GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimenti a carattere generale - 23 novembre 2006

[doc. web n. 1427027]

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Guiding Principles Applying to the Processing of Employees' Personal Data for the Purpose of Managing Employment Relations in the Private Sector

1. Foreword

1.1 Purpose. In order to provide guidance and recommendations concerning the processing of personal data (including sensitive data) of employees in the private sector, the Garante has considered it appropriate to adopt these guiding principles and review them regularly by also taking account of the decisions issued by the Authority in this area.

The guidance below leaves unprejudiced the application of any laws and/or regulations setting out more stringent prohibitions and/or limitations in respect of certain sectors or specific data processing situations (see Sections 113, 114, and 184(3) of the Data Protection Code, DPC).

1.2. Scope. The scope includes mainly communication and dissemination of the data; the information notices to be provided by employers to employees (section 13 of the DPC); processing of data suitable for disclosing health; and access rights.

The processing operations at issue concern mostly:

- data identifying (past and current) employees; biometric data; pictures and sensitive data also related to third parties, in particular where they are suitable for disclosing religious beliefs or trade union membership; data suitable for disclosing health, which are contained as a rule in medical certifications and/or other documents submitted to justify leave of absence and/or be granted specific permits or benefits as possibly mentioned in collective labour agreements;
- information that is related more closely to work performance, such as the type of contract (time-limited or not, full- or part-time, etc.); job description and position; salary paid, also based on "ad personam" arrangements; benefits; time schedule, including overtime; vacations and time off (whether past or yet to be granted); leaves of absence as provided for by law and/or (collective) labour agreements; transfers to other offices; disciplinary measures and proceedings.

The data in question may be:

- contained in records and documents made available by employees either upon their recruitment (on this point, see previous guidance issued by the Garante as for the information gathered via classifieds) or during the employment relationship;
- contained in documents and/or files processed by (or on behalf of) the employer during the employment relationship to ensure contract performance, to be subsequently collected and kept in personal records and corporate filing systems whether automated or manual;
- made available via notice boards and/or corporate intranets.

2. Compliance with Personal Data Protection Principles

2.1. Lawfulness, Relevance, Transparency. The aforementioned personal information may be processed by an employer to the extent it is necessary in order to appropriately fulfil employment obligations; in some cases, the information may be also indispensable to comply with requirements set out in laws, regulations, contracts and collective agreements.

The information in question should be relevant and not excessive, and all the provisions contained in the legislation in force

on personal data protection, which is partly grounded on Community directives, will have to be complied with.

In particular, the DPC has implemented EC Directives 95/46 and 2002/58 and requires that personal data be processed:

- pursuant to the principles of data minimization and lawfulness, which concern data quality (Sections 3 and 11);
- by providing prior, adequate information to data subjects (Section 13);
- by applying for the employees' prior consent only where it is inappropriate, also in the light of the nature of the data, to use any of the other preconditions that are equated to consent (Sections 23, 24, 26, and 43 of the DPC);
- by complying with the requirements laid down by the Garante in the relevant authorisations, if sensitive or judicial data are to be processed (Sections 26 and 27 of the DPC; see, in particular, the general authorisation no. 1/2005);
- by taking suitable security measures to protect the data against events such as unauthorised access and/or misuse, for which an employer may also be held liable under both civil and criminal law (Sections 15, 31 et seq., 167, and 169 of the DPC).

2.2. Purposes. The processing of personal data (including sensitive data) related to individual employees is lawful if it is aimed at fulfilling obligations arising from the relevant employment contracts (e.g., in order to check that the performance requested was actually carried out; to perform payments also related to overtime and/or benefits; calculate vacation days and days off; to establish whether the employee's leave of absence was substantiated).

Some purposes are also laid down in collective agreements in that they relate to circumstances concerning the individual employment relationships (e.g. in order for an employee to be granted days off and/or leaves of absence in connection with trade union activities, or compensation time, or else in connection with the recruitment of employees entitled to specific contractual terms); in other cases, the purposes are laid down in a law (e.g. as regards disclosures to social security and pension funds).

