GUIDE

Data Protection in Labour Relations

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CONTENTS

GUIDE
Data Protection in Labour Relations

PAGE

Introduction

The Spanish Data Protection Agency has published various guides with the aim of promoting the application of Organic Law 15/1999 of 13 December on the Protection of Personal Data (LOPD) and Royal Decree 1720/2007 of 21 December, which approves the Implementing Regulation of Organic Law 15/1999 of 13 December on the Protection of Personal Data.

One of the main objectives of these publications is to offer tools to help public and private organisations to comply with the prevailing legislation. These guides have been designed to tackle general issues, such as the Guide for Data Controllers, or specific issues, such as the Guide to Data Security or the Guide on Video Surveillance.

The Guide to Data Protection in Labour Relations offers a new approach. It examines aspects of data protection that are either fundamental from the perspective of regulatory application and compliance, or which have posed difficulties in their interpretation or practical application. Unlike previous publications, the Guide to Data Protection in Labour Relations therefore aims to consider a number of the practical aspects that companies are typically faced with.

On the other hand, practically ten years after the LOPD came into effect, and with a widely publicised implementing regulation, businesses and administrations must begin to acquire the maturity needed to enable adequate compliance with the law. At present it is not a question of adapting structures to a new law, but of incorporating data protection into company culture and the design, organisation and operation of organisations. In this task, small and medium-sized companies have needed to have practical information available to them, a need that we particularly wish to address.

Since its creation, the Spanish Data Protection Agency has amassed a great deal of experience, which expressed in the various sections of this Guide can be used to provide guidance in the area of regulatory compliance.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Personnel Management

■ CASES OF NON-APPLICATION OF THE LOPD

One of the new features included in the Implementing Regulation of Organic Law on the Protection of Personal Data is the exclusion, under certain conditions, of its application to data defined as "personal contact data".

"This Regulation shall not apply to data processing regarding legal entities, nor to the filing systems that only include data on individuals providing their services in them, comprising only their names and surname(s), functions or jobs performed, as well as the postal or e-mail address and professional telephone and fax numbers" (Article 2.2, RDLOPD).

Under no circumstances shall this exclusion entail the non-application of the LOPD to personnel filing systems. The Regulation sets out one exception to the application of the laws guaranteeing the right to data protection, and must therefore be interpreted in a strict sense and a restrictive fashion. To do this, various requirements must be met:

- The data processed is effectively limited to the data that is necessary to identify an individual within the legal entity to which that person provides services. Any processing that contains data in addition to the data mentioned shall be fully subject to the LOPD.

  "As such, filing systems that include the data subject's national identity card data, for example, would not be excluded from the Law, since this data is not necessary for the maintenance of the business contact. Similarly and for obvious reasons, it shall never be considered that a company's filing systems for its own personnel are excluded from the Organic Law, when it is held not only for contact purposes, but for exercising the organisational and management powers accorded to the company by law" (Report 78/2008).

- The purpose of the data processing must pursue a direct relationship between the data processor and the entity, and not between the former and somebody holding a specific position within the company. As such, the use of the data should be supervised by the legal entity, with the subject's data being solely the medium by which this purpose is achieved.

  "This would occur in the event that processing takes the form of "business-to-business" relations, so that communications addressed to the company simply include the name of the person as a means of graphically representing the recipient of the communication" (Report 78/2008).

- The foregoing does not affect the provisions of the Law on Information Society Services and E-Commerce (LSSIyCE) so that the principles governing the electronic sending of commercial communications apply both to individuals and legal entities, including contact persons.

REGISTRATION OF FILING SYSTEMS

The concepts of "filing systems" and "database" are colloquially identified with existing programs that provide this type of service. However, the legal definition is much broader and goes beyond this type of software. As such, the application of the LOPD is not aimed at any specific computer program.

"k. Filing system: Any structured set of personal data which is accessible according to specific criteria, whatever the form or method of its creation, storage, organisation and access" (Article 5, RDLOPD).

In order to process a filing system subject to the LOPD, access to data should be enabled "according to specific criteria". As such, it must have criteria for sorting the data enabling data to be retrieved for a specific individual.

E.g. Name and surname, invoice number, customer code, date, address, telephone number, etc.

The filing system concept not only applies to computer programs. The LOPD applies to personal data stored on non-computer media where the data may be subject to processing.

"Non-automated filing system: any set of personal data organised in a non-automated and structured manner according to specific criteria regarding natural persons, that allows access without disproportionate effort to personal data, whether it is centralised, localised or distributed by function or geographically" (Article 5.1.n), RDLOPD).

E.g. Filing systems organised in paper format such as clinical records, curricula vitae, invoices. Analogue audio and video recordings from video-surveillance systems. Photographic negatives.

The determining factor when it comes to identifying a non-automated file system or processing method subject to data-protection legislation is the fact that it holds structured information from which it is possible to recover records relating to a specific individual.

"to receive this consideration, data files require a structure or organisation according to specific criteria. The mere accumulation of data without any criteria shall not be deemed as a filing system in the eyes of the law.

(…)

It is clear to this Court that records on a physical support are equivalent to a filing system under the provisions of the law. This conclusion can be adequately reached by reading Article 2 in full and comparing it with Article 3 of the Directive on which it is predicated and which may be used to interpret it.

Therefore, for a manual action regarding personal data (collection, recording, keeping, preparation, modification, blocking, etc.) to be considered "personal data processing" subject to the protection system of Organic Law 15/1999, the data must be contained or intended to be included in a filing system, i.e. in a structured or organised set of data based on specific criteria. If this is not the case, the manual processing of personal data shall remain outside the scope of application of the law and shall not be "personal data processing" under the legislative concept provided for in law.

In reality, the existence of the "filing system" in the legal sense is always necessary for personal data processing to be subject to the legal protection system. In cases of automated data processing (which are always subject to the law) it is difficult to imagine the non-existence of a filing system (though this is not an express requirement) given that the data processed using automated systems are always subject to prior structural or organisational criteria" (Ruling of Section One of the Judicial Review Division of the Spanish High Court [Audiencia Nacional] of 16 February 2006).

The LOPD establishes the duty of disclosing the existence of filing systems:

"1) Any person or body creating filing systems of personal data shall first notify the Data Protection Agency.

(…)

3) The Data Protection Agency must be informed of any changes in the purpose of the computer file, the controller and the address of its location" (Article 26, LOPD).

Common sense usually identifies the existence of a filing system subject to the LOPD when a database manager is used, whereas such a filing system is not deemed to exist when the data is

processed with a word processor. However, filing systems subject to registration may exist even where a database is not used.

E.g. 1) A list of customers in a word processing, .pdf or other type of document. 2) The professional contact book in an e-mail system; 3) Photographic negatives or digital photos when the customer is identified.

On the other hand, each filing system is usually identified using a single resource. However, the reality is much more complicated. A filing system may include resources subject to automated and non-automated processing.

"1. Notification of a personal data file is independent of the processing used in its organisation and the support or supports used for processing the data.

2. When the personal data being processed is stored on different support media, automated and non-automated, or there is a copy of an automated filing system on a non-automated support, only one sole notification shall be required regarding this filing system" (Article 56, RDLOPD).

The same filing system can exist on different computers.

"from the provisions established in the Directive and in the Organic Law itself, it seems to emerge that the filing system concept is not directly linked to the requirement that the filing system may be found at a single location, but rather it is possible that filing systems may be distributed across geographical locations that are remote from one another, provided that the organisation and systematisation of the data responds to an organised and standardised set of data, subject to some kind of centralised management." Report 368/2003.

A single filing system may be deemed to exist for registration purposes in cases where filing systems may be combined in a single unit in logical terms, for example, because they are arranged for a single purpose.

E.g. The registration of the human resources filing system can include the software used for payroll management, curricula vitae managed in a recruitment process, and the folders in which social-security documents are organised.

It must be pointed out that it is the filing systems, not the processing, that are registered.

E.g. Video-surveillance systems that do not make recordings must comply with personal data protection laws, except for the duty of registration.

The Spanish Data Protection Agency website has a system for recording filing systems called NOTA, which uses predefined forms to help with the registration of the most common filing systems, such as those dealing with personnel or customers.

