Services. Any future proposal for EU legislation will take on board these developments and reflections so it provides a solid and future-proof basis for IMI and data protection.

In the first quarter of 2011, a staff working paper will be published on the functioning and development of the IMI system in 2010. This report will also cover data protection.