Whilst the above purposes are lawful, generally speaking, it is necessary to comply with the principle whereby the purposes to be achieved should be compatible (Section 11(1), letter b) of the DPC). That is, the purpose to be achieved in concrete by an employer via the processing of personal data must not be incompatible with the purposes for which those data have been collected.

3. Data Controller and Data Processor

3.1. Data Controller and Data Processor. In connection with personal data protection, special importance should be attached to the identification of the entities that are entitled to process the data, by clearly setting out the respective powers; this applies, in particular, to both the data controller and the data processor (see Section 4(1), letters f) and g), and Sections 28-29 of the DPC).

In principle, to identify the data controller consideration should be given to the entity that is actually a party to an employer-employee relationship irrespective of the outward corporate structure.

However, the identification in question may turn out to be difficult in particular where the corporate structure is especially complex; this circumstance may actually also hinder exercise of the rights referred to in Section 7 of the DPC (see below on this point).

3.2. Corporate Groups. As a rule, the companies included in corporate groups as defined in the law (Section 2359 of the Civil Code, and legislative decree no. 74/2002) are separate, autonomous data controllers in respect of the processing of the personal data related to their employees and collaborators (Section 4(1), letter f), and Section 28 of the DPC).

However, subsidiaries and related companies may entrust the parent company in their group with the task of fulfilling legal obligations related to employment, social security and benefits as per the relevant laws. In this case, the parent company will have to be appointed as data processor pursuant to Section 29 of the DPC.

A similar arrangement will have to be made (in pursuance of Section 31(2) of legislative decree no. 276/2003) as for the processing of personal data carried out within the framework of consortia of co-operatives, whereby any of the cooperatives in the consortium may be appointed as data processor for the said purposes – on condition the processing operations they perform are identical.

3.3. "Competent Physician". Further considerations are required in connection with specific processing operations that may or must be carried out within a company in pursuance of the legislation on occupational safety and health (in particular, legislative decree no. 626/1994 as subsequently amended).

That legislation, which has also been enacted to transpose Community directives and is part of the broader set of measures aimed at safeguarding workers' bodily and mental integrity (Section 2087 of the Civil Code), requires the physician that is competent for occupational safety and health to carry out mandatory medical surveillance – including the related processing of the data contained in health care records, as per Sections 16 and 17 of legislative decree no. 626/1994.

In this context, the competent physician performs preventive, regular medical examinations on workers (Section 33 of Presidential decree no. 303/1956; Section 15 of legislative decree no. 626/1994) as well as creating and updating a health and risks record pursuant to specific legislation (Sections 17, 59-quinquiesdecies(2), letter b), 50-sexiesdecies, and 70 of legislative decree no. 626/1994).

The said record is kept at the company/production unit "without prejudice to professional secrecy, and [is delivered] in copy to the worker upon termination of the employment relationship, or else at the worker's request" (Section 4(8) of legislative decree no. 626/1994). Upon termination of the employment relationship, the original health record is sent to ISPESL (Central Agency for Occupational Prevention and Safety) in a closed envelope.

Based on the above provisions, the competent physician is in charge of processing employees' medical data, noting the relevant information in health records, and taking suitable security measures in order to ensure confidentiality of the information by having regard to the purposes and mechanisms of the processing operations in question. These obligations must be fulfilled irrespective of the specific data controller.

The employer is not entitled to access the aforementioned health records, whilst he is simply required to co-operate with a view to ensuring that they are kept securely at the company's premises also in view of possible inquiries carried out by the competent authorities/bodies – as said, this will have to be done "without prejudice to professional secrecy". (Failure to do so carries criminal punishments).

Whilst the employer is required to take preventive measures and/or safeguards in respect of his employees as based on the competent physician's opinion, or else if the latter informs him about abnormalities that can be accounted for by risk exposure, he is not allowed to become acquainted with information on possible diseases. The only piece of information that may be disclosed to the employer relates to the ultimate assessment as to whether a given employee is medically fit to discharge certain tasks/functions.

This is actually in line with the legislation requiring the health and risks record to be forwarded to ISPESL in case of either assignment or termination of an employment relationship; it is prohibited for an employer to get access to the records in question also in such cases.