■ CRITERIA FOR BLOCKING AND CANCELLING DATA

When the purpose is no longer valid or when the data subject requests it with reasonable and justified grounds, data must be cancelled. Cancellation takes place in two stages, the first of which is blocking:

> "Cancellation: procedure through which the data controller stops using the data. Cancellation shall imply data being blocked, comprising its identification and retention in order to prevent processing with the exception of being available to public administrations, judges and courts for the purpose of determining any liability arising from processing, and only for the duration of such liability. At the end of this term, the data shall be deleted" (Article 5.b, RDLOPD).

This means that cancellation procedures must take account of the blocking period. To do this, the following must be taken into account:

- The period for holding or using the data, the time when its purpose becomes invalid, or the event that legitimised its processing, must be specified.

  E.g. If a worker's employment relationship comes to an end, the blocking of his or her data could commence from such time.

- In order to define the blocking period, the applicable law must be taken into account since this contains criteria for defining this period.

  E.g. The prescription period for tax obligations is four years. As such, data relating to the tax withheld for an employee should remain blocked for a period of four years following the deadline for filing the declaration for each tax year.

When this period does not exist, or if it is inferior to one year, the prescription periods for infringements under the LOPD shall be taken into account, which in the case of very serious infringements is three years.

- The use or alteration of data must be prevented. In practice, the data will remain "frozen" and inaccessible to users. The only possible action shall be making it available to the competent authorities.

Human Resources

Personnel management raises vary different questions, especially with regard to the processes of information capture and use.

■ INFORMATION ON THE PROCESSING OF PERSONAL DATA. MODES:

The duty of disclosure of Article 5 of the LOPD is an essential part of the right to data protection. The essential nature of this data applies both to the collection of personal data for processing requiring consent, and to cases in which consent is not required.

> "Article 5 of Organic Law 15/1999 establishes a duty generally imposed on data controllers, so that in principle affected parties must be notified of the processing of their data, both in cases where processing has the consent of the data subject, and for cases in which processing has been enabled due to other causes admissible under Article 6 of this Law." (Report 60/2004)

In the first case, this is because the consent, in addition to being given freely, specifically and in advance, must also be communicated and therefore the failure to inform invalidates the declaration of consent by the data subject or interested party. In addition, the content of the information defined under Article 5 of the LOPD constitutes a guarantee of data subjects' rights, since it enables them to know in respect of whom these rights may be exercised.

> "1. Data subjects from who personal data is requested must previously be informed explicitly, precisely and unequivocally of the following:
>
> a) The existence of a filing system or personal data processing operation, the purpose of collecting the data, and the recipients of the information.

b) The obligatory or voluntary nature of the response to the questions put to them.

c) The consequences of obtaining the data or of refusing to provide it.

d) The possibility of exercising rights of access, rectification, cancellation and opposition.

e) The identity and address of the controller, or its representative if appropriate.

Where the controller is not established in the European Union and is using resources located in Spanish territory for the processing, it must designate a representative in Spain, unless these resources are being used for procedural purposes, without prejudice to any actions that may be taken against the controller itself.

2. Where questionnaires or other forms are used for collection, they must contain the warnings set out in the previous paragraph in a clearly legible form.

3. The information set out in subparagraphs (b), (c) and (d) of paragraph 1 shall not be required if its content can be clearly deduced from the nature of the personal data requested or the circumstances in which they are obtained."

In the area of personnel management, organisations must be particularly careful, both in the procedure they choose and the time at which they carry out the capture of personal data.

IN PERSONNEL RECRUITMENT PROCEDURES

The first processing of personal data may take place when the future worker is simply a job candidate. Certain precautions must be taken into account:

- It is advisable, when resources permit it, to make use of printed forms with which to prepare the curriculum vitae and a procedure for preparing and delivering these by candidates. This not only enables information to be adequately provided but also to accurately define the type of data to be processed and to establish security measures, etc.

- If any kind of announcement or public tender is carried out for personnel recruitment, this must include the information from Article 5 of the LOPD.

- In the event that an unsolicited curriculum vitae is presented directly by the candidate, information procedures must be established by which it is acknowledged or confirmed that the candidate is aware of the conditions under which data processing will take place.

E.g. If the curriculum vitae sent by post or e-mail and an e-mail address is provided by the data subject, information may be sent back using this medium, requesting confirmation that this has been received and making the data processing conditional upon the acknowledgement of receipt.

If the candidate appeared at a counter or office, he or she must be immediately informed, using any means that gives proof of compliance with this duty, for example signs, acknowledgement of receipt documents and in general any means which ensures the duty of disclosure and enables compliance therewith to be proven.

It must be remembered that the Implementing Regulation of the Organic Law on the Protection of Personal Data states that the duty of disclosure must be satisfied using a medium that enables compliance to be proven, and which must be retained for so long as the affected party's data is subject to processing.

- With groups of companies or other forms of business cooperation, it must be taken into account that the transfer of data contained in the curriculum vitae, or of the document itself, must have the consent of the candidate (PS/00239/2007).

IN CONTRACTING

Employment contracts are a suitable means of informing workers of the processing that will be carried out with regards to their data. Nevertheless:

- The disclosure of information should not be confused with the expression of consent. As such, the employment contract represents an appropriate means of offering information on data processing directly related to the provision of labour. This is not the case with other types of processing.

  E.g. A company formalises an agreement through which the worker obtains advantages for certain purchases, but requires that the former confirm the identity of the beneficiary. Since this deals with consumer decisions taking place outside of the contractual relationship, the employment contract is an ineffective tool with which to obtain consent.

- Any further processing of personal data that the company decides to carry out once the employment relationship has been established shall not be exempt from the duty of disclosure.

DURING THE PROVISION OF LABOUR

Labour relations are dynamic and may be subject to changes occurring both from the worker's point of view and from the perspective of the business.

E.g. A worker who initially does not welcome the possibility that union fees be deducted from his wages decides to become a member and requests that this be the case.

The company installs a new attendance control system based on the use of video-surveillance facilities.

To do this it will be necessary to inform the worker of all cases in which changes may take place affecting the processing of personal data, such as new processes or new purposes coming into being.

IN RELATIONS WITH TRADE-UNION REPRESENTATIVES

The principle of the duty of disclosure of Article 5 of the LOPD is targeted at the data subject.

"Data subject: The natural person to whom the data undergoing processing pertains" (Article 5, RDLOPD).

Nevertheless, in processing which has an impact on the workforce as a whole, it is highly recommended that advance notice be given to the workers' representatives, given that this facilitates awareness and general understanding of such processing.

E.g. This necessity becomes particularly evident in the event that business controls are implemented, such as video surveillance, internet access controls or the use of biometric controls to check arrival, departure and presence at the workstation.

■ CONSIDERATION OF DATA WITH SPECIAL PROTECTION

Article 7 of the LOPD establishes different categories of data with special protection:

1. Data regarding ideology, religion or beliefs, for which notice must be given of the right not to provide this data at the time that consent is requested.

For this data and the data relating to trade-union membership, consent shall be provided expressly and in writing except when the data is collected by an organisation - a political party, trade union or religious entity - with regards to its members.

2. Personal data which refers to racial origin, health or sex life may be collected, processed and assigned only when, for reasons of general interest, this is provided for by law or the data subject has given his explicit consent.

This is data is worthy of special protection due to its religious or ideological nature, or because it belongs to the private core of the individual. This means that it is compulsory to make use of procedures which ensure:

- That adequate information is provided when data is collected, given that the importance of compliance with this duty is highlighted here.

  "As a consequence, the possibility of accepting express consent not stated in writing for the processing of health data is conditional on it being possible to prove that this is an expression of free, unequivocal and specific consent, which is granted once knowledge is gained of specific information. This shall necessarily include a record of the specific, explicit and legitimate purpose of the processing that will be carried out using the personal data of the subject. Logically, the existence of these points shall be stated in each specific instance." (PS/00029/2004 PS/00525/2007).

- Before collecting this type of data, it is necessary to analyse the proportionality and legitimacy of the processing.

