BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

EU Data Protection

Employee Information

Guidelines recently released by the Italian Data Protection Authority for the first time provide—within a global and coordinated framework—rules and guarantees aimed at regulating the gathering and the processing of personal data within the workplace and, the author says, can also be interpreted as a practical set of rules executing related provisions of the Italian Code on privacy.

Italy: Recent Developments in Data Protection—Guidelines on the Processing of Employee Personal Data by Employers Within the Private Sector

By Avv. Alessandro del Ninno

On December 13, 2006, the Italian Data Protection Authority (hereinafter the *Garante*) made public the guidelines on the processing of employees' personal data for labor relationship management purposes by employers within the private sector (the guidelines). For the first time, the Italian *Garante* has defined—within a global and coordinated framework—rules and guarantees aimed at regulating the gathering and the processing of personal data within the workplace. The guidelines can also be interpreted as a practical set of rules executing the general principles contained—on this specific subject matter—in the related provisions of the Italian Code on privacy (legislative decree of June 30, 2003 no. 196).

By Avv. Alessandro del Ninno, Information & Communication Technology Department, Studio Legale Tonucci & Partners, Rome. The author may be contacted at adelninno@tonucci.it.

It is worth noting that March 1 the Italian *Garante* issued a separate set of guidelines concerning the processing of the employees' personal data within their use of e-mail and Internet connections from the workplace. The guidelines also set out principles and rules applicable to employers and employees within the private sector. With regard to the public sector the rules are dif-

 ISSN 1538-3423

ferent, and, in any case, these guidelines are focused on private employers and employees.

§ 1. Processing Employee Personal Data: The General Scopes Considered by The Guidelines.

The principal issues taken into consideration by the guidelines mainly refer to the following aspects of the processing of employee personal data:

a. employee personal and generic data (without regard to whether the employee is not working any more), biometric data, pictures and sensitive data (also when referring to third parties) with particular regard to data allowing the disclosure of religious beliefs or memberships to trade unions;

b. employee personal data disclosing health (usually contained in medical certificates, or in other documents delivered by the employee to the employer for justifying absences from work or to get permits and benefits provided by the laws or by collective agreements);

c. information more closely related to the carrying out of the work activities, for example: information related to the kind of contract (whether temporary or permanent, full time or part-time, etc.), information relating to the employee's professional level or title, to his salary (even when calculated *ad personam* [as part of a group rather than by individual]), to prizes awarded, to overtime, to holidays, to individual permits (whether used or not), and information relating to absences from work, transferrals to other workplaces, disciplinary measures or proceedings involving the employee.

The above are considered personal data under the guidelines, when they are:

a. contained in acts and documents delivered by the employees during the hiring process (note that the *Garante* in the past enacted several specific acts regulating the processing of personal data within pre-employment background screening procedures);

b. contained in documents and/or *files* accessed by (or on behalf of) the employer during the work relationship, for the purposes of executing the work contract, and successively gathering, and storing in personal files, papers or on the company's databases;

c. made available in the company's registers, notice boards or *intranets*.

§ 2. The Data Controller and The Data Processor of The Employees' Personal Data.

Having considered the general *privacy* principles applicable to the processing of employees' personal data, personal data undergoing processing must be processed lawfully and fairly. In order to ensure compliance, the data must be:

- collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes;
- accurate and, when necessary, kept up to date;
- relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed;
- kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data is collected or subsequently processed.

The guidelines clarify the rules aimed at identifying the various different persons who are allowed to process personal data. In particular, the guidelines provide the criteria to identify the ''data controller'' and the ''data processor.'' With regard to the ''data controller'' (which the Italian Code on privacy defines as ''*any natural or legal person, public administration, body, association or other entity that is competent, also jointly with another data controller, to determine purposes and methods of the processing of personal data and the relevant means, including security matters*'') what is important is the effective source/center of the working relationship, regardless of the company structure adopted. For example, when the personal data are processed within groups of companies, each of the companies has to be considered as a ''data controller'' with regard to the processing of personal data referring to their employees. Nevertheless, within groups of companies, the subsidiaries or controlled companies may delegate some of the privacy requirements, with the consequence that holding such data will make the organization to whom it is delegated, the ''data processor'' of the employees' personal information, which has been provided by the subsidiaries or parent company. It must be pointed out that according to the Italian Code on privacy, the ''data processor'' is ''*any natural or legal person, public administration, body, association or other agency that processes personal data on the controller's behalf*.''