4. Biometric Data and Access to "Restricted Areas"

4.1. Concept. The Garante has been receiving several requests concerning the possible use of biometric data at the workplace, also pursuant to the prior checking procedure (Section 17 of the DPC) – in particular with a view to regulating access to specific premises in a company.

These data are derived from an individual's physical or behavioural features on the basis of a specific procedure, which is partly automated and yields a (reference) template. The latter consists in a set of numerical values that are calculated via mathematical functions from the said individual features and are intended to allow personal identification by means of the appropriate comparison between the numerical (digital) code calculated every time access is attempted and the original code.

The blanket, unrestricted use of biometric data, in particular those resulting from fingerprints, is not permitted. On account of their nature, these data require special precautions to prevent harming data subjects – in particular because of unlawful conduct resulting into the unauthorised "reconstruction" of a fingerprint from the reference template, so as to subsequently use it unbeknownst to the data subjects.

Using biometric data may only be justified in specific cases by taking account of the relevant purposes and the context in which the data are to be processed; as regards the workplace, this is the case if access to "sensitive areas" is to be regulated by having regard to the activities performed within those areas – e.g. dangerous or high-security production processes, or else because certain premises are intended for the storage and preservation of secret or confidential goods or documents, or else valuables.

4.2. Biometric Systems. Additionally, whenever it is permitted to process biometric data, it is – as a rule – both disproportionate and unnecessary to centralise the personal information that is processed in connection with the biometric recognition procedure in the form of templates. Information systems must be configured in such a way as to minimise the use of personal data and rule out their processing if the purposes being sought can be achieved via mechanisms that only allow identifying data subjects in case this is necessary (Sections 3, 11 of the DPC).

Therefore, effective biometric verification and identification systems, rather than the centralised processing of biometric data, are to be regarded as both appropriate and sufficient, providing they are based on the reading of fingerprints stored as encrypted templates on media that are held exclusively by the relevant data subjects (e.g. smart cards or similar devices) and bear no identification data related to the latter – as it is enough to allocate a different numerical code to each employee.

This recognition mechanism is suitable for ensuring that access to a restricted area is only permitted to previously authorised individuals, who are free to decide whether to avail themselves of the said smart card and/or a similar device. Their fingerprints can be compared with the template(s) stored on the card and/or device by means of standard comparison procedures that are implemented directly on the card and/or device in question, whereby the creation of a database including sensitive biometric information can be avoided. Indeed, if the card and/or device is lost/mislaid, there are currently limited

risks that the biometric information they contain may be misused.

4.3. Security Measures and Retention Periods. The personal data that are required to generate a template may only be processed in the enrolment phase; the data controller must first obtain the data subjects' informed consent in order to use those data.

In addition to the minimum security measures laid down in the DPC, additional arrangements should be made in order to protect the data by giving ad-hoc written instructions to the persons in charge of processing – detailing, in particular, what to do in case the cards and/or devices committed to them are lost or stolen.

It must be possible for the staff in charge of checking compliance with security measures in the company to access the stored data, exclusively in order to verify the said compliance; in so doing, they will have to take account of the legislation applying to the distance surveillance of employees – see Section 4(2) of Act no. 300/1970, as referred to by Section 114 of the DPC.

Any data that is collected may not be stored for longer than seven days, as a rule; appropriate automated data erasure mechanisms will have to be implemented also in case the retention period may be lawfully extended.

4.4. Prior Checking. The need for data controllers to file an ad-hoc prior checking request with the Garante in pursuance of Section 17 of the DPC is hereby left unprejudiced as regards specific situations and/or exceptional cases that are not referred to herein, if the said data controllers' intention is to depart from the above guidance.

5. Communication and Dissemination of Personal Data

5.1. Communication. It is permitted to disclose the personal data concerning an employee to a third party with the said employee's consent.

Whenever it is inappropriate for the employer to avail himself of any of the legal preconditions for processing the data that are equated to consent (Section 24 of the DPC), it is not permitted to sidestep the consent requirement in order to communicate personal data (concerning, for instance, an employee's recruitment, status or position, or the imposition of disciplinary sanctions, or an employee's transfer) to third parties such as:

- employers' associations, including trade associations, or associations among former employees (including those from the same company);
- personal acquaintances, family members, relatives.

