ARTICLE 29 DATA PROTECTION WORKING PARTY

01911/07/EN
WP 140

Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI)

Adopted on 20 September 2007

TABLE OF CONTENTS

1. Introduction

The project of setting up a computerised system as a tool for exchange of information concerning personal data raises important concerns with respect to the fundamental rights of individuals, in particular the right to privacy.

The complexity of the Internal Market Information system (IMI) and the diverse issues it involves led DG Internal Market of the European Commission to request the opinion of the Article 29 Working Party (WP29). The WP29 Opinion will focus on the same issues addressed in the documents "Issue paper on Data Protection in IMI" (D-4784) and "General Overview" (D-1804). The objective of this Opinion, then, is to analyse the implications IMI creates with respect to personal data, protected by Directive 95/46/EC ("Data Protection Directive") and Regulation (EC) No 45/2001 ("Data Protection Regulation").

> In March 2006, Member State representatives in the Internal Market Advisory Committee gave the go-ahead to develop the Internal Market Information (IMI) system, aimed at improving communication among Member State administrations. IMI is an electronic tool that provides a system for information exchange to enable Member States to cooperate more effectively on a day-to-day basis in the implementation of the Internal Market legislation in the sectors covered by Directives 2006/123/EC[1] on services in the internal market, and Directive 2005/36/EC on the recognition of professional qualifications of regulated professions and services[2]. IMI is intended to help overcome practical barriers that make it difficult for the competent authorities of Member States to communicate and cooperate with each other, such as different administrative and working cultures, different languages, and a lack of clearly identified contact points in other Member States. Its aim is to reduce administrative burdens and to increase efficiency and effectiveness in day-to-day co-operation between Member States.

The importance of developing administrative cooperation between Member States was well-recognised in the renewed Lisbon Strategy[3] and in the EU Better Regulation agenda[4] because it will help improve the application of Community law by Member States.

It is up to Member States to ensure the smooth and effective functioning of Internal Market law within their respective territories. But they need the tools to work together and with the Commission in order to ensure that the full benefits of the legal framework are realised for citizens and businesses. IMI is being developed in response to that need, and in response to the legal obligation set out in Article 34 (1) of Directive 2006/123/EC on services in the internal market (hereinafter "Services Directive") to establish an electronic system for the exchange of information between Member States.

> The first priority within the IMI framework will be to develop applications to support Directive 2005/36/EC ("Professional Qualifications Directive") and the Services Directive.

[1] OJ L 376, 27.12.2006, p. 36.
[2] OJ L 255, 30.9.2005, p.22.
[3] See page 18 COM (2006) 30 final "Time to move up a gear –the new partnership for growth and jobs"
[4] See page 3 COM(2006) 689 final "A strategic review of Better Regulation in the EU"

2. Description of the IMI system

IMI will consist in a number of horizontal applications providing language support and a communications tool between Competent Authorities, as well as vertical applications to support specific pieces of legislation. The IMI itself will be stand-alone, and all its functionality will be accessible from a web page. The main users of the systems will be Administrations and Competent Authorities of the Member States.

2.1 Architecture: Commission tasks and national systems

IMI's structural priority is to facilitate Member States' performance of their legal obligations to exchange information, but it will also permit new and more complex forms of administrative cooperation. IMI will provide a search function to identify the appropriate competent authority in the partner Member State and a set of pre-translated menus with a structured set of questions to support the required exchange of information. WP29 emphasises that it is crucial that the Commission must design and draft the menus and structured set of questions in such a way as to minimize the risks of collecting data which are irrelevant, disproportionate, or pertain to third parties. In turn, it is equally important that the users of the system (Competent Authorities exchanging information) ensure that they do not use the system to exchange irrelevant or excessive data, or data that pertain to third parties.

The system is designed to take into account the variety of arrangements of national administrations in different Member States (centralised or decentralised systems, at different degrees, for example) and therefore allows each Member State to customise the organisation of its competent authorities for IMI purposes and maximise effectiveness.

The key actors are briefly described below, with reference to the General Overview document.

2.2 Authorities involved

The main actors in the IMI system will be the Competent Authorities throughout the European Economic Area (EEA) who will use IMI to exchange information relating to the areas of Internal Market legislation on regulated professions and services.

With respect to the role and powers of each authority in the processing of personal data, it is necessary to emphasise that both the European Commission and the Member States will play important roles in the IMI system. Each Member State will have the opportunity to design its own structures to suit its specific needs, but all of the Member States will need to fulfil the same function in the IMI context.

The specific roles of the authorities are described in the following excerpt from the Commission document entitled "Data Protection in IMI."

2.2.a European Commission

The document "Data Protection in IMI" provides that "*The data base will be stored on a Commission server in Luxembourg. All exchange of data will go through this server and exchanged data will be stored on that server. The Commission's responsibilities, [generally delegated to the EU System Administrator], will be related to the registration of the National IMI Coordinator in each Member State, database administration at the system level,*

administration of legislation-based question sets and translation of all IMI system components into all official EU languages."