  E.g. As examined in greater detail below, it is possible that certain health data is required in order to adapt a workstation, or that this data is deduced from the proposed adaptation. However, this does not authorise the company to include and process the health data in its information systems unless it has its own occupational-risk prevention service or company medical service. In such instances, occupational medical records shall be managed, although the employer and personnel managers shall only be able to find out data of the type "suitable/unsuitable" and the proposed adaptations.

- The processing of this type of data is planned for the organisation since it requires the adoption of high-level security measures, with the exception of the cases in the Implementing Regulation of the Organic Law on the Protection of Personal Data. Nevertheless, it should be remembered that the regulations permit the adaptation of measures to the actual structure of the information system.

"8. For the purposes of facilitating compliance with the provisions herein, when an information system has files or processing that, depending on their specific purpose or use, or on the nature of the data they contain, require the application of a level of security measures different to that of the main system, they may be separated from the latter, with the relevant level of security measures being applicable in each case and whenever the relevant data and users with access to them can be delimited, and this is recorded in the security document" (Article 81, RDLOPD).

■ INTERNAL COMPLAINTS OR "WHISTLEBLOWING" SYSTEMS

These systems generally take the form of internal mailboxes through which company employees, generally using an online procedure, can reveal the existence of conduct that breaches the law or the company's internal conduct regulations, carried out by company employees or auditors.

E.g. Employees may use these systems to report behaviours in which auditors are "bribed" to manipulate the accounts of a company, or in which a company executive provides confidential information to third parties.

Such systems may be established in accordance with data protection laws, but this requires that they be adapted to the principles established in these regulations.

- In this case, the provision of the information is of the utmost importance. Both whistleblowers and alleged offenders must have been informed in advance of the existence of these systems, of the data processing involved in making a complaint and of the consequences that may arise for the accused parties as a result of this event.

  Likewise, information may be given in the employment contract or this duty of disclosure may be established when a service such as an audit is contracted externally and the complaint is made about the parties contracted. Another possibility is to send circulars to personnel and their representatives, disclosing the existence and purpose of data processing related to these mailboxes or complaints systems.

- If the data contained in the complaints systems were to be sent to a third company to investigate the allegations, a data transfer shall take place, for which the interested parties, both the whistleblower and the accused, must be duly informed. This same disclosure shall refer, where appropriate, to the possible international transfer of data to other Group companies.

E.g. Complaints regarding the violation of data protection laws are sent to the "Chief Privacy Officer" who is based at Group headquarters in Japan.

- In any event, the existence of these mailboxes should respect the principle of proportionality, so that the complaints refer solely to those cases in which the deeds or actions have effective involvement in the relationship between the company and the accused, thus defining which actions should be subject to formal complaint and specifying the laws or internal codes of conduct to which complaints may relate.

  E.g. In systems regarding individuals, complaints mailboxes should refer to actions that may lead to the worker or employee being subjected to a sanction or to the termination of his or her contract.

- In order to ensure the accuracy of information, mechanisms should be established that guarantee that only complaints are accepted in which the person making the complaint is clearly identified. The establishment of anonymous complaints systems is unsuitable. In all cases, the confidentiality of the whistleblower's information should remain secure. As a general rule the whistleblower is not identified to the accused.

- Precisely as a consequence of the foregoing, in relation to the processing of such data, measures must be introduced to ensure the adequate security and confidentiality of the information. Strengthened security measures may be implemented and maximum precautions taken to ensure compliance with the duty of confidentiality.

  E.g.: Adopted measures may include: 1) limiting access to the content of complaints for the users that carry out the investigation and listing them in the security document; 2) establishing a system of access logs, even when it is not appropriate to apply the high-level measures described in the Implementing Regulation of the LOPD; 3) signing reinforced confidentiality commitments with authorised users, with special measures to deter violations of the duty of confidentiality.

- The retention of this data should be limited to the time necessary for the allegations to be investigated and only in the event that this investigation gives rise to specific measures against the accused should the data be retained for a longer period, otherwise it must be deleted.

  E.g. In the event that the investigation of a complaint against an executive should lead to a dismissal procedure or to demands in respect of civil liabilities, it shall be possible to retain the data once the truth of the allegations has been proven, for so long as the relevant civil or industrial proceedings should continue.

- The accused party's rights of access, rectification, cancellation and opposition shall be guaranteed, without this involving the provision of the complainant's data to the former. In any case, the accused should be able to find out the allegation that has been made in the shortest time possible in order to duly defend his or her interests.

  E.g. Providing the accused with this information after a reasonable length of time during which the preliminary investigation into the allegations is carried out.

- Filing systems created in the context of these systems shall be disclosed to the General Data Protection Register. Similarly, international transfers of data that are to be carried out must be notified and/or authorised.

LIFE INSURANCE AND PENSION PLANS

Companies and groups of companies frequently set up life insurance policies and pension plans on behalf of employees, either voluntarily or through collective agreements.

It must be remembered that:

- The data processing required for contracting this type of product must be authorised, either with the worker's consent or through the existence of the employment relationship.

- The company can carry out various types of processing:

  - The transfer of workers' identification and contact details to the insurance or pension-plan management company.

  E.g. Subject to informing its employees, the company limits itself to providing workers' data to the insurer or pension manager , so that they in turn can establish relations with the insured parties or pension-plan participants, and can collect all the necessary data.

- The collection of data linked to the contract to be signed, so that it can be transferred to the insurer or pension-plan manager.

E.g. Providing the worker with access to the file or the request to join the collective life insurance policy, which must be completed with the data necessary, for example in relation to the beneficiaries.

- In any case, when collecting data, workers must be informed under the terms described above, taking into account the existence of different possibilities:

  - In the employment contract.

When consent is required because the data processing is not based on the duties or obligations of the parties in an employment relationship, the contract is not the most suitable instrument. Where used, information shall be expressly provided about the terms under which the right of opposition must be exercised.

  - Through the preparation of specific information directed at workers.

- In this type of processing, the worker's right of opposition must be taken into account when processing data without consent, by virtue of the obligations imposed on employers by regulations or a collective agreement.

- Data processing may affect family members or individuals related to the workers when the latter have to designate the beneficiaries of the insurance policy or pension plan. In this case, data processing shall be legitimised by the existence of the employment relationship, although it must be remembered that the data must only be what is necessary (proportionality) and relevant to the contracting of the insurance policy or pension plan (purpose).

"The Spanish Data Protection Agency considers that in cases in which, though not identical to the present, there is a certain degree of similarity, the reference to the "parties" in a legal relationship envisaged in Article 6.2, may be considered on an equal footing with the "personal elements" of said relationship, so that when the relationship is formalised by the data subject in a third party's favour, the processing of the latter's data, required to formalise the relationship, may be deemed protected by Organic Law 15/1999.

In this sense, it is considered that the processing of the data of a life-insurance policy beneficiary is protected pursuant to the provisions of Article 6.2 of Organic Law 15/1999, even when the beneficiary has not given consent to the data processing" (Report 363/2008).

- It is therefore advisable to accurately define the procedure for capturing and processing personal data, opting for the most efficient method of guaranteeing data subjects' rights. In this sense, from a data processing perspective that fully respects the fundamental right, the most appropriate action may consist, subject to informing the workers, of solely transferring the data of insured parties or pension plan participants to the insurer or pension plan management company, leaving it up to them to carry out subsequent steps.

OUTSOURCING OF PAYROLL MANAGEMENT

Payroll management is often outsourced to an employment consultancy or group company. The contracted firm has to access personal data in order to carry out its services and, in accordance with the LOPD, is defined as the data processor.

> "Specifically, in the event that the company provides data to the agency for the specific purpose of carrying out data processing activities, and therefore the customer must decide as to the purpose and use of the information, the former shall be considered as the data controller responsible for the filing system and shall disclose its existence to the General Data Protection Register.
>
> Given that this case deals with a scenario in which the agency will be designated as the data processor, the relationship between the two entities shall be subject to the provisions of Article 12 of the Law" (Report on analysis of the Data Controller concept).