Subject to compliance with the general principles referred to above as for the processing of personal data (see point 2), the employer is further entitled to regulate the processing operations in question by appointing the external and/or internal entities that may access the data related to management of the employment relationship as either data processors or persons in charge of the processing; account will have to be taken in this regard both of the tasks discharged by the said entities and of appropriate written instructions the latter will have to abide by (see Section 4(1), letters g) and h), and Sections 29-30 of the DPC). Where necessary, ad-hoc documents will have to be made available and delivered to the entities in question.

Additionally, the employer is also empowered to communicate data derived from the information concerning individual employees and/or groups of employees to third parties, in truly anonymous format. This applies, for instance, to the information concerning total overtime and/or non-worked hours in respect of the company and/or individual production units, or to the amount of corporate performance-based bonuses as set out on a range basis or else with regard to the individual work positions/levels, possibly inside individual functions and/or units.

5.2. Corporate Intranet. By the same token, the employee's consent is necessary to publish personal information related to him/her (e.g. pictures, identification data, CVs) on the corporate Intranet – even more so if the data are to be posted on the Internet; such a wide-ranging dissemination of personal data is to be regarded as basically unnecessary "to fulfil obligations arising from the employment contract" (see Section 24(1), letter b), of the DPC). Indeed, those obligations may be fulfilled independently of this specific type of data dissemination; however, the latter may at times be relevant, in particular on account of the size and/or geographic penetration of a company, in which case the individual employee's prior consent must be obtained except as provided otherwise by the law.

5.3. Dissemination. Where it is not specifically provided by law that an employer is required and/or authorised to disseminate personal data related to his/her employees (Section 24(1), letter a) of the DPC), or none of the other legal preconditions set out in the DPC are met, dissemination of the data is only permitted if it is necessary to fulfil obligation arising from the employment contract (see Section 24(1), letter b) of the DPC). This is the case, for instance, with the posting on the corporate notice board of work instructions, shift schedules for workdays and holidays, or provisions on work organisation and the tasks committed to the individual employees.

Apart from the above cases, it is unlawful, as a rule, to disseminate personal information related to individual employees also by posting such information on corporate notice boards and/or publishing it in corporate communications intended for the staff as a whole – in particular if this is not done in connection with the fulfilment of employment obligations. The

dissemination of personal data in the said situations is also in breach of the lawfulness and relevance principles set out in Section 11 of the DPC, such as whenever information is posted on

- the salaries paid, possibly in connection with specific personal circumstances;
- the imposition of disciplinary sanctions and/or the existence of legal disputes;
- sick leaves;
- an employee's membership/enrolment in given associations.

5.4. Badges. Dissemination of personal data may also result from the inclusion of those data in personal badges pinned, for instance, on an employee's dress or uniform – which usually is done in order to improve customer relations.

In this connection, the Garante has already stressed that the obligation to wear a badge may be accounted for – as regards the private sector – by provisions contained in agreements between trade unions and a corporation, whereby compliance with those provisions can be equated to the fulfilment of obligations arising from the employment contract. Nevertheless, it has been found that it is disproportionate to include personally identifiable information in a badge - such as the employee's given name and family name or other identification data – since other types of information may well be considered sufficient in view of facilitating customer relations – e.g. identification codes, or the employee's first name or position.

5.5. Communication Mechanisms. Except where the mechanisms and arrangements for disclosing personal data are set out in specific provisions (see Section 174(2) of the DPC), the employer will have to communicate individually with each employee by taking such measures as are especially suitable to prevent the personal data – in particular, sensitive data – from being disclosed to entities other than the relevant recipients, irrespective of whether such entities are in charge of certain processing operations. The measures in question might consist, for instance, in using closed and/or stapled envelopes to send out correspondence; urging data subjects to personally collect the relevant documents from the competent office; or sending electronic communications to the employee's account.

Similar precautions will have to be taken – in the light of the specific circumstances – with regard to other communications addressed to employees, whenever they may disclose personal situations and/or circumstances.