All responsibility for data entry, compliance with data use and quality standards, notification and maintenance of the rights to access, correction and erasure, is at the national level.

WP29 emphasises that, given that the Commission will also be carrying out certain data processing tasks (i) both on behalf of the Member States (e.g. storage and erasure) and (ii) on its own account as the system administrator (data pertaining to IMI users and contacts), the Commission must share the responsibility for compliance with applicable data protection laws with Competent Authorities in Member States. The tasks and responsibilities of the Commission and Competent Authorities in Member States must be clearly defined.

2.2.b Competent Authority (CA)

The same document states, in relation to Competent Authorities, that "*Public administrations in each Member State will be designated as Competent Authorities [and may be competent for more than one area of legislation]. After being registered in the system, CAs will be able to send and receive information requests via IMI.*" Regardless of their relations with DIMICs (in those Member States which opt to designate them), all CAs in a given Member State will be supervised by that Member State's NIMIC[5].

The WP29 points out that in some Member States it is not always a single CA which holds all the information that a requesting CA may need with respect to a particular migrant worker or service provider. For example, it may be necessary to distinguish between recognition of degrees, for which the Competent Authority might be a particular cabinet minister, and recognition of professional licensing evaluations, for which the CA might be a professional association. In such cases, the requesting CA may need to contact two different CAs. To address these and similar issues, the WP29 welcomes that the designers of IMI have foreseen a network of coordinators within each Member State to help requesting CAs find their counterparts in other Member States, as will be described below in Sections 2.2.c and 22.d. At the same time, the WP29 emphasises that the interface of IMI must also be designed in such a way as to minimize the risks of confusion as to which CA is competent with respect to any particular issue.

2.2.c National IMI Coordinator (NIMIC)

Each Member State will appoint one national coordinator for the IMI system to serve as its highest-level IMI authority and the direct interlocutor in communication with the European Commission and other Member States for all technical IMI issues, and when escalation procedures are necessary to elicit responses.

As established in "Data Protection in IMI", a National IMI Coordinator will be able to view a list of all requests sent or received by CAs or delegated IMI coordinators of its Member State; however, this list will not contain any personal data.

The WP29 welcomes this limitation as indeed, as confirmed by the Commission, there appears to be no need for NIMICs to access personal data in order to be able to carry out their tasks. Therefore, access to personal data would be a violation of Article 6.1(c) of the Data

[5] The role of DIMIC (delegated IMI coordinator) and NIMIC (national IMI coordinator) will be discussed in Sections 2.2.c and 2.2.d below.

Protection Directive, which requires Member States to ensure that processing of personal data is: "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*."

That said, the WP29 also believes that it is necessary to make this limitation explicit, and to identify more precisely the information that these lists will contain.

The WP 29 is also of the opinion that the division of the competences and duties between the Commission, Coordinators and Competent Authorities should be more clearly established, given that their IMI roles are best described as joint controllership. To some extent, the WP29 sees that each actor in the IMI system will play both the roles of data processor and data controller in some capacity, depending on the processing activity performed in each specific situation. The complexity of IMI means that it may not always be clear whether actors are controllers or processors or both. The potential for this confusion underscores the importance of identifying explicitly and specifically the objective for each data processing action; this will enable all parties to understand the appropriate uses of data and how to comply with data protection rules even in a situation where the precise nature of their intervention is mixed or unclear.

2.2.d Delegated IMI coordinator (DIMIC)

A third kind of role, at the discretion of each Member State, is optional DIMICs to coordinate and supervise the roles played by individual Competent Authorities in a single legislative or policy area.

As explained in the document "Data Protection in IMI", a delegated IMI coordinator would be able to view a list of all requests sent or received by competent authorities to which it is linked. As the document notes, the list will contain sufficient high-level information for the coordinator to monitor the flow of requests, but will contain no link to any personal data. This role is specifically designed to enable Member States with centralised CA systems to coordinate with Member States that are more decentralised or that have many Competent Authorities.

The WP29 notes that the distinct roles of NIMICs and DIMICs, and their responsibilities with respect to ensuring adequate protection of the personal data that are exchanged under their supervision, must be clarified and better defined in order to more definitively analyse their implications.

2.2.e Linked Authorities

A Competent Authority may also grant "*monitoring access"* to other public administrations in its Member State. *Monitoring access* allows another authority to view a list of all requests sent or received by the Competent Authority, without access to any personal data processed.

This feature would allow professionally-linked organisations (such as professional associations) the possibility to view an anonymised list of requests directed to related organisations, perhaps with the objective of ensuring that requests are referred to the proper CAs. However, the WP29 believes that the specific goals and benefits of the linked authority's role, as well as the specific information to which they have access, must be more explicitly defined, to ensure that there is indeed no unauthorised access to personal data.