Data processing by third parties is a concept regulated in great detail by Article 12 of the LOPD, which establishes the need to formalise a contract and define its content and the obligations of the parties. Article 20 *et seq*. of the RDLOPD regulated the details of these services provided with access to data. Of the provisions set forth in these rules, the following must be taken into account:

- The assignment will be regulated through a contract which must be drawn up in writing or any other manner that provides proof of its content and execution. Verbal contracts are excluded.

E.g. Another way might be to execute the contract using electronic media which place its content on record.

- The content of contracts envisaged under Article 12 of the LOPD shall be adjusted to the personal data processing that the contract regulates, and cannot consist merely of the repetition of this precept.

- It is extremely important to bear in mind specific security needs, particularly when the processing is carried out on the data supports of the data processor.

- The conditions for destroying or returning the personal data to the data controller may include possible delivery to a new data processor.

- If the data processor decides to subcontract, it must be authorised to do so by the data controller. There are two possibilities in this respect.

  - Subcontracting may be provided for in the contract with the data processor, either indicating the authorised subcontractor or defining the circumstances in which subcontracting may take place.

  - Subsequent authorisation from the data controller at the request of the data processor.

  In either case the data controller shall know the identity of the subcontractor and a contract shall be signed between the data processor and the subcontractor in accordance with Article 12 of the LOPD.

- Specific tasks may be entrusted to the data processor, such as attending to the rights of access, rectification and cancellation, or responsibility for the security document.

  E.g. When a data controller outsources the payroll management so that this is carried out entirely at the premises of the data processor, the responsibility for the security document may be delegated.

- The RDLOPD permits data processors to retain blocked data, where there is a legal obligation or liability that justifies this.

Occupational Risk Prevention

Law 31/1995 of 8 November on the Prevention of Occupational Risks (LPRL) and its implementing regulations impose a series of activities on companies with the ultimate goal of preventing or reducing occupational risk. The processing of workers' personal data is necessary for this task.

E.g. It is obvious that, as a minimum, prevention planning requires a detailed list of all workstations and the individuals that occupy them. In addition, a series of questions must be addressed regarding the risks inherent to the job, answers to which may often depend on the personal or medical characteristics of the workers themselves. Are they allergic to certain chemical elements? Do they require certain conditions in terms of the brightness or the size of letters on their computer screen? Are they capable of clearly identifying an acoustic alarm?

CONSENT IN RISK PREVENTION

In principle, the processing of personal data in the field of risk prevention is legitimised by the existence of a contractual relationship, and is rendered necessary by the compliance, performance and control thereof (Article 6.2, LOPD).

This must be dealt with in the area of health monitoring, which may be voluntary or compulsory. The general rule is that of willingness, in which case consent is required.

"Employers must guarantee that their workers undergo periodic monitoring of their state of health according to the risks inherent in the work.

This monitoring may only be carried out when workers provide their consent..." (Article 22.1, Law 31/1995 of 8 November on the Prevention of Occupational Risks).

Nevertheless, this monitoring may be compulsory under Article 22.1 of the Law on the Prevention of Occupational Risks, subject to the report of the workers' representatives, in cases where medical examinations are essential for assessing the effects of the working conditions on the health of

the workers, for ascertaining whether a worker's state of health represents a danger to himself, to other workers or to individuals related to the company, or when included in a legal provision relating to protection against specific risks and particularly hazardous activities.

Nevertheless, in any of these cases it must not be forgotten that:

- Compliance with the duty of disclosure is essential.

- Particular attention must be paid to the principles of quality and proportionality, with the collection and use of data being strictly limited to those necessary for the purposes of prevention.

RISK PREVENTION ACTORS

The execution of risk-prevention tasks requires the presence of specialised areas of action (safety, ergonomics and psycho-sociology, industrial hygiene, occupational nursing and medicine) and of professionals with diverse organisational requirements and profiles. It is important to have the adequate means and resources, which are not always available to all companies.

In practice, this has meant that legislation provides for the existence of internal and external prevention services and that the professional performance of risk prevention is assigned to various professional profiles. This has a dual impact on data protection.

- The role of the file manager or data controller varies depending on whether the prevention service is internal, external or combined. If it is an in-house company service, the company shall be responsible for the filing system used for prevention management.

  It must not be forgotten that if the prevention service is in-house, different profiles and powers for accessing health data will exist within the company. Healthcare personnel shall have full powers in this respect. For management, access powers shall be limited to data of the type "suitable/unsuitable".

Companies acting as external prevention services shall be considered as data controllers (Report 0299/2009).

- The implementation of risk-prevention policies defines various roles from the perspective of personal data protection. Prevention services shall be interdisciplinary by nature. As such, the information systems dedicated to the management of prevention services must take the following into account:

  - The security level. This shall be high in all cases in which health data is included containing specific identification of diseases, injuries etc., or where occupational health records are managed.

    "Health-related personal data: information regarding the past, present or future health, physical or mental, of an individual. In particular, data referring to the level of disability and genetic information of a person is considered as health related" (Article 5.1.g, RDLOPD).

  - The access profiles and functions of all users must be precisely defined.

    E.g. The profile of an administrative worker who arranges appointments cannot be the same as that of an occupational doctor. In the same way, the person responsible for the ergonomic adaptation of a workstation should be able to access the health data required for this activity.

- Workers' clinical records must be governed by the provisions of the LOPD, as well as by the principles of Law 41/2002.

  "At the same time, healthcare personnel carrying out occupational health monitoring activities have the right, as set forth under the second paragraph of Article 22.4 of this Law, to find out the medical information deriving from these activities. In this sense, this information shall comprise, in accordance with the provisions of the same Law, the occupational medical history of the worker. It must be taken into account that medical histories would be subject to the provisions of Basic Law 41/2002 of 14 November, regulating the autonomy of patients and the rights and obligations in matters of clinical documentation and information, which requires the healthcare centres or professionals providing medical services relating to the patient to be responsible for this documentation, and in this case it is the worker that is subjected to tests resulting from the health monitoring activities" **(**E/01040/2005**)**.

- Procedures must be established to ensure workers' rights of access, rectification and cancellation.

Regarding access to medical histories, it must be remembered that specific legislation imposes duties such as the limitation of access to the subjective notes of the medical practitioner, the existence of limits on rectification contained in sector regulations on matters of social security, and the im-

possibility of cancelling data which must be retained by virtue of public health regulations. In all circumstances, requests must be answered, giving grounds for refusal.

ACCESS TO DATA BY THE COMPANY AND BY HEALTH AND SAFETY REPRESENTATIVES

In occupational risk prevention there are various regulatory provisions that involve the possibility of transferring personal data. As such, legislation enables and requires data to be transferred to health and safety representatives, to the public health authority in the framework of the Law on General Health, to the labour inspectorate, and to the labour authority, without forgetting the specific cases mentioned under Article 11.2 of the LOPD, such as the transfer of data required by judges and courts, or those necessary in the event of a medical emergency, or in epidemiological studies. The cases which pose greater difficulties are those regarding access to information by the company itself and by the health and safety representatives.

Company powers to access information are extremely limited and in practice refer to finding out the worker's status of suitability or unsuitability.

> "As such, the processing of medical records by occupational risk prevention services as a consequence of the medical examinations carried out on workers, shall be limited by the provisions of Article 22.4 of the aforementioned Law on Occupational Risk Prevention (LPRL). In this sense, access to medical information obtained pursuant to the provisions of the LPRL is prohibited to entrepreneurs and third parties, including persons or bodies with responsibilities in the field of prevention, other than "the medical personnel and public-health authorities that carry out occupational health monitoring", and with the sole exception of conclusions deriving from this monitoring in relation to workers' suitability to carry out their job" (PS/00142/2005).

Nevertheless, it is possible that the employer must access workers' personal information in a specific way, in order to comply with its obligations, which goes beyond the suitable/unsuitable nature of the content. In such cases, legitimisation of data processing derives from the same Law, but shall be limited to the data strictly necessary.

> E.g. It is evident that if a computer screen must be adapted to a certain letter size then there are visual problems; that there are hearing problems if an acoustic warning signal needs to be exchanged for a visual one; and that if a work uniform has to be of a certain fabric, there may be an allergy. In each of these cases it may be possible to deduce the presence of a disability or illness.