6. Data Suitable for Disclosing Employees' Health

6.1. Medical Data. Special precautions will have to be taken also in processing sensitive data related to an employee (Section 4(1), letter d), of the DPC), in particular those suitable for disclosing their health. Such data may include the information related to sick leaves irrespective of whether the medical diagnosis is also mentioned.

Even apart from data protection provisions, there are special safeguards in place under the law to limit disclosure of this type of information to what is indispensable to an employer with a view to performance of the employment contract (see, in particular, Section 8 of Act no. 300/1970).

Given this context, the general requirements laid down in the DPC must be co-ordinated with and supplemented by other sector-related and/or special provisions (see point 3.3 above).

At all events, it is prohibited to disseminate medical data (see Section 26(5) of the DPC).

6.2. Sick Leaves. As regards specifically the processing of data suitable for disclosing employees' health, the relevant laws as well as the clauses contained in collective labour agreements justify processing of the data related to sickness (sometimes also to visits by medical specialists and/or medical examinations) where such sickness results into work impairment – whether temporary or not, with the resulting suspension/termination of the employment contract. By the same token, an employer may process data related to invalidity and/or the inclusion in disability and other socially disadvantaged groups in accordance with the mechanisms and purposes set out in the legislation in force.

There are indeed detailed regulatory provisions in this field, also envisaging communication obligations (vested in the employee) and certification obligations (vested in the employer and the social security body) as regards diseases and sickness. Fulfilling such obligations is meant not only to justify the allowances and benefits an employee may be entitled to, but also to allow an employer to check on the employee's actual health – in accordance with the law.

Ad-hoc forms are to be used in order to comply with the above requirements, consisting in a sickness certificate that must be delivered to the employer (it only refers to the start and (expected) end dates of the sick leave, i.e. the so-called "prognosis") plus a diagnosis certificate that each employee is required to deliver to INPS (National Social Security Agency), or the competent public body as specified by INPS pursuant to an agreement with the different Regions – if the employee is entitled to sickness allowance paid by the social security body.

However, even where an employee submits medical certificates drawn up on forms other than those referred to above, whereby the prognosis information is not reported separately from the diagnosis, the employer is required whenever feasible to take suitable measures and precautions so as to avoid receiving the information in question, or anyhow to blank that

information.

6.3. Reporting Information to INAIL (National Occupational Accident Insurance Agency). Conversely, in some cases an employer may be entitled to obtain information on an employee's health in order to fulfil communication obligations related to medical data.

This is most often the case in connection with the obligation to report occupational accidents and diseases affecting employees to the national occupational accident insurance agency (INAIL). The relevant legislation expressly requires such reports to be submitted jointly with specific medical certificates (Sections 13 and 53 of Presidential decree no. 1124/1965).

Although an employer is lawfully entitled to be informed about the medical diagnosis in such cases, he/she is nevertheless obliged to only communicate the medical information related to and/or connected with the reported event – which does not include any medical data concerning other sick leaves granted in the past to the given employee. If this information were communicated, it would be excessive and irrelevant and therefore could not be used – exactly on account of its being irrelevant to the case being reported (see Section 11 (1) and (2) of the DPC).

6.4. Other Medical Information. Reference should also be made to other cases in which it is permitted to process data related to an employee's health (including his/her relatives), also in order to grant the benefits and allowances provided for in the law (e.g. prolonged leave of absence with security of employment). This is the case, for instance, with the information related to disability.

An employer is also entitled to obtain information on an employee's drug addiction, where the latter employee applies for admission to rehabilitation and/or treatment programmes with security of employment (without pay), as specific medical records must be submitted to the employer in compliance with collective labour agreements as well as with Section 124(1) and (2) of Presidential decree no. 309/1990.

6.5. Communications to INPS. Additionally, data suitable for disclosing employees' health may be lawfully communicated by an employer to public bodies (social security bodies) in charge of paying the required allowances pursuant to specific obligations arising from laws, regulations and/or contractual clauses, whereby only indispensable information may be communicated.