2.3 Roles and rights in the system

The main data processing acts will take place within the IMI system during the information exchanges between Competent Authorities of Member States, but there will also be processing of personal data by the Commission itself, of information about Competent Authorities. The parties involved in the processing of personal data, whether they be CAs, NIMICs or DIMICS, will always be subject to the national laws implementing Directive 95/46/EC[6] in the Member State in which they are situated The Commission, in turn, will be subject to the Data Protection Regulation.

Given that there are different roles and various actors in the IMI system, it is necessary to establish for which kinds of data processing each of these actors is considered to be the "data controller". The "controller" is defined in Article 2(d) of the Data Protection Directive as "*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*."

On the other hand, the Directive defines "data processor" in Article 2(e) as "*the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*." Thus the processor is the person or authority that effectively processes data upon the controller's instruction.

The Data Protection Directive further stipulates in Article 17.3 that the processing of personal data by a third (non-controller) party must be governed by a contract or legal act binding the processor to the controller and which ensures, in particular, that the processor shall only act on instructions from the controller.

This document will not analyse in-depth every possible processing scenario, but the WP29 considers the controller in each individual processing act to be responsible for compliance with the principles and safeguards established in this document, including with regard to security measures. A processor, in turn, will be responsible for adhering to its confidentiality obligations, taking the appropriate security measures and ensuring that it acts upon instructions from the controllers.

The Competent Authorities and the Commission must have an explicit understanding of shared responsibility for the storage and deletion of data. A document setting out the framework between the controller and processor for these processing acts will need to be drafted. This document must clearly identify the tasks and responsibilities of the parties**.**

The structure of IMI creates an unusually complex network of controllers and processors. Accordingly, it is necessary to understand that the responsibilities of each party may vary with the nature of each individual action, and that it may not always be clear whether an actor is a controller or a processor. Of course, regardless of this distinction, all parties that control or process data must maintain the level of data security and comply with the data processing principles identified by the Data Protection Directive or the Data Protection Regulation, as the case may be.

---

6 OJ L 281, 23.11.1995, p. 31

3. Personal data processed

The IMI system has the potential to affect the fundamental rights of a large number of migrant workers and service providers who exercise their rights of free movement within the European Union. The system also stores data on the users of IMI (personnel of CAs, NIMICs and DIMICs).

Article 2 of the Data Protection Directive defines personal data as "*any information relating to an identified or identifiable natural person.*"[7] Given that IMI will process and store such data for two distinct purposes, the WP 29 can consider the system to include two distinct categories of personal data processing.

- The first relates to personal data of CAs (as well as of NIMICs and DIMICs) who will use IMI. Since they are user contacts, the system will store their telephone numbers, names, email addresses and similar information. The list of data which will be collected from these individuals must be specifically identified, and must comply with the requirement of the Directive's that it contains no more data than necessary for the system's functions (data quality).

- The second type of data processing is that related to workers and service providers within the context of the Services Directive and the Professional Qualifications Directive. These data will include the name, telephone number, email address, date of birth and nationality of each service provider (where relevant, usually, for purposes of identification) as well as data related to their professional qualifications and more sensitive data such as data on good conduct, disciplinary measures, penal sanctions and information related to the legality of establishment.

4. Legal analysis of the system and specific issues

4.1 Legal basis for the processing of personal data (Article 7)

The Professional Qualifications and Services Directives each create specific obligations for administrative cooperation between Member States, incorporating requirements to exchange information, in most cases related to "*identified or identifiable persons*." This means that the relevant legislative framework will undergo substantial changes as these Directives are transposed; however, the rules to be introduced with regard to the IMI must be consistent with the general data protection principles set out in the Data Protection Directive and the Data Protection Regulation.

The IMI system will unavoidably produce major effects on data processing mechanisms and the related supervision and control activities entrusted to the competent authorities.

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.*

[7] See Opinion 4/2007 on the concept of personal data. WP 136.

"*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 also mandates mutual assistance:

*"*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*."*

The cooperation required by these Directives must be executed diligently, but require improved capabilities and responsiveness. To this end, the Services Directive calls for the creation of an electronic tool for simplified, accelerated information exchange. Specifically, Article 34 of the Services Directive requires that "[*t]he 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.*"

WP29 believes that it is necessary to state clearly that the IMI system must respect the existing standards in the field of data protection. This requirement is explicitly specified in Article 43 of the Services Directive, which emphasizes the importance of continued and consistent application of the Data Protection Directive as well as of Directive 2002/58/EC ("Directive on privacy and electronic communications").

On a general level, the legal basis for data processing in the Member States is found in Article 7 of the Data Protection Directive, which establishes the conditions that legitimise data processing activities. Specifically, under Article 7(c) processing of personal data may take place when it is "necessary for compliance with a legal obligation to which the controller is subject*." Article 5(b) of the Data Protection Regulation contains similar provisions.*

As noted above, Article 34 of the Services Directive creates this legal obligation for data controllers and (once implemented in Member State laws) therefore permit them to process the relevant personal data. This legal base, however, raises several potentially problematic issues.