Further:

a. the data processor may be designated by the data controller on an optional basis;

b. where designated, the data processor shall be selected from employees who can appropriately ensure, on account of their experience, capabilities and reliability, thorough compliance with the provisions in force applying to processing as also related to security matters;

c. if necessary, on account of organisational requirements, several entities may be designated as data processors also by sub-dividing the relevant tasks;

d. the tasks committed to the data processor shall be detailed in writing by the data controller;

e. the data processor shall abide by the instructions given by the data controller in carrying out the processing. The data controller shall supervise over thorough compliance with both said instructions, also by means of regular controls.

§ 3. Specific Aspects of Data Processing Within The Italian Decree Concerning The Improvement of Occupational Safety and Health in All Workplaces.

The Italian legislative decree of September 19, 1994 no. 626 (implementing a set of European Union direc-

  PVLR ISSN 1538-3423

tives on safety and hygiene in the workplace) specifically provides for the processing of the employees' health data. In particular, this sets out that specific ''sanitary surveillance'' on the employees must be carried out. Article 16 of the Legislative Decree 626/94 states that ''sanitary surveillance'' includes preventive controls (clinical, biological examinations and instrumental surveys) carried out in order to ascertain the health conditions of workers, with respect to the risks they may incur. The task of undertaking sanitary surveillance, according to the current provisions, should be assigned to a medicine graduate specialized in preventive medicine of workers and in industrial psychology, industrial toxicology or an equivalent specialisation.

Article 17 of the same legislative decree vests physicians with certain specific functions:

a. carrying out an updated risk health record for every worker submitted to sanitary surveillance, which is to be stored by the employer, with the obligation of professional secrecy;

b. carrying out medical examinations requested by the worker (besides those laid down by article 16) in case such request is linked to professional risks;

c. cooperating with the employer and with the prevention and protection services, to develop, and carry out measures to protect the psychological and physical health of employees;

d. cooperating with the training and information activities of the workers;

e. visiting the workplace at least twice a year and participating in planning the controls of the workers contact with particular agents, whose results must be communicated timely in order to take the proper measures;

f. cooperating with the worker to set up a first-aid service;

g. informing the workers about the sanitary controls they underwent, and in case of contact with agents having long-term effects, about the need to carry out controls even when they stop doing the work which entailed the contact with such agents;

h. informing those employees of the results, for those who want to know about their sanitary controls, and upon request giving them a copy of the relevant documents;

i. communicating with the representatives in charge of the safety, the anonymous collective results of the clinical and instrumental controls which were carried out, as well as explaining their meaning.

In light of the above, the guidelines clarify that the ''privacy role'' of the physicians is that of an autonomous ''data controller'' of the employees' personal information, processed according to the mandatory tasks provided by the legislative decree 626/1994.

§ 4. Biometric Data and Access to "Restricted Areas"

The processing of employees' biometric data has become increasingly common, *i.e.*, personal information relating to physical features—such as the data subject's fingerprints—of individuals that are to be identified uniquely by means of a reference template. The latter consists in a set of digital values that are derived mathematically from the individual features referred to above and are intended to allow identification of an individual via the comparison between the numerical code derived at each access and the initial template.

Fingerprints

Fingerprints are personal data insofar as they can be related to individual employees. Regardless of the fact that only part of them are collected and that they are only used to complete the enrolment phase—as well as the numerical codes subsequently used for comparison purposes. Hence, the provisions laid down in the Italian Code on privacy apply both to the enrolment phase and to any comparison/matching carried out thereafter, including the creation of files relating to an employees' achievements.