In particular, an employer may provide INPS (National Social Security Agency) with the data concerning employees absent from work, even for just one day, in order to have checks carried out on their health (Section 5(1) and (2) of Act no. 300/1970). To that end, employers must hold and produce, at the request of INPS, such documents and records as they are in possession of. Any controls on an employee's health as per Section 5 of Act no. 300/1970 may be carried out – at the request of either INPS or the competent public health care body specified by INPS – by physicians working for the health care systems specified by the individual Regions (pursuant to Section 2 of Act no. 33/1980).

7. Information Notices

Employers are required to provide their employees with individual information notices including all the items specified in Section 13 of the DPC prior to processing personal data concerning such employees – as also related to the cases in which the employees' consent is not necessary under the law.

As regards, in particular, those companies/entities where employees may find it difficult to exercise their rights pursuant to Section 7 of the DPC – either because of organisational reasons (e.g. highly fragmented geographical distribution of production units, substantial use of outsourcing mechanisms) or because of the sheer size of the company – it is appropriate to appoint a data processor specifically in charge of handling these issues. Alternatively, external data processors may be appointed and entrusted with the task of managing, for instance, the administrative files concerning human resources. At all events, the relevant information will have to be spelled out in the information notices.

8. Security Measures

8.1. Medical Data. The employer, acting in his capacity as data controller, is required to take such security measures – including minimum security measures – as are set out in the DPC to protect employees' personal data, irrespective of how these data are processed within the framework of the employment relationship; in so doing, special attention will have to be paid to the sensitive nature of any data in question (see Section 31 et seq. and Annex B to the Code).

The data at issue must be kept separate from any other personal data concerning data subjects. This also applies to the employees' personal records kept on paper; for instance, ad hoc sections might be created and used specifically for the preservation of sensitive data, including those suitable for disclosing the employee's health – which must be kept separate and/or in such a way as not to let them be accessed unrestrictedly in the course of standard administrative activities.

Similarly, if an employee submits a medical certificate that is drafted on a different form from the one described under 6.2., an employer may not use the relevant information for further purposes (see Section 11(2) of the DPC) and must make

appropriate arrangements to prevent the diagnostic information contained in the certificate from being visible (e.g. by requiring the certificates to be sent in a closed envelope after blanking the information in question). This is aimed at preventing the data from being accessed without authorisation by entities that have not been appointed as data processors and/or persons in charge of the processing (see Section 31 et seq. of the DPC).

8.2. Persons in charge of the processing. The above considerations leave unprejudiced the employer's obligation to appoint staff specifically in charge of processing the employees' personal data. Such staff "need to know about data protection and receive proper training. Without an adequate training of the staff handling personal data, there could never be appropriate respect for the privacy of workers in the workplace." (See Opinion no. 8/2001 by the Article 29 Working Party).

8.3. Physical and Organisational Measures. An employer is required to take, inter alia (see Section 31 et seq. of the DPC), such physical and organisational measures as can ensure that:

- the places where employees' personal data are processed are protected as appropriate against unauthorised intrusions;
- personal communications that are related exclusively to individual employees are performed in such a manner as to prevent them from becoming known to third parties and/or entities that have not been appointed as persons in charge of the processing;
- unambiguous instructions are given to the persons in charge of the processing as to the need for complying with official secrecy requirements, also with regard to employees that are not entitled to get access to specific personal information;
- personal data that are processed electronically may not be acquired and reproduced in the absence of suitable authentication and/or authorisation systems, and documents containing personal information may not be acquired and reproduced by unauthorised entities;
- the involuntary acquisition of personal information by third parties or other employees is prevented; for instance, the appropriate arrangements will have to be made depending on the configuration and/or location of the work premises, in the absence of suitable arrangements to prevent dissemination of the information (e.g. if the requirement to wait behind a line is not provided for, or confidential information happens to be handled in public areas rather than in private offices).

9. Exercising the Rights Set out in Section 7 of the DPC – Replies Provided by the Employer

9.1. Access Rights. Any employee may apply to his employer in order to exercise the rights set out in Section 7 of the DPC, in accordance with the mechanisms specified in Section 8 et seq. of the DPC – including the right to access the data concerning them (as opposed to the right to access the documents where those data are contained), have the data updated, rectified, supplemented, erased, anonymised or blocked (if the data are processed against the law), and object to the processing on legitimate grounds.