First, the Professional Qualifications Directive does not refer to any electronic tool for sharing information, although it also requires cooperation. Indeed, Article 56(2) lays down an obligation for exchange of information between Member States' competent authorities 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, but it does not provide for the establishment of an electronic system in this respect. Other provisions of the Directive also provide for information exchanges to the extent that a

competent authority has a reasonable doubt about a specific issue. Although in the opinion of DG MARKT the legal basis for the information exchange is to be found in these specific provisions, it is arguable whether there is a fully adequate legal basis for data processing using the IMI system in the framework of cooperation under the Professional Qualifications Directive.

Second, for Article 7(c) of the Data Protection Directive to serve as the legal basis for processing data, the Professional Qualifications and Services Directives must be transposed into national law. If a particular Member State has failed to transpose the Directives, it is again questionable whether an appropriate legal basis exists, and thus, whether the processing of data via IMI is permissible.

In addition, the WP29 also points out that, even if the Services Directive and the Professional Qualifications Directives, once implemented into national law, provide a legal basis of a general nature, it must be ensured that each individual exchange of data is justified. In particular, in accordance with the Data Protection Directive, each instance of data processing must have specified, explicit and legitimate purposes and an adequate legal basis specific to its purpose.

Finally, the WP 29 also points out that Article 7(e) of the Data Protection Directive may also arguably provide for an additional, complementary legal basis of the processing: *"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;"*. The purpose of the IMI system is to provide information and facilitate the cooperation of the various Competent Authorities in different Member States. This serves the public interest, in contributing to ensure the proper functioning of the internal market by those persons who want to avail themselves of the freedom of establishment and the freedom to provide services in the pursuit of their professional activity.

Despite the potential availability of Articles 7(c) and 7(e), considering the legal uncertainties noted, the WP29 recommends, as an *ad hoc* solution to support the legal basis, the adoption of a Commission Implementing Decision, as the Commission itself recently decided to do. In addition to strengthening the legal base of the processing, the Decision should also establish what data fields should be included in the database, the minimum content of requests, responses and flows, and should also specify the roles and responsibilities of the various actors and the legal requirements from a data protection point of view.

4.2 Application of the principles of data quality (Article 6)

4.2.a Data quality and necessity

The IMI system is a tool designed specifically to share information and to permit access to that information by Competent Authorities when needed. It constitutes an information flow, some of which is sensitive (with data held for six months, as explained in Section 4.2.c below), and which therefore must comply with the principles established in Article 8 of the Data Protection Directive. IMI is explicitly made subject to the Data Protection Directive's guarantees to safeguard the legitimate rights of data subjects, which have been transposed into national law in all of the Member States.

First, the requirement of data quality, set out in Article 6 of the Data Protection Directive, must be satisfied. This principle requires that personal data be collected only to accomplish explicit, legitimate and pre-determined ends, and that such data may not be further processed in a way incompatible with those purposes. Accordingly, compliance with this principle requires, then, that there be a clear definition of the purpose for the collecting and processing personal data using the IMI system.

Second, it is necessary to analyse compliance with the proportionality and legitimacy principles, keeping in mind the risks posed to data protection, fundamental rights of individuals, and especially the necessity, if it exists, to disclose information related to disciplinary proceedings.

4.2.b Proportionality

Proportionality is an essential principle in the legal framework established by Directive 95/46/EC and Regulation (EC) No. 45/2001. It requires that in the questionnaires used in the IMI for information exchanges, CAs may not provide information that is irrelevant or excessive considering the identified objective of the exchange. Therefore, in the context of information exchange concerning a migrant worker or service provider, the purpose must be defined in advance.

A full report of any information exchange may be printed in any official EU language by designated persons. IMI will also have uploading and storage capacities for relevant additional documents or images.

Furthermore, in the application of the proportionality principle, the WP29 recommends that the CA responsible for the IMI should carefully assess whether it may be appropriate to limit the number of persons eligible to send and answer information requests.

Additionally, in the IMI system, it is important that the list of questions via which CAs will be able to exchange information be developed with attention to proportionality. To this end, from the data protection perspective, the safest option would be to specifically list all data fields (that is, all pre-set questions and answers) in the proposed Commission Implementing Decision (see Section 4.1). However, the WP29 acknowledges that the designers of the system may wish to keep a certain amount of flexibility to allow future adaptations and improvements of IMI. To address these competing concerns, while at the same time also ensuring the transparency of the information exchange, the WP29 recommends that the new Commission Implementing Decision should explicitly state that (i) all pre-defined questions must directly derive from the requirements of the Professional Qualifications and Services Directives (or possibly, from additional future directives to be included in an updated annex to the Commission Implementing Decision), (ii) must be drafted in consultation with stakeholders in Member States and (iii) must state that the pre-defined questions and answers shall be made publicly available on the IMI website.

4.2.c Special questions relating to retention personal data

The intention of the Commission is to provide a 6-month automatic retention period, and also to build-in automatic reminders into the system architecture about deletion of data.