The guidelines specify that general and uncontrolled processing of employees' biometric data (especially in relation to fingerprints) is not lawful. Using such data in the workplace may be justified in specific cases, in relation to the purposes and context of their processing—*e.g.*, in connection with accessing certain premises in a company that require especially stringent security measures, either because of specific circumstances, or on account of the activities performed in those areas. Alternatively, their use may be justified in order to ensure security for the processing of the personal data.

In addition to this, the processing at issue could also be regarded as disproportionate, in the light of the envisaged technical arrangements—*i.e.*, the centralized storage of the identification codes derived from the analysis of biometric data. From this perspective, less invasive technological approaches can undoubtedly be implemented. Bearing in mind the principles set out in Section 3 of the Data Protection Code (''*Information systems and software shall be configured to minimise the use of personal data and identification data. In such a way as to rule out their processing if the purposes sought in the individual cases can be achieved either by using data anonymously, or suitable arrangements to allow identifying data subjects only in cases of necessity*.'') One could argue that—providing the use of biometric information is permitted—it is preferable to store the identification code on a medium that is in the data subject's exclusive possession (*i.e.*, a smart card or similar devices) after completing the enrolment phase, rather than recording the codes at centralised level in the company's information system. The latter approach may actually be more prejudicial to individual rights, if the security measures are breached, unauthorized entities access the data, or the stored information is misused—whether or not by third parties.

Furthermore, the guidelines incorporate the following rules on the processing of employees' biometric data:

a. the data necessary to set up the reference template can be processed exclusively during the enrollment phase; the processing must be based on prior and express consent given by the data subject;

b. in addition to the minimum security measures provided by the Italian Code on privacy, additional measures and guarantees for the data must be adopted;

c. the individuals in charge of the processing must be instructed by means of specific and written guidelines;

d. biometric data—where the processing is allowed—can be stored for a maximum period of seven days, unless exceptional needs are proved. After such a term has elapsed the data must be erased (even by means of automatic erasure);

e. a preliminary verification on an employers system using biometric data (for example systems or devices for the company security or for the employees' access monitoring by electronic badge) must be requested from the *Garante* if such systems or devices do not comply with the above rules.

§ 5. Communication and Dissemination of Employee Personal Data.

The guidelines point out important rules on the communication and dissemination of employee personal data. It is worth mentioning that according to the Italian Code on privacy:

a. "*communication*" shall mean disclosing personal data to one or more entities other than the data subject, the data controller's representative in the State's territory, the data processor and persons in charge of the processing in any form whatsoever (this includes by making available or interrogating such data).

b. "*dissemination*" shall mean disclosing personal data to unidentified entities, in any form whatsoever, including by making available or interrogating such data.

In general, disclosing an employees' personal data to third parties (like employers' associations, trade-unions, parents and relatives, and so on) is allowed where this is based on the data subject's prior consent. Nevertheless, the employer may bypass the mandatory requirement of consent under the following circumstances, if the processing:

a. is necessary to comply with an obligation imposed by a law, regulations or Community legislation;

b. is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or else in order to comply with specific requests made by the data subject prior to entering into a contract;

c. concerns data taken from public registers, lists, documents or records that are publicly available, without prejudice to the limitations set down by law, regulations and community legislation with regard to their disclosure and publicity;

d. concerns data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy;

e. is necessary to safeguard the life or bodily integrity of a third party;

f. is necessary for carrying out the investigations by a defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes, and for no longer than is necessary. Thereby complying with the legislation in force concerning business and industrial secrecy, and with the dissemination of the data being ruled out;

g. is necessary to pursue the legitimate interests of either the data controller or a third party recipient in the cases specified by the *Garante,* and on the basis of the principles set out under the law. This shall also apply with regard to the activities of banking groups and subsidiaries, or related companies. Unless said interest is overridden by: the data subject's rights and fundamental freedoms, dignity or legitimate interests, or if the dissemination of the data is ruled out;

h. Where external communication and dissemination, is carried out by not-for-profit associations, bodies or organisations (whether recognised or not), with regard either to entities having regular contacts with them or to members in order to achieve specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements, whereby the mechanisms of utilisation are laid down expressly in a resolution that is notified to data subjects with the information notice;

i. it is necessary for exclusively scientific and statistical purposes in compliance with the respective codes of professional practice, or else exclusively for historical purposes in connection with private archives that have been declared to be of considerable historical interest.