Where the access request does not refer to a specific processing operation and/or specific data and/or data categories, it will have to be considered to refer to all the personal data concerning an employee irrespective of how and why they are processed by the employer (Section 10) – including evaluation data in accordance with the conditions and limitations set out in Section 8(5) of the DPC.

The data in question do not include, however, information of a contractual or professional nature that is not personal information as it cannot be related in whatever manner to identified or identifiable individuals.

9.2. Replies by the Employer. Any employer receiving an access request is required to reply in full to the individual employee – that is, rather than simply listing the categories of data in his possession, he will have to provide unambiguous, understandable information on all the data in question.

9.3. Timeliness of Replies. Replies will have to be provided by 15 days as from receiving the data subjects' access requests – which must be lodged in compliance with the relevant requirements. A longer term (i.e. 30 days) only applies if the operations required to comply in full with an access request are especially complex, or else on account of other justified reasons (see Section 146 of the DPC), provided that the data subject is informed thereof.

Therefore, suitable organisational procedures will have to be i by an employer – especially in a large-sized company and/or entity – in order to fully comply with the provisions set out in the DPC as to data access and the exercise of all other rights. To that end, ad-hoc software may also be deployed in order to accurately retrieve the data related to individual employees as well as to simplify and expedite the reply mechanisms.

9.4. Reply Mechanisms. Replies may also be provided verbally; however, if so requested, the employer will have to report the information on paper and/or computerised media, or else to send it to the relevant data subject via electronic networks (see Section 10).

Based on the provisions set out in Section 10(1) of the DPC, whereby the data controller must take suitable measures "to simplify and expedite reply mechanisms", one may argue that a data subject may lawfully request that the data at issue

should be communicated to him/her at his/her home or work premises.

9.5. Personal Data and Documents. The Garante has clarified repeatedly that the access right only allows obtaining communication of the personal data related to the applicant insofar as such data are held by the data controller (see Section 10 of the DPC) and can be extracted from records and documents. Conversely, it does not entail the right to request direct, unrestricted access to documents and whole categories of record; the creation of documents that do not exist as such in an archive or data filing system; the aggregation of such documents in accordance with specific mechanisms as suggested by the data subject; the provision – in all cases – of copies of the documents held by the data controller; or that the data controller should reply in a specific manner (except for the requirement that the data be reported on paper media pursuant to Section 10(2) of the DPC).

Access may also be granted – especially if the data controller holds a considerable amount of personal information – by making available the relevant personal file or folder to the data subject, who will subsequently extract the personal information at issue.
The data controller may decide to produce or provide a copy of records and documents containing the requested personal data exclusively if extracting the data from those records and documents proves especially difficult; any personal data related to third parties will have to be taken out (see Section 10(4) of the DPC). If the data controller decides to reply in this manner to an access request, he is not required to provide copies of all the various documents (e.g. letters, instruments, notes) containing the same personal data related to the data subject.

When replying to an access request lodged pursuant to Sections 7 and 8 of the DPC, the data controller is required to communicate the requested data insofar as they are actually held by him – that is, he is not required to retrieve and/or collect other data that are not in his possession and are not processed by him in whatever manner at that time either because they had been processed at an earlier stage and are no longer available, or because the data have never been actually at the data controller's disposal. This might be the case with data contained in the correspondence exchanged, in whatever manner, between employees of a given employer. Apart from the need to take account of the secrecy of correspondence principle, the employer would not be actually empowered to decide on purposes and mechanisms of the processing of such personal data in the case at issue (see Section 4(1), letter f), of the DPC).

9.6. Updating. Finally, an employee has the right to have the personal data relating to him updated.

As for the request to rectify the personal data contained in an employee's professional profile, this is only permitted if the employee can provide proof that the claimed personal qualifications are actually and lawfully held by him – for instance on the basis of decisions and/or documents issued by the employer and/or third parties, obligations arising from the employment contract, measures issued by judicial authorities with regard to the data subject, and/or any other instruments or documents providing suitable proof of the data subject's claim for the purpose of applying the legislation on personal data protection. At all events, an employee may raise his claim for recognition of the specific qualifications and/or skills before other entities by producing the appropriate evidentiary records.