The Data Protection Directive requires that personal data shall only be kept for the period of time necessary to achieve the purpose for which the data have been collected or processed (Article 6 (1) e) and Regulation (EC) No. 45/2001).This is essential to ensure compliance with the principle of proportionality of the processing of personal data.

The WP29 believes that the 6-month period proposed by the Commission may appear to be reasonable at first sight, considering that there may be follow-up questions regarding the same case between competent authorities. However, the WP29 recommends that the future Commission Implementing Decision should explain the reasons to retain the data for this specific period.

4.2.c.i Retention by the Commission

The data stored on the Commission server in Luxembourg must be subject to similar data protection rules as those applicable to data stored in Member State databases. In particular, these data may only be retained in the IMI system as long as needed to fulfil the purpose of their collection.

The data contained on the server must not be used for other reasons or information requests, and always be processed in conformity with data protection law. It is of paramount importance that they are protected against unauthorised access.

The determination of the appropriate retention period in 6 months, and therefore of compliance with Article 4 e) of Regulation 45/2001, will require a clear and explicit understanding of the objective or purpose of every data processing action, and it is also of paramount importance that they are protected against unauthorised access.

4.2.c.ii Retention period of data processed and stored by national authorities

In the event that national authorities also retain personal data, these data must only be stored until the conclusion of the exchange or transaction for which they were collected, with particular deletion timelines as required by the national law of each Member State.

This requirement becomes extremely important in situations where a CA official is able to store this information on his individual computer's local hard disk or other device. The retention period limitation still applies, and data must be blocked as soon as they have ceased to be useful for the purposes for which they were obtained. This requirement is, of course, in addition to the obligations created by data protection rules established at the national level.

4.2.d Specially protected data

The processing of sensitive data creates the need for special attention to compliance with data protection standards. The conditions and restrictions on sensitive data are established by Article 8 of the Data Protection Directive and in Article 10 of the Regulation (EC) No. 45/2001.

These data include indications about racial and ethnic origin, political opinions, religious or philosophical convictions, membership in trade unions, health and sexuality. Processing of data relating to offences, criminal convictions or security measures are also considered sensitive data by the Directive (and the Regulation (EC) No. 45/2001). Member States may also consider as sensitive data those data relating to administrative sanctions or judgements.

The "Data Protection in IMI" document states that IMI "*is not intended*" to process sensitive data of this kind. However, IMI exchanges could possibly include health data – for example, regarding job applicants who are disabled.

The WP29 is of the opinion that the expression "is not intended" is too permissive and vague. To ensure compliance with data protection requirements, the language must be mandatory: sensitive data "shall not be processed." Any exceptions should be clearly specified and made subject to additional safeguards.

Article 8 of the Data Protection Directive clearly sets out that the "*Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*.". Article 10 of the Regulation (EC) No. 45/2001 contains similar wording.

Specifically, Article 8.5 establishes that "*[p]rocessing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority*.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority"

The Professional Qualifications Directive provides a legal basis for the transmission of criminal data and disciplinary measures in Article 56.2, reaffirming that exchanges of data must conform to the requirements cited above. However, the specific conditions for exchange of information of criminal data should be based in national law implementing Directive 95/46/EC.

"*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 [Data Protection] 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 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)*."

Furthermore, Article 33 of the Services Directive foresees specific rules for the exchange of information regarding the good repute of the migrant service provider. These rules must be fully analysed well in advance of implementation to assess their data protection implications. "*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 involving fraud taken by their competent authorities in respect of the provider which are directly*

relevant to the provider's competence or professional reliability. The Member State which supplies the information shall inform the provider thereof."

With respect to the legal requirements that legitimise data processing, it is necessary to keep in mind the principles established in the Data Protection Directive, which explains more concretely the concepts of proportionality, quality and use limitations in data protection. It is essential to ensure that personal information is both accurate and current when sensitive data are exchanged. For example, criminal records which are outdated should not be exchanged**.**

Furthermore, there will be situations in which data related to administrative sanctions are not essential for the pursuit of a profession in a particular Member State. In this case the professional statutes of both the Member State of origin and the Member State to which a service provider migrates must be considered. Without considering the particular relevance of the data in this type of situation, IMI data processing will have to comply with the principle of proportionality required by the Data Protection Directive[8].