Save for the above, employers are also free to communicate data to third parties when such information are processed anonymously or in aggregate ways (for example: comprehensive number of overtime hours worked, comprehensive economic prizes assigned, etc).

Company's Intranet.

The prior consent of employees is mandatory when the employer wants to make public within the company his/her information (for example: picture, general data, CV's) by means of the intranet (obviously the same consent is required for the publication on the Internet).

Dissemination of employees' data.

Where employers are not allowed to disseminate their employees' personal data [through lack of the requirements listed above (a) to (i) or the prior consent], such dissemination is legitimate only when it is necessary for the performance of obligations resulting from the work contract (for example: publication in the company's notice boards of service orders, work shifts, holidays periods, other internal provisions related to the organisation of the work). In other cases, the dissemination of the employees' personal data (even by means of company's notice boards or by means of other internal communications addressed to all the employees) is disproportionate and unlawful, especially when such dissemination is not linked to the execution of work duties. For example, the dissemination is illicit in relation to the following cases:

a. dissemination/publication of salaries, wages or other emoluments referring to personal conditions of the employee;

  PVLR ISSN 1538-3423

b. sanctions applied to the employee within disciplinary proceedings;

c. information relating to legal actions regarding the employee;

d. absence from work due to illness;

e. employee membership of associations.

Cards/labels identifying the employees.

The guidelines provide a set of rules about the employees' personal data displayed on identifying cards or labels pinned on their clothing and on work uniforms. Such cards or labels usually aim to improve the relationships between operators and the public. In this regard, the guidelines point out that the obligation to exhibit identifying labels or cards may be founded on the work contract. Nevertheless, with regard to the relationships with the public, it may be disproportionate displaying detailed personal particulars such as; name, surname, date/ place of birth, and photo's on such cards. It is sufficient – in light of their requirement to assist the public, to only display certain information on the ID cards, such as: identifying codes, the sole name of the employee (without indication of the surname), the individual's role, etc. . .

Methods for communicating personal data.

Save for what is specifically provided by the law, employers must adopt individual forms of communication with the employees, avoiding unlawful communication of personal data (especially when sensitive) to third parties (including to the individuals in charge of the processing within the company), and to anyone other than the interested employee. The guidelines consider the following to be correct forms of communication:

a. addressing communications in closed envelopes;

b. inviting the interested employees to directly collect the communication from the relevant office;

c. sending individual electronic communications to the relevant employee.

§ 6. Processing Employees' Health Data. The Security Measures.

Specific guarantees must be adopted by the employers in relation to the processing of health data (for example: medical information justifying the employee's absence from work). To this regard, the first mandatory rule is the following:

When the employee delivers to the competent office the medical certification to justify the absence from work, such certificate cannot include the specific diagnosis and may display only the prognosis. Should the employee deliver a medical certification including also the diagnosis, the employer shall have to delete from it the related information.

The second rule is the general prohibition of disseminating the employees' health data.

According to: the Code on privacy, to the collective agreements and to the sectorial laws regulating the labour relationships, employers are allowed to process the following:

a. data relating to employees' illnesses (including information on specialised medical examinations or on clinical checks) when related to the temporary or permanent inability of an employee to work and when necessary for the employers to verify the declared illness;

b. data relating to disabled employees for the fulfilment of legal duties in relation to the so called *''protected categories'';*

c. data and documents relating to accidents at work or to illnesses, to be communicated to the public insurance body;

d. health data in general (including the employees' family data) when necessary to allow the employee to apply for particular benefits provided by the law (for example: permits, extended leaves, etc);

e. data relating to drug addiction, when an employee asks to be admitted to particular therapeutic or recovery programs provided by the law;

f. health data to be communicated by the employer to the competent public social security and insurance bodies.

