EUROPEAN DATA PROTECTION SUPERVISOR

PETER HUSTINX
SUPERVISOR

Mr Jonathan FAULL
Director-General
DG Internal Market and Services
European Commission
BRU-SPA2 08/020
B-1049 Brussels

Brussels, 27 July 2010
PH/ZB/ktl/ D(2010)1194 **C 2010-0025**

Subject: Commission report on the situation of data protection in the Internal Market Information System (IMI) (COM(2010)170 final)

Dear Mr. Faull,

As anticipated in our informal comments on the draft Commission report, now that the report has been adopted, the EDPS would like to take stock of what has been achieved and what further progress needs to be made on the issues raised in the report. A copy of this letter will be published on our website and circulated to data protection authorities in European Union Member States.

General comments

First of all, let me say that we welcome the progress made and the good cooperation between our services based on the step-by-step approach agreed upon. We appreciate the good work of your team and also encourage you to continue keeping data protection in mind when further developing the system and before extending it to other areas of internal market legislation.

This should include further safeguards implemented at the practical level, using the principles of Privacy by design, and also cooperating, as necessary, with stakeholders, including data protection authorities in Member States, to make sure that their concerns are addressed. The audits and periodic reporting briefly mentioned in the report are particularly welcome and encouraged by us as tools to ensure verification of compliance and good administration.

Comprehensive framework

Our main comment concerns the need for adoption of a new legal instrument, preferably a Council and Parliament Regulation, necessary to set a more comprehensive framework for the operation of IMI and provide for legal certainty and a higher level of data protection. In our earlier interventions in relation to IMI, we continuously underlined the importance of such framework.

Taking into account the expected scale and complexity of the system, as well as the need to obtain some experience with the practical use of IMI by the Commission and the Member States, we were sensitive to the Commission's preference for a step-by-step approach. Based on this approach, significant progress has been made so far, which included - in addition to progress at the practical and technical level - the adoption of the following documents:

- Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC);
- Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI) (C(2009) 2041 final);
- Commission Decision of 2 October 2009 on 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 (2009/739/EC); and, most recently,
- Commission Report of 22 April 2010 on the state of data protection in the Internal Market Information System (COM(2010) 170 final).

While we are pleased with the results that the step-by-step approach has brought so far, it will be inevitable for an important and complex European information system such as IMI, that a binding legislative instrument be adopted as a subsequent step, preferably under the ordinary legislative procedure. Its adoption should not be unduly delayed. As we discussed with your services on a number of occasions, work on the development of such an instrument should take into account the first experiences with IMI and should start as soon as possible.

The report shows that the system has already been expanded significantly, with over 4500 competent authorities registered to use IMI by the end of January 2010. In 2009 about 2700 information requests were made; this figure has shown an exponential growth, from just over 300 requests in the first quarter of 2009 to over 1100 in the fourth quarter, mainly due to the introduction of exchanges under the Services Directive. This means that - while the use of the system is still in a relatively early phase – an increasing amount of data is being processed and a comprehensive set of data protection safeguards will become increasingly necessary. The legislative process itself will take time and adequate safeguards will be needed before IMI will become a truly large-scale information system.

For these reasons, we urge you to start making the necessary steps towards building this comprehensive legislative framework as soon as possible.

Practical progress

As to the progress made at the practical level, we welcome that national data protection authorities have been consulted in many countries, that privacy notices have been posted at national or local level, and that data protection has been made an integral part of the training provided to users of the system.

We also welcome that the Commission's IMI webpage provides a good overview of the functioning of IMI, including its data protection aspects. The engagement of stakeholders including national - and, where relevant, sub-national - data protection authorities, as well as training, awareness raising and transparency are particularly important safeguards to ensure fair processing of data in IMI.

We furthermore welcome that steps have been taken to verify and ensure the security of the system, and that the Commission plans to conduct a new risk assessment for IMI in 2010 and update its 2009 security plan accordingly.

We also encourage the Commission to explore possibilities for improvement of the existing authentication measures in the longer term. These are crucial to induce trust among the users of the system, especially in an environment where - at the current level of harmonization of data protection among Member States - still very different practices exist. The initiative in the report that an external audit in early 2011 may also cover at least some issues related to data protection, and in particular, data security, is welcome and encouraged.

With regard to the alert system, we find it very important that the system was developed in such a way as to restrict the information circulated to what is strictly necessary. For example, competent authorities and IMI users cannot send and receive alerts by default as this function has to be activated separately; checklists to ensure necessity and proportionality are to be completed before sending off the information; information is only sent, by default, to the country of establishment; alert coordinators provide an additional scrutiny to ensure that no unnecessary alerts are circulated; and finally, the Commission receives alerts without personal data.