With respect to data regarding outstanding debts or criminal infractions, the "Working Document on Black Lists" (WP65)[9] establishes the following:

"*Article 8(5) and (6) of Directive 95/46/EC mentions the processing of data relating to criminal offences or criminal convictions, and lay down that, generally, such processing may only be carried out under the control of official authority unless the Member States adopt exceptions which must have adequate safeguards in order not to affect citizens' fundamental rights and must also be notified to the European Commission.*

"*The legitimacy of processing the kind of file, which incorporates data on criminal offences, centres on the obligation on authorities to maintain security and public order. Beyond any doubt, this principle justifies such processing provided that the restrictions mentioned in the preceding paragraph are observed, as provided by Article 7(e) of the Directive.*

"*As regards the processing of personal data relating to criminal offences, most Member States have files incorporating this kind of information which are controlled by an official authority…*

"*This kind of processing must always uphold the data quality principles contained in the Directive, and those on accuracy and up-to-dateness in particular. Likewise, special attention must be paid to the right to routine or automatic correction and erasure of a subject's data once the time provided by law has passed and to marshalling to this effect the various mechanisms which make this possible, easier and prompter, given that the retention of information referring to a person on these files beyond the periods laid down can have prejudicial consequences.*

[8] For example, Directive 2002/92/EC on insurance mediation clearly indicates the extent to which criminal and reputation information are relevant for the practice of that profession. Article 4.2 establishes that "*[i]nsurance and reinsurance intermediaries shall be of good repute. As a minimum, they shall have a clean police record or any other national equivalent in relation to serious criminal offences linked to crimes against property or other crimes related to financial activities and they should not have previously been declared bankrupt, unless they have been rehabilitated in accordance with national law*."

[9] WP 65. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp65_en.pdf

"*This is especially relevant with not guilty verdicts, limitation of liability or the discharge of bankrupts. There would be no point in retaining such data. It should be noted that most Member States regulate these aspects under the respective criminal law, and the criteria laid down to this effect vary.*

"*Another fundamental point, which must be considered, is access to information, i.e. determining which persons or institutions are entitled to access the data included on these files. Data subjects must also always have the right of access to the information concerning them on a file.*

"*This access provision can give rise to somewhat complex and problematic situations, such as when the data subject is a job seeker in that, in those Member States in which it is permitted, as part of the selection process, an employer could ask a worker to produce the contents of a certificate of any criminal record issued by a public authority data controller. The candidate would obtain such a certificate, which could contain data on any criminal convictions or other security measures. The employer thus gains access to the content of certain data which is not directly legally recognised.*

"*This hypothesis can be further complicated in situations which may arise as a result of the employer's subsequent use of this information, given that, in principle, simply consulting the information made available by the candidate during the selection process would not be in breach of the provision of Article 8(5) of the Directive, whereas any subsequent manual or automated processing could be*."

In order to minimize unnecessary transmission of these sensitive but not always relevant data, the WP29 recommends that whenever no actual criminal record information is strictly necessary to be transferred, pre-defined questions and answers in the IMI interface should not include a request for criminal records and should be phrased differently, in such a way to minimize sharing sensitive data. For example, a host country competent authority may be satisfied with knowing that a migrant lawyer is legally registered and in good standing with his home bar association, and does not need to know whether he has a road traffic offence on his criminal record, if that does not prevent him from working as a lawyer in his home country.

4.3 Use of a national identification number.

As stated in the document Data protection in IMI: "*Finally, Member states, in accordance with Article 8 para 7. of Directive 95/46/CE shall determine the conditions under which a national identification number or any other identifier of general application may be processed. Processing such personal data will certainly make the information exchange between competent authorities easier to the extent that it will facilitate the identification of the provider concerned. National restrictions on such an exchange of data would not therefore seem justified*."

This question is highly sensitive. Regulation of processing national identification numbers is expressly left to the Member States' discretion in the Article 8 (7) of Data Protection Directive's: "*Member states shall determine the conditions under which a national identification number or any other identifier of general application may be processed*." Therefore, Member States are competent to determine all the conditions and modalities under

which a national identification number may be conveyed via IMI, including possible restrictions. For example, in some Member States, identification number usage is strictly regulated and subject to the authorization of a special committee set up within the Data Protection Authority. Such restriction is valid under the Data Protection Directive and therefore is applicable in the IMI context as well.

5. Rights of data subjects

5.1 Right of information

Articles 10 and 11 of the Data Protection Directive require the controllers to inform data subjects of the processing of their data. The Data Protection Regulation also contains the obligation of information. For those cases in which data are collected directly from the data subject, Article 10 of the Data Protection Directive sets up the requirement of clear and complete information on the system and obliges the controller to inform data subjects about the existence, purpose and functioning of the scheme, the recipients of the data and the right of access, rectification and erasure.

In addition,, Article 11 of the Data Protection Directive requires data controllers to inform data subjects when their personal data are collected from a third party and not from them directly. The right of information also allows the exercise of the aforementioned rights.

In order to facilitate this right of information, the Article 29 Working Party would recommend a layered approach to the notice provision.

By this layered approach, several measures could be taken into account, as for example an information notice providing that the information required under Articles 10 and 11 of the Directive - namely, the identity of the controller and the purposes of processing, - must be provided beforehand to ensure a fair processing.

First, a detailed notice should be included on the Commission's website, containing information required under Articles 10 and 11 of the Data Protection Directive and corresponding provisions of the Data Protection Regulation, and describing the roles of the Commission and the CAs in detail, and making special reference to the data subject's rights in clear language.