Transfers of data regarding the worker's suitability are admitted in the event that the mutual society contracted to carry out prevention tasks previously had access to relevant information on the performance of the job in a new company.

> "We consider, given the special concurrent circumstances, that in the present case, the transfer of data that took place is protected by Article 11.2.a) of the LOPD, and that it has a legitimate purpose, which is that referring to the correct application of the aforementioned regulations on Social Security and the Prevention of Occupational Risk and, indirectly, to the prevention of fraud, therefore consent is not required of the complainant worker" (High Court judgement of 24/05/07).

Health and safety representatives are authorised to access information and documentation relating to working conditions where necessary for the performance of their functions and, in particular, to the information envisaged under Articles 18, 23 and 36 of the LPRL.

> "c) To be informed by the employer of damages to the health of workers once the former has become aware of these, it being possible to visit the site of the alleged events, even outside working hours, in order to find out about the circumstances.
>
> d) To receive information from the employer, obtained by it from the people or bodies responsible for the activities of protection and prevention within the company, as well as from the competent bodies with responsibility for the health and safety of workers, without prejudice to the provisions of Article 40 of this Law on matters of cooperation with the Labour and Social Security Inspectorate" (Article 36.2 of the LPRL).

They will therefore be able to access personal data regarding damage to workers' health when this is the result of a harmful event, related to the working environment, for the sole purpose of the control attributed to them by the LPRL and limited to strictly necessary data, understood to be data relating to the seriousness and nature of the damage. The health and safety representatives are assignees and are bound by the principles of personal data protection. In particular they should keep to the duty of confidentiality in accordance with the LOPD and specific legislation in this area.

> "The provisions of Article 65, paragraph 2 of the Workers' Statute shall apply to health and safety representatives regarding due professional confidentiality in relation to the information to which they may have had access as a result of their activities in the company" (Article 37.3, LPRL, E/00312/2007).
>
> "2. The works council and its members and any experts in attendance shall observe the duty of confidentiality in relation to all information which, in the legitimate and objective interest of the company or the work site, has been communicated to them expressly and in confidence" (Article 65.2 of Royal Legislative Decree 1/1995 of 24 March, approving the consolidated text of the Law on the Workers' Statute).

Business controls

The Workers' Statute has attributed specific powers to companies which facilitate control over the provision of labour. The exercise of these powers often involves the processing of personal data.

"3. Employers may adopt the monitoring and control measures they deem appropriate in order to verify the worker's compliance with his labour obligations and duties, maintaining due consideration for their human dignity and taking into account the actual capacity of disabled workers, if any, in the adoption and application of these measures.

4. Employers may verify the status of workers' illnesses or accidents, where alleged by the latter to justify absences from work, through examinations performed by medical personnel. Any refusal to undergo such examination may lead to the suspension of the worker's economic rights by the employer as a result of such situations". (Article 20.3 and 4, Royal Legislative Decree 1/1995, of 24 March, approving the consolidated text of the Law on the Workers' Statute).

CONTROLS BASED ON THE USE OF INFORMATION TECHNOLOGIES

When information technologies are used to control business functions, the possible repercussions for workers' rights are multiplied. The use of these kinds of technologies is manifested in very different ways.

Techniques include biometric controls such as fingerprints, video surveillance, computer-based controls (such as remote monitoring, analysis and checks, the indexing of internet browsing, or the checking and monitoring of e-mail and/or the use of computers), or controls on the physical location of the worker using geo-localisation.

The processing of personal data exists in most of these cases and it is therefore necessary to comply with data protection principles. The Spanish Data Protection Agency and past cases in the courts have indicated different scenarios in which such processing is acceptable and the conditions in which it can be carried out.

However, the use of information technologies multiplies the possibilities for company control, requiring workers' fundamental rights to be respected and the adoption of control measures that are proportional and respectful of their dignity, their right to data protection, and their private lives.

As such, there is a set of principles that should be respected, when these are practically applicable.

- The legitimacy of the data processing derives from the existence of the employment relationship and therefore, in accordance with Article 6.2 of the LOPD, it does not require consent.

  "2. Consent shall not be required when the personal data is collected to perform the functions of public administrations within the scope of their responsibilities; when it relates to the parties in a contract or preliminary contract for a business, employment or administrative relationship, and is necessary for its maintenance or enforcement; when the purpose of processing the data is to protect a vital interest of the data subject under the terms of Article 7(6) of this Law, or when the data is contained in sources accessible to the public and its processing is necessary to satisfy the legitimate interest pursued by the controller or that of the third party to whom the data is communicated, unless the fundamental rights and freedoms of the data subject are at risk. (Article 6.2, LOPD).

- The principle of proportionality must apply when deciding to adopt a control measure that involves the processing of personal data.

  E.g. It may be perfectly reasonable for a geolocalisation device to be designed for tasks such as the transport of goods, in which it is important to know the current location of the vehicle and the time at which it will be possible to make a certain delivery. This does not mean that a device of this nature is provided to all the workers in a company when the nature of their functions does not make this necessary.

- There must be a purpose which, in this case, must be that which is established by Article 20.3 of the Workers' Statute, "to verify compliance by the worker with his labour obligations and duties".

  "With regard to the possibility that fingerprints are processed without the consent of the data subject, (...) it shall be possible that processing takes place without consent, given that Article 6.2 of the LOPD envisages that it shall not be necessary to obtain consent where data 'relates to the parties in a contract or preliminary contract for a business, employment or administrative relationship, and is necessary for its maintenance or enforcement'." (Report on the Processing of Workers' Fingerprints).

- The data obtained and stored must be accurate and up-to-date and shall not be retained for longer than is necessary. Employers are advised to establish a data storage period.

- The duty of disclosure to workers must be fulfilled. This duty is particularly significant when dealing with controls over the use of the internet and/or e-mail.

  In this case it is highly advisable that the information provided to workers is clear with regards to the company's policy on the use of e-mail and the Internet, describing in detail the extent to which workers may use the company's communications systems for their private or personal use. It is also recommended that this includes the purpose of the monitoring, information on the monitoring measures adopted, and when it might have an impact on the resources normally used by the worker.

Furthermore, insofar as these kinds of controls have an influence on the whole of the business, it may be advisable to also provide information to the workers' representatives on the policies adopted in this matter.

In no way does this mean that the worker should become aware of the details of security policies that may affect those areas that the company needs to protect. However, it is essential that workers are aware of whether they can receive private messages or leave photographs in certain places on their computer or on a corporate server.

Prior information and evidence of this is essential, given that this type of processing does not require the consent of the worker and is an expression of the company's powers of control.

> "It is important to remember what has already been said about the existence of a general social habit of tolerance towards the moderate personal use of computer resources and means of communication provided by companies to workers. This tolerance creates a similarly general expectation of confidentiality in these uses; an expectation which cannot be ignored, although neither can it become a permanent impediment to company control, because although workers have the right to respect for their privacy, they cannot impose this respect when using a resource provided by the company against the instructions established by the company for its use, outside the controls envisaged for this use and for ensuring the continuance of the service. As such, the company must establish prior rules for the use of these resources (with the application of absolute or partial prohibitions) in accordance with the requirements of good faith, and inform workers about the existence of the control and
>
> the resources that must be applied in order to check this compliance, as well as the measures that have to be adopted where appropriate to ensure the effective work-related use of the resource when necessary, without prejudice to the possible application of other preventive measures, such as the exclusion of certain connections. Therefore, if the resource is used for private purposes, contrary to the prohibitions and in the knowledge of the applicable controls and measures, it cannot be said that "the reasonable expectation of privacy" has been violated when controls are carried

out under the terms established by the judgements of the European Court of Human Rights of 25 June 1997 (Halford case) and 3 April 2007 (Copland case) in order to assess the existence of a violation of Article 8 of the European Convention on the Protection of Human Rights" (Judgement of the Social Division of the Supreme Court of 26 September 2007).

CONTROLS ON WORKPLACE ABSENTEEISM

The Workers' Statute authorises companies to carry out checks in cases of occupational accidents or illnesses that result in non-attendance. This check shall be made by means of medical examination and the law provides for the possibility of proceedings against the worker in the event of a refusal to submit to the examination.