In addition, we welcome that the report clearly states that once the risk that triggered the alert has disappeared, the alert needs to be closed by the responsible authorities in the Member State of establishment. We also welcome that the responsible authorities are sent email reminders to close cases, that the alert becomes invisible upon closure, and that all personal data contained in it is automatically removed from the system within six months of closure at the latest.

Further safeguards

With regard to the retention of personal data contained in bilateral information exchanges, our concern remains that as there is no deadline set forth for “manual” closure of cases by case handlers and as the system does not provide for automatic deletion of inactive cases irrespective of closure, some cases may remain open unnecessarily and for an unduly long period of time.

The statistics provided on the Professional Qualifications Directive for 2009 show that in about seven percent of the cases the information requested is not provided within eight weeks, and therefore, these cases may remain open and inactive for a potentially longer period. Although this figure does not appear excessive, it is certainly not negligible, and, in the long term, may also have cumulative effect, and result in a large number of inactive, but open cases, containing potentially outdated data.

Therefore, we welcome your plans to build technical safeguards into the system, such as urgency lists and reminders, to ensure that cases are closed in a timely manner. This should be done without delay and it is particularly important where criminal record information or other information that may become obsolete or inaccurate over time is exchanged.

We recommend that you monitor the situation (number of cases open for a long time and the reasons therefore), and explore further what other measures can be taken to conclusively ensure that cases are closed in a timely manner. One option, already suggested earlier by us, is to add a new “default setting” for case closure: for example, if a case has been inactive for six months as of the last communication, one or more reminders should be sent automatically. If

still no formal closure or other activity takes place, the system should automatically delete the case. A similar mechanism should also help ensure that alerts are closed as soon as they are no longer needed.

As to the plans to increase the conservation period from the currently available six months after closure, these need to be carefully reconsidered. This means that first there should be a very specific and concrete justification as to why the currently available six months are insufficient and how much additional time is needed. Second, while “blocking” of data may be an option to keep truly necessary data in the system for a limited period of time, its implications should be fully explored, including a clear understanding on who can access blocked data and for what purposes.

Third, a limited time period must also be set. Extension of the current conservation period should not be taken lightly: the longer the data are retained, the higher the risks of "function creep": considering the sensitive nature of many of the data held in IMI, including alert data and criminal records, it is particularly important to ensure that the data retained are not subsequently used for unforeseen purposes or disclosed to unforeseen recipients who might use them for additional, incompatible purposes. Of course, the findings of the Court of Justice in *Rijkeboer* (C-553/07) must also be taken into account.

Following the principle of Privacy by design, we also encourage you to continue considering the possibility of "building in" into the system architecture ways to assist competent authorities to cooperate, in case an access request or request for rectification is made to one of them and they need to contact their counterparts elsewhere to be able to authorize the request or to ensure that the correction or update is made throughout the whole system.

When such cooperation between competent authorities is necessary to ensure that access will be provided or corrections will be made, the IMI system architecture should be taken advantage of: competent authorities must be able to communicate with each other about access or rectification requests in the same efficient way as when using their question sets for their information exchanges under the Professional Qualifications or Services Directives. The fact that thus far, at this early stage of the functioning of the system, there has not been a significant amount of access or rectification requests reported does not mean that an efficient procedure for this should not be foreseen for the future, in a preventive and timely manner.

As for the national use of IMI, we welcome that the report specifically mentions that national data protection authorities should be consulted before any national use of IMI is authorized and that their concerns should be addressed. For example, it is possible that in some countries there may not be a legal basis for the national use of the alert system while other bilateral information exchanges may not pose data protection problems.

Follow up of comments

We hope you will find the above comments helpful. As the next step, we would appreciate if you could react to the comments raised above.

In particular, we look forward to receiving your feedback on the concrete steps to be taken towards adoption of a comprehensive legal framework for IMI, preferably under the ordinary legislative procedure, with short timelines.

Also on other points we look forward to your reaction:

a) firm commitment towards incorporating data protection into audits and periodic reporting on IMI (including also data security aspects);
b) proposed steps and timelines towards practical implementation of items noted as "technical improvements" under Section 7.1 of the Commission report (reminders and urgency lists);
c) proposals for other "technical improvements" as suggested in this letter, following the principle of Privacy by design, including default setting for automatic closure of inactive cases (both alerts and exchanges); and "building in" mechanisms to facilitate cooperation among the competent authorities with respect to access and rectification requests;
d) a specific and concrete justification for any proposed extension of the currently applicable six months conservation period, with detailed explanations regarding the implications of such an extension, and proposal of adequate data protection safeguards for an eventual period of "blocking".

We look forward to working with you towards building, step-by-step, a comprehensive data protection framework for IMI.

In the light of your feedback, we will also consider the possible need for a joint meeting with national - and, where relevant, sub-national - data protection authorities in due course, to look into issues that may arise in the context of supervision or further consultation with regard to IMI.

Yours sincerely,

(**signed**)

Peter HUSTINX