Second, each CA should provide a privacy notice on its website, containing also a link to the Commission Privacy notice.

Third and finally, in the IMI system as in other contexts, the required notifications and information must also be supplied directly, individually, and immediately, as soon as documents are obtained from citizens or Competent Authorities. This obligation should be made explicit to all actors in the IMI system.

5.2 Rights of access, rectification, erasure and blocking

Article 12 of the Data Protection Directive, related to the right of access and rectification, gives the data subject the right to access his/her stored personal data in order to check their accuracy and rectify the data if they are inaccurate, incomplete or outdated. The IMI system must be constructed so as to enure compliance with individuals' right to access and rectify incorrect, incomplete or outdated data.

Furthermore, data subjects must have the right to rectify or erase their data where the processing of such data does not comply with the provisions of the Data Protection Directive, in particular because of the incomplete or inaccurate nature of the data (per Article 12(b)).

In the event of rectification or blocking of inaccurate or otherwise invalid data, the data controller must notify all the Competent Authorities which have been part of the unlawful processing as well. This responsibility must be made explicit, and an IMI interface specifically designed to permit such notification would be extremely useful to all parties. It may also be necessary to create a procedure to ensure that if citizens exercise their rights to data erasure, then these data are actually removed from all databases, including those outside of the IMI system, establishing also a coordination between Competent Authorities.

Any objection to granting access must be based on a specific exception under the applicable national data protection law, and duly motivated.

If the authority involved fails to respond within a reasonable time, or fails to raise objections, the authority to which the access request has been submitted may decide on the basis of its own national law. If the authorities do not agree as to whether the access should be granted, the authority that supplied the information should be the one to ultimately apply the criteria for access provision.

If access is denied, it must be made clear on what grounds it is denied, and that the data subject may contact another competent authority instead to access the data, or approach the Data Protection Authority as provided in Art. 28, without prejudice of the right to commence legal proceedings.

Similar cooperation mechanism should apply with respect to rectification, erasure or blocking.

In case of a request for data addressed to the Commission, the Commission may only give access to data to which the Commission itself has legitimate access, and in all cases, the data subject needs to be directed to the authority which has access to the information, taking into account the safeguards established in the Data Protection Regulation.

5.3 Measures for redress

It is also vital to ensure that data subjects have the right to legal recourse in cases in which the rights guaranteed to data subjects are violated. People who suffer adverse consequences as a result of improper or illegal processing of their personal data must also have the right to demand remuneration for the damage they suffer.

6. Security

In conformity with Article 17 of the Data Protection Directive, data controllers must implement adequate technical and organizational measures to protect personal data from destruction, accidental or illegal loss or transmission and unauthorised access. These security measures should be proportionate to the ends for which the data are collected and should comply with the security rules of the individual Member State. Similar requirements are also set forth in corresponding provisions of the Data Protection Regulation.

The legality of a system of data processing with exceptional risk potential is dependent on the maintenance of an adequately high level of data security in every aspect of the system's functionality.

Moreover, to ensure the security of the system in light of the possibility of especially sensitive data (such as those related to criminal sanctions), the WP 29 believes it is essential to require implementation of a series of specific measures of a technical and organisational nature that would avoid alteration, loss, unauthorised processing or access, guaranteeing the confidentiality and integrity of the information. While this document does not endorse a specific technological framework or tool for data security, these criteria must be fulfilled for IMI to adequately protect personal data.

Security measures must be sufficient to ensure that:

- unauthorised persons cannot access the system;
- it is possible to check which data have been processed, when, and by whom;
- data entry is controlled, to impede the unauthorised addition or modification of data;
- access controls are in place that guarantee that users have access only to the data they are competent to process;
- communication is controlled to enable determination of which authorities are authorised to release certain data; and
- transmission is secure to prevent unauthorised access, copying, modification or suppression of data during information exchanges.

Other measures are focused on generating back-up copies, data recovery and pre-implementation testing using real data and transmission through telecommunications networks, either by encoding the information or using other mechanisms to guarantee that the information is not intelligible or capable of manipulation by third parties.

The Commission will be responsible for these measures with respect to the function and security of the central server, but secure networking practices are also of paramount importance at the Member State level.

Furthermore, the Commission is subject to the security requirements set forth in the Data Protection Regulation, but these should be interpreted in light of best practices in Member States.

Competent Authorities will be responsible for compliance with the data protection laws adopted in their respective Member States, and with the requirements for data security laid out in Article 17 of the Data Protection Directive.

The WP29 also recommends that, since the Commission sees no need to access the personal data of the migrant workers or service providers stored on the central server, these data should be encrypted to allow a secure communication between the Competent Authorities of Member States, thus effectively preventing the Commission from accessing these data.

7. DPA notification and prior checking.

In the application of Articles 18 to 20 of the Data Protection Directive, organisations that use the IMI system will have to comply with the requirements of notification to, or prior checking by, at least some of the national data protection authorities.