"4. Employers may verify the status of the workers' illnesses or accidents, where alleged by the latter to justify absences from work, through examination performed by medical personnel. Any refusal to undergo such examination may lead to suspension of the worker's economic rights by the employer as a result of such situations" (Article 20 of the Workers' Statute).

However, two previously indicated elements in this Guide must be taken into account:

- The processing of medical data shall require the express consent of the worker or the existence of a legal provision granting exemption from this requirement. The LOPD contains specific procedures in cases concerning the provision of medical care, which is not applicable to this case.

  "6. Notwithstanding the provisions of the preceding paragraphs, the personal data referred to in paragraphs 2 and 3 of this Article may be processed when such processing is necessary for purpose of preventive medicine or diagnosis, the provision of medical care or treatment, or the management of healthcare services, provided such data processing is effected by a health professional subject to professional confidentiality or by another person also subject to an equivalent duty of confidentiality.

  The data referred to in the preceding subparagraph may also be processed when this is necessary to safeguard the vital interests of the data subject or another person in the event that the data subject is physically or legally incapable of giving his consent" (Article 7.6, LOPD).

- The possibility of the company accessing this health data and using it for purposes other than those for which it was collected is impossible since, as indicated previously, the company may only be aware of the conditions of suitability.

- The inclusion of health data in a filing system which has the sole purpose of carrying out checks on absenteeism is disproportionate.

  "through the creation of the database under discussion seems to be a more effective control of workplace absenteeism, according to the powers granted to employers in this regard by the prevailing legislation. In this sense, it is first of all advisable to warn that these powers do not include the storage of data pertaining to workers' health - and specifically that of medical diagnosis - in computerised format, which requires the consent of the workers. Moreover, and independent of the foregoing, the truly important issue is that the measure adopted by the company, subject to the norms established for checking whether a measure restricting a fundamental right exceeds the principle of proportionality, is not considered a suitable, necessary and proportionate solution for achieving the purpose, in this case the control of absenteeism in the workplace [Constitutional Court Judgements 66/1995, court consideration 5, 207/1996, court consideration 4. E) and 69/1999, court consideration 4.], given that this is not a considered and balanced measure, since the benefits or advantages that derive from it in a general or company interest, do not outweigh the detriment to the aforementioned right to privacy" (Constitutional Court Judgement 202/1999).

The control of absenteeism acquires particular importance when carried out by contracting a service provider, since in addition to complying with the obligations inherent to a data processor, it must abide by certain conditions:

- The information provided to the worker must be very precise and indicate that this is a work-related control. As Article 5 indicates, one of the pieces of information that must be provided if appropriate refers to the obligation to supply data and the consequences of refusing to supply them.

  The information shall refer to the fact that the conditions of suitability are being verified on behalf of the company and that the nature of this processing conforms to Article 20.4 of the Workers' Statute.

- The express consent of the worker shall be required in order to be able to include his or her health data in a clinical record.

  "in this case the object is not patient care - a purpose that justifies the exception to the prohibition established in the law, given that the maintenance of the medical record is of benefit to the patient's health - but a technique for controlling absenteeism. (...)

  In this sense, and contrary to the argument, the reasoning of Constitutional Court Judgement 202/1999 of 8 November applies, when it argues that the filing system falls outside the exceptions of Article 7 of the Organic Law because "they are not aimed at the preservation of the workers' health, but at the control of absenteeism"; therefore the existence of the filing system without the express consent of the data subject is an inappropriate measure that

infringes the right to informational freedom. For the rest, Article 8 of Organic Law 15/1999 does not apply, given that this law regulates the transfer of health-related data based on the prior existence of a legal data filing system, and we have already seen that this is not the case. In short, we must comply with the judgement of the High Court (1st section) of 12 April 2002 (Appeal 1271/2000)" (Judgement of the First Section of the Judicial Review Division of the High Court of 10 May 2002).

There is no obstacle to the pursuit of the dual purpose of verifying the worker's state of health and controlling absenteeism. However, if data processing is carried out relating to health, the express consent of the worker must be obtained.

- In the event that the external provider carries out health monitoring services, the latter should formulate procedures to ensure compliance with the principles of data protection, particularly the duty of disclosure, the principle of purpose, and the guarantee that consent is provided for any processing carried out.

- Lastly it must be remembered that in this type of service, the external provider holds the status of data processor and must comply with the provisions of Article 12 of the LOPD.

Trade union relations. Communication of data, notice boards, censuses.

The Spanish Constitution recognises the right to freedom of association, and the implementing legislation establishes a set of rights, competences and functions for workers' representatives, which requires the processing of personal data and the establishment of certain data flows, typically though the communication of this data by the company.

> "1. All have the right to freely join a trade union. The law may restrict or exempt the exercise of this right in the Armed Forces or Institutes or other bodies subject to military discipline, and shall lay down the special conditions of its exercise by civil servants. Trade union freedom includes the right to set up trade unions and to join the union of one's choice, as well as the right of trade unions to form confederations and to found international trade union organisations, or to become members thereof. No one may be required to join a trade union.
>
> 2. The right of workers to strike in defence of their interests is recognised. The law governing this right shall establish the necessary safeguards to ensure the maintenance of essential public services" (Article 28, Spanish Constitution).

THE PUBLICATION OF PERSONAL DATA ON NOTICE BOARDS

The Organic Law on Trade Union Freedom recognises the right to use a notice board which allows union information to be provided to workers.

> "For the purposes of enabling the dissemination of such notices that may be of interest to union members and workers in general, the company shall place a notice board at their disposal which shall be located in the work site and in a location that is suitably accessible by all workers" (Article 8.2.a, Organic Law 11/1985 of 2 August on Trade Union Freedom).

It is a common practice to publish notices, announcements, declarations and even judgements on this type of notice board. Moreover, technological developments have given rise to the availability of online bulletin boards, either in spaces provided by the company itself, or on domains belonging to the relevant trade union. When these documents contain personal data, the mere act of their publication constitutes a form of processing that may involve the data being accessed by third parties that are unauthorised to do so.

"the right to freedom of association (…) must prevail over the right to personal data protection, when, as occurred in the case in question, industrial action includes the recurrent union activity of passing specific information between workers and work centres, data which is solely required for understanding the news, providing a certain awareness of the information that is relevant from the trade-union perspective" (Judgement of the High Court of 19 December 2007, E/00729/2008).

This requires a series of aspects to be taken into account in order to apply the laws appropriately and ensure the rights of the individuals concerned:

- The data controller of the notice board, and therefore the party responsible for the information published on it, shall be the body or organisation that makes decisions regarding its use and purpose, and which materially places the information on it.

- The specific physical or virtual space in which the notice board is located must be considered so that in the event that it contains personal information, it is only visible to users who are authorised to consult it.

  E.g. It is unreasonable for a notice board from which union information can be obtained to be situated in an area that is freely accessible by customers or suppliers.

- It is essential that online union notice boards are located on the company intranet and never on the Internet.

  "If the information in question had been published on the corporate intranet, in view of the existing circumstances, there would have been no violation of the right to data protection and the complainant would probably not have brought the events to the attention of the AEPD.

  What makes this case special with regards to the provisions of the judgement, is that the personal data: name, surname, professional category (traffic police officer) and warrant card number are published on an Internet web page. Publication on the net is neither suitable, necessary or proportionate to the purpose of keeping workers informed of issues that may have a direct or indirect impact on labour relations.

  This access to the complainant's personal data (...) by any Internet user is what makes this case unique regarding the content of the aforementioned judgement of 19 December 2007.

  As such, in view of the specific existing circumstances, the Court considers that the right to freedom of association can be fully satisfied without the need to publish the complainant's personal details on the Internet, therefore such publication cannot be protected under the facade of the aforementioned right to freedom of association.

Furthermore, it should be noted that neither can the right to truthful information and rights to the freedom of expression prevail over the right to data protection, since it was possible to disclose information without placing the complainant's personal data on the Internet, according to the criterion followed in the judgement of this Section of 16 February 2007 cited by the contested decision, which contrary to the arguments put forward in the claim, indeed presents a similarity with the present case.