With regard to the mandatory security measures in the processing of the employees' health data, employers must undertake to do the following:

a. ensure that data disclosing health and sex life are processed (both electronically or not) separately from the other personal data allowing employees to be identified directly. *E.g.*, a specific and not generally accessible envelope containing said data must be contained in an employees personal file;

b. adopt measures to avoid abusive access to the employees' data, including the implementation of proper measures aimed at preventing illicit intrusions in the work premises or the illicit gathering of data by other employees;

c. organise training activities for persons in charge of the processing with a view to informing them: of the risks applying to the data, the measures that are available to prevent harmful events, the most important features of personal data protection legislation in connection with the relevant activities, the potential issue of liability and the arrangements to get updated information on the minimum security measures adopted by the data controller;

d. adopt measures in order to ensure data integrity and availability as well as protection of areas and premises, insofar as they are relevant for the purpose of keeping and accessing such data.

§ 7. Privacy rights of the employees.

The first guideline states that employers must provide proper information to employees before commencing the processing of their data. Art. 13 of the Italian Code on privacy provides:

- That the data subject as well as any entity from whom personal data are collected, shall be informed, either verbally or in writing, and even in the cases where the data subject's consent is not mandatory, the purposes and methods used in the processing for which the data are intended.

- The obligatory or voluntary nature of providing the requested data; the consequences if (s)he fails to reply.
- The entities or categories of entity to whom, or which the data may be communicated, or who/which may get to access the data in their capacity as data processors, or persons in charge of the processing, and the scope of dissemination of said data; the privacy rights.

Secondly, employees may exercise the following rights:

a. right of access to the data and to obtain confirmation as to whether or not personal data concerning them exist, regardless of whether such data has been recorded in an intelligible form

b. the right to obtain update, rectifiy or, where interested therein, integration of the data;

c. the right to obtain erasure, anonymisation or blocking of data that have been processed unlawfully. Including data for which retention is unnecessary for the purposes for which they have been collected or subsequently processed;

d. the right to object, in whole or in part, on legitimate grounds, to the processing of personal data concerning him/her, even though they are relevant to the purpose of the collection.

The response provided by employers to the data subject shall include all the personal data concerning him/her that have been processed. Unless the request concerns either a specific processing operation – or specific personal data – or categories of personal data.

Employees' exercise of the above rights may be also permitted with regard to data of non-objective character on condition that it does not concern rectification of, or additions to, personal evaluation data in connection with judgments, opinions and other types of subjective assessment, or the specification of policies to be implemented, or decision-making activities by the data controller.

With a view to effectively exercising the employees' rights, employers shall take suitable measures in order to;

- facilitate access to personal data by the data subjects, even by means of ad hoc software allowing accurate retrieval of the data relating to the individual identified or identifiable data subjects;
- simplify the arrangements and reduce the delay for the responses, also with regard to public relations departments or offices.

Employers must provide employees with complete answers, without limiting the response to the sole list of the categories of information hold. Employers must answer within 15 days from the receipt of the employees request (the term is 30 days in cases of particular difficulty in collecting the requested data).

The data may also be communicated to the requesting party verbally, or else displayed by electronic means – on condition that the data are easily intelligible in such cases (in the light of the nature and amount of the information). The data shall be reproduced on paper or magnetic media, or else transmitted via electronic networks, whenever this is requested.

It must be specified that the employees' right of access regards the data as a such and not the documents. Accordingly, an employee cannot request the delivery of documents, or categories of acts held by the employer. Nor can it be used for the creation of documents not stored in the company's databases or for different aggregation of existing documents. In any case, if the data retrieval is especially difficult, the response to the employee request may also consist of producing or delivering copies of records and documents, which contain the personal data in question.

  PVLR ISSN 1538-3423