In Member States providing for such a procedure, the processing operations might be subject to prior checking by the national data protection authority, inasmuch as those operations are likely to present a specific risk to the rights and freedoms of data subjects. This could be the case where national law allows the processing of data relating to suspected criminal offences only under specific conditions (which themselves might include prior checking by the competent national supervisory authority).

This could also be the case where the national authority believes that the processing operations have the potential to exclude reported individuals from a right, benefit or contract. The evaluation of whether such processing operations fall under prior checking requirements depends on the national legislation and the practice of the national data protection authority.

Article 20 of the Data Protection Directive also provides that prior checking may be carried out in the context of preparation either of a measure of the national parliament or of a measure based on such legislative measures, which define the nature of the processing and lay down appropriate safeguards.

On the other hand, the European Commission appointed a Data Protection Officer (DPO) according to Article 24 of the Data Protection Regulation. The data processing operations carried out at the Commission level will be notified to him as specified in Article 25 of the Regulation. IMI will be included in the DPO's register as well, per Article 26. Considering the role of the Commission in the data processing operations in this specific case, prior checking by the European Data Protection Supervisor is unlikely to be necessary (Article 27 of the Data Protection Regulation).

8. Transfer of personal data to third countries.

The IMI system is not designed to permit international transfer of data outside of the European Community; its purpose, as established in its mandate in Article 34 of the Services Directive is the exchange of information among Member States.

WP 29 wishes to emphasise that these data must not be transferred outside the IMI framework, given that transfers would inherently be beyond the scope of the initially established purpose for processing. Transmission of IMI data to third countries would therefore violate the use limitation laid out in the Article 6 1 b) of the Data Protection Directive.

9. Conclusions and recommendations of WP29.

1. The IMI system, must be designed in complete conformity with the principles established in applicable data protection laws, including the Data Protection Directive and the Data Protection Regulation. The principles of data protection must properly be implemented within the system if IMI is to realise its potential to improve the protection of the fundamental right to personal data protection.

2. To this end, the WP 29 wishes to emphasise the importance of compliance with the data protection requirements concerning data quality, necessity and proportionality. These should be considered at every phase of IMI development and by every actor in the system – in the drafting of standardised information requests, the selection of Competent Authorities, and so on. IMI should also be notified to, and prior checked by, the data protection authorities in Member States which require such procedures pursuant to Article 18 of the Data Protection Directive.

3. IMI is a complex system with the potential to simplify the process of information-sharing by providing additional tools to Member States. However, these changes must be accompanied by strict adherence to the principles established in the Data Protection Directive. IMI users must be particularly attentive to ensure compliance with national law and the Directive as their information transmission capabilities are enhanced with digitalised communication and document attachments. Furthermore, the supervisory role of national Data Protection Authorities and other controls in place in the various Member States must be maintained where required. The *sui generis* role of the European Commission must also be explicitly recognised in the IMI context, with the concomitant obligations of that role.

4. To better enable Competent Authorities to use IMI in a way that is consistent with data protection rules, it is necessary to clarify the precise roles played by all users in the system. IMI Coordinators and Linked Authorities must be better defined and their rights and responsibilities, including the specific information to which they will have access, must be made explicit. This will minimise unnecessary data processing, protecting the rights of citizens and CA personnel, while at the same time enhancing IMI's efficiency.

5. It is important to establish clearly the competences and duties between the Commission, Coordinators and Competent Authorities, given that their IMI roles are best described as a joint controllership.

6. As IMI is developed, there must be a careful reassessment of the potential applications of the system to convey sensitive data, even within the context of this first implementation concerning the Professional Qualifications and Services Directives. Such applications are not abstract probabilities; rather, they are actually enumerated (as in Article 56.2 of the Professional Qualifications Directive, which specifies that criminal record information may be transmitted through IMI). Because IMI will almost certainly be used to process data relating to health, criminal history or other protected information, the security and verification safeguards in place must also be rethought and improved.

7. It is of the utmost importance that every individual data processing action rest upon individual and legitimate legal grounds tailored to its specific purpose and objectives.

8. The need for a more concrete legal basis for each individual IMI transaction throws into sharp relief the need for explicit identification of the goals of data processing actions in the system. Only when a clear objective is specified can IMI actors be sure that they are complying with the principles of necessity, data quality and proportionality. Each of those criteria refers directly to the purpose of processing. Retention periods, too, are dependent upon a specific understanding of the action's

goal; it is impossible to know if the task has been completed if one is unsure of its desired result. In a network of data processing relationships as complex as IMI's, where it may be unclear as to who is playing which role, an explicit statement of data processing objectives is absolutely essential to enable informed behaviour under uncertain circumstances.

9. The IMI system can never be subservient to 27 different national regimes. For this reason, a more specific Commission decision is necessary; such a decision must be precise and should address the areas of concern discussed above.

Done at Brussels, on _____ 2007

For the Working Party

The Chairman
Peter Schaar