In addition, the published information lacks general interest and relevance to the public, which are the predominant factors taken into consideration by the Constitutional Court in granting preference to the right of freedom of expression over other constitutional rights" (Judgement of the First Section of the Judicial Review Division of the High Court of 8 July 2009).

- Utmost consideration must be granted to the principle of quality from the point of view of the proportionality of the data processing and its purpose.

  E.g. Published information should be limited to what is strictly necessary. As such, if in a given moment it was decided to publish a certain administrative decision or a court judgement of interest to workers, personal data should be rendered anonymous where these may affect the rights of the parties or other individuals who may appear in such decisions or judgements, and where the publication of the data is lacking in relevance from the freedom of association perspective.

- It is advisable to consider the possibility of preventing unauthorised third parties from accessing the information on notice boards.

ACCESS TO DATA BY THE WORKS COUNCIL

The Workers' Statute attributes a raft of powers to union representatives, especially to the works council. In some cases, the exercise of these powers may involve access to data.

E.g. In accordance with Article 64 of the Workers' Statute, works councils shall have the right: to be informed of all sanctions imposed due to very serious offences and to receive basic copies of the contracts and notifications of deferrals and complaints in this respect within a ten-day period of them taking place.

Nevertheless, this potential access to personal data must be governed by strict compliance with the principles of data protection.

- This data may only be transferred in cases in which this is strictly necessary for compliance with the duties that the Workers' Statute establishes for the company.

  E.g. This method shall be chosen in all cases in which information may be presented in an anonymous and statistical manner, whilst allowing the council to fulfil its functions.

  E.g. In the case of access to the master copy, access should only be to the data that enables the control function assigned to the workers' representatives to be carried out, and should not allow the transfer of all the worker's data.

- The recipients of the information shall be those stated by the law, who authorise the transfer.

  E.g. Occasionally unions and workers' representatives tend to become confused. When the possibility of accessing personal information is granted to a works council or to the incumbent representative of the workers, the duty of secrecy is extended to the relations maintained by the representative, including with his or her union.

- The works council or union representatives who access workers' information are obliged to maintain its confidentiality and to comply with the principles of the LOPD and those specifically envisaged in applicable laws.

  "2. The works council, its members and any experts in attendance shall observe the duty of confidentiality with regards to all information which, in the legitimate and objective interest of the company or the work centre, has been communicated to them expressly and in confidence.

  3. Under no circumstances shall any document delivered by the company to the works council be used outside the strict sphere of the former, or for purposes other than for which it delivered.

  The duty of confidentiality shall continue even following the expiry of its mandate and irrespective of its location"

  (Article 65 of the Workers' Statute).

TRANSFERS OF PERSONAL DATA TO UNIONS

The most common transfer of data to union organisations is that relating to the collection of union fees from wages. Given that this is a request that must be made by the worker, the conditions of Article 7.2 of the LOPD must be in place.

"Personal data which reveals the ideology, trade union membership, religion and beliefs may be processed only with the explicit and written consent of the data subject. Exceptions shall be files maintained by political parties, trade unions, churches, religious confessions or communities, and associations, foundations and other non-profit bodies with a political, philosophical, religious or trade-union aim, as regards the data relating to their associates or members, without prejudice to the fact that assignment of such data shall always require the prior consent of the data subject."

The processing of this data requires procedures to be adopted by the organisation to protect particularly sensitive information.

- It is advisable to make use of procedures for obtaining consent, such as request forms in which the worker may provide express written authorisation for data processing.

- It is extremely important to limit the use of this data to the purpose for which it is being collected: collecting fees and transferring amounts to the union organisation.

  E.g. For example, it is not possible to process data on union membership for the purposes of applying deductions to the salaries of striking union members. (Constitutional Court Judgement 11/1998).

- It must be remembered that if the processing takes place under exactly the same terms and for the purposes described here, its security level shall be basic.

Secondly, the sending of union information via e-mail must also be explained. This activity requires the processing of personal data since, as has been indicated on a number of occasions, e-mail addresses are personal data.

The Constitutional Court has indicated that the sending of this type of e-mail message constitutes a union right included under the fundamental right of freedom of association (Constitutional Court Judgement.281/2005). Nevertheless, certain conditions must be in place, such as the company having an available e-mail service and e-mails being sent in a manner that is proportionate and not detrimental to the normal functioning of the organisation.

When these circumstances are in place, the transfer of personal data to unions shall be legitimate. However, the following considerations must be taken into account:

- That there are automated processes that allow compliance with the right to freedom of association without the need to make a data transfer, thereby minimising risks and obligations of legislative compliance for both the company and the trade union.

  E.g. The use of mailing lists enables the union to send information to a corporate address of the type unionlist@company.com, without accessing the data. On the other hand, though the company does process personal data, it may include the information from Article 5 of the LOPD at the foot of the e-mail and automate cancellations and opposition to data processing by removing addresses from the lists at the request of the user (Report 0101/2008).

- The communication of data shall be limited to those cases strictly necessary.

  E.g. Under no circumstances shall data such as the worker's private e-mail addresses be transferred.

- Data shall be used strictly for the purpose for which it was transferred.

- As the assignee, the union is obliged to comply with the provisions of the LOPD.

- The union must satisfy the workers' right of opposition, except in the event of union elections, at which time the freedom of association prevails over the right to data protection.

  "According to the provisions contained in the LOPD regarding the right of opposition, the workers' right to demonstrate their opposition to the receipt of messages with union-related content must be recognised, along with the consequent union obligation of ceasing to process the data of the requesting parties. Nevertheless, in relation to the union information sent to workers during the electoral period, it should be noted that at this time the right to trade union activity, established in Article 2.1 of the Organic Law on Trade Union Freedom, must prevail over the fundamental right to data protection.

  As such, during trade union elections, workers may not oppose the processing of their personal data provided that the union uses it in a manner conducive to the aims of the electoral process itself" (TD/01119/2008).

It must not be forgotten that the holding of trade union elections legitimises the transfer of census data, needed to enable the union to send electoral information and to participate in the electoral process.

TRANSFERS OF DATA CONTAINED IN TC2 SOCIAL SECURITY PAYMENT DOCUMENTS

Labour laws, and in particular collective bargaining agreements, establish two possibilities for facilitating the delivery of copies of these documents and, as a consequence, for transferring the personal data they contain. These possibilities are provided for two very specific purposes; union control over the actions of the company, and ensuring compliance with the company duties in the event of subcontracting.

SUBMISSION OF TC2 DOCUMENTS TO THE WORKS COUNCIL

The submission of this type of document is subject to compliance with certain principles:

- The council must act within the framework of the functions attributed to it by the Workers' Statute.

  "Transfers of workers' data may only be understood to be protected in the event that these take place within the scope of the functions performed by workers' representative bodies, where the right of representative bodies to access specific worker data within the sphere of its competences is recognised by the Workers' Statute. Otherwise the consent of the data subject shall be required in order to proceed with the communication of his or her data. Moreover, the use of data by the workers' representatives should be limited to the purpose of control attributed to the representative by the Statute itself (…)

  As a consequence, taking into account the works council's competences to receive copies of the work contracts signed with the company, which necessarily entail a knowledge of the persons linked to it through an employment relationship and monitoring it in relation to social security, there is no objection to the transfer of workers' data to the works council, provided that this data does not exceed the data contained in the aforementioned contracts". (Report 0247/2009).

- The type of information that may be accessed is limited.

  "taking into account the competences of the works council, under no circumstances shall access be provided to the workers' payslip, for example. The only existing obligation is that of submitting the TC1 documents, the social security payment receipts in which data appears to identify the company and establish the debt, and the TC2, in which the list of employees appears, containing data relating to the identification of the workers, their bases for calculation and the provisions that have been satisfied in the delegated payment system" SEE REPORT OF 28 MAY 2007.

Nevertheless the collective agreement may contain specific provisions which, being regulatory sources of the employment relationship, may extend the scope of the transfer.

> "Article 3 of the Workers' Statute of 24 March 1995 includes collective agreements among the sources of the employment relationship, which regulate the rights and obligations concerning this relationship. From this it is deduced that the proposed communication of data, expressly set forth in the collective agreement, would be contemplated under Article 11.2 paragraph c), as cited in the preceding paragraph, making it possible that the data be released from within the company, thereby responding to the implementation and compliance of the employment relationship between the data controller and data subject" (Report 252/2006).

- In any case there are no legitimate grounds for making this document public on a company notice board.

> "Therefore given that Article 7.3 of the aforementioned Organic Law (the LOPD) applies, the communication of TC2 data requires a Law or the express consent of each worker" (Report 0247/2009).

TRANSFERRING THE PAYSLIPS AND TC2 DOCUMENTS OF SUBCONTRACTED WORKERS TO CONTRACTOR COMPANIES

In cases where there are subcontracted companies, the Workers' Statute establishes obligations with regards to the main company that may legitimise the transfer of personal data. Two cases need to be distinguished:

- The time prior to the contracting or subcontracting, in which a certificate must be requested from the Tesorería General de la Seguridad Social (General Treasury of the Social Security) to check that the contractors are up to date with social security payments, and in which no transfer is contemplated.

> "Employers that contract or subcontract other parties to carry out works or services related to their own activities must check that these contractors are up to date in their social security payments. For this purpose, a social security clearance certificate shall be obtained in writing, with the identification of the company concerned, from the Treasury, which must issue this certificate within thirty days (which cannot be extended) and under the terms established in regulations. Once this deadline has expired, the requesting employer shall be released from liability" (Article 42.1 of the Workers' Statute).

- Subsequently, in relation to the joint and several liability for the salary and social security obligations, grounds would exist based on the existence of a legitimate interest derived from the provisions of the law (Article 10, RDLOPD).

  "Article 42.2 of the Workers' Statute imposes joint and several liability on the main contractor, a liability that implies compliance with a wage-related obligation and those obligations related to social security during the valid period of the contract.

  (…) when in the presence of a joint and several obligation, each debtor shall provide in full the item to which this obligation relates. If the main contractor is jointly and severally obliged to make wage and social security payments during the valid period of the contract, it must be aware of the full content of this obligation in order to be able to meet it.

  (…)

  As a result, the transfer of TC2 data is covered by Article 7.3 of Organic Law 15/1999, in relation to Article 42.2 of the Workers' Statute, and by the scope imposed by the Civil Code on joint and several obligations" (Report 0412/2009).

This justification would apply to data relating to union membership. Payslips may include data of this nature when it relates to compliance with the duty to deduct and transfer union fees. This data may form part of these joint and several obligations.

- The principle of proportionality must be applied when defining the group of workers affected.

  "In all cases, access by the contractor should be limited to data related to subcontracted workers and not to all workers in the subcontracted company" (Report 0412/2009).

Duties of workers with access to personal data: confidentiality and security.

The LOPD deals with the duty of security along with the duty of confidentiality when it regulates data protection principles. Both duties are considered to be of primary importance.

> "The controller or, where applicable, the processor shall adopt the technical and organisational measures necessary to ensure the security of the personal data and to prevent its alteration, loss, unauthorised processing or access" (Article 9).

> "The controller and any persons involved in any stage of processing the personal data shall be subject to professional confidentiality as regards such data and to the duty to keep them. These obligations shall continue even after the end of the relations with the owner of the file or, where applicable, the person responsible for it" (Article 10).

Both principles are necessary and constitute a guarantee of the fundamental right to data protection. Secrecy and confidentiality ensure that personal data are only known by the data subject and by those users in the organisation whose profile gives them the power to use, consult, modify or include the data in information systems.

> "This duty of confidentiality means that the controller of the stored data can neither reveal nor disclose its content, having the 'the duty to keep them, obligations that shall continue even after the end of the relations with the owner of the file or, where applicable, the person responsible for it'. This duty is an essential requirement prior to the recognition of the fundamental right to informational freedom, referred to in Constitutional Court Judgement 292/2000 of 30 November, and insofar as the present case is concerned, means that the processed data cannot be known by any external person or entity outside the cases authorised by the Law, since this is precisely the meaning of confidentiality" (PS/00192/2008, Judgements of the First Section of the Judicial Review Division of 18 February 2002 and 1 February 2006).

Furthermore, in addition to confidentiality, security guarantees the availability of data and therefore its recovery in the event of an incident, and its integrity, protecting it in the event of unauthorised use. The company should have policies for compliance with these two principles, given that they not only guarantee a fundamental right, but also offer reliability and security to the public. In addition, with the implementation of security measures, important company assets, such as customer and supplier data, are protected.

To adequately comply with these two duties, it is essential to make use of personnel management policies in which personnel training procedures and the functional profiles of each job are very clearly defined. It is therefore not surprising that the RDLOPD should regulate both of these aspects specifically.

> "1. The functions and obligations of each of the users or user profiles with access to the personal data and to the information systems shall be clearly defined and documented in the security document.
>
> The monitoring functions or authorisations delegated by the data controller of the filing system or processing shall also be defined.
>
> 2. The data controller shall adopt the necessary measures so that members of staff understand the security regulations that affect the performance of their functions as well as the consequences that may arise in the event of non-performance" (Article 89, RDLOPD).

In certain sectors such as healthcare, the requirement to establish user profiles derives from law, which specifically defines the functional profile for each type of worker.

> "1. The clinical record is an instrument fundamentally designed to ensure that the patient receives the appropriate treatment. The healthcare professionals at the centre where the diagnosis is made or the patient is treated have access to the patient's medical history as a fundamental instrument for the appropriate treatment.
>
> 2. Each centre shall establish methods to enable patients' clinical records to be accessed at all times by the professionals attending to them.
>
> (...)
>
> 4. Administration and management personnel at healthcare centres may only access clinical records data relating to their own functions"
>
> (Article 16 of Basic Law 41/2002 of 14 November on the autonomy of the patient and the rights and obligations with regard to information and clinical documentation).

The obligations of confidentiality and security in the field of data protection represent extremely specific duties linked to the processing itself, going beyond the traditional concept of professional confidentiality. Failure to adequately comply with these obligations endangers the fundamental right to data protection and typically causes serious damage to the reputation of the company.

E.g. One of the most common infringements in the area of data protection is to abandon non-destroyed documents in the general waste by cleaning personnel. Recently the absence of limits on the installation of peer-to-peer programs, such as the well-known e-Mule, has exposed vast amounts of personal data to the world.

It is therefore advisable:

- To design staff functions and responsibilities taking into account their connection to the processing of personal data.
- To provide adequate training for workers, taking into account their different levels of responsibility and ensuring that they are aware of their duties of confidentiality and security. Training must help to create a culture of commitment to data protection.
- To warn and train even those workers who, though not having a direct relationship with information systems and the processing of personal data, may endanger its confidentiality and security.

RESOURCES OF THE SPANISH DATA PROTECTION AGENCY

The Guide to Data Protection in Labour Relations aims to analyse specific aspects in this field. The Spanish Data Protection Agency has a series of guides and resources which will allow you to explore this subject in greater depth, and will help you to apply the prevailing regulations appropriately.

The Guide for Data Controllers contains directions about the basic principles that must be taken into account to adequately comply with data protection legislation.

The Guide to Data Security will help you to implement, review and apply the security measures contained in the Implementing Regulation of the Organic Law on the Protection of Personal Data.

The Guide on Video Surveillance describes the issues relating to the processing of images, especially those relating to security and use for labour control purposes.

The Spanish Data Protection Agency's **NOTA** system enables data controllers with responsibility for personal data, whether publicly or privately owned, to comply with the obligation established in the LOPD to inform the Spanish Data Protection Agency of its filing systems. NOTA provides you with information and guidance on the requirements of this notification process. This free, simple tool enables you to provide information on a number of filing systems relating to the management of freeholders' associations, customers, pharmacy prescription books, patients, school administration, video surveillance, payroll and human resources under private ownership.

EVALUA is a diagnostic procedure based on a self-test or form with multiple-response questions. Simply complete the procedure and the Spanish Data Protection Agency can provide you with a report with the directions and resources to guide you, where appropriate, to comply with the provisions of the LOPD or to check the status of your compliance in relation to security measures.