PERSONAL DATA PROTECTION – FAQ

These Frequently Asked Questions are broken down into three parts:

Part 1 contains answers to general questions on personal data protection.

Part 2 is about employees' personal data protection rights.

Part 3 covers the obligations to which employees are held in matters of personal data protection.

1. General questions

1.1 What is considered personal data?

Personal data means information about a natural person who is or can be identified either directly or indirectly using an ID number (e.g. social security number), one or more properties specific to that person (e.g. first and last initials) or a combination of other characteristics such as birth date, place of residence, biometrics, etc.

1.2 How does French law provide for the protection of personal data?

France's data privacy act (known as the "Loi Informatique et Libertés du 6 janvier 1978", as amended on 6 August 2004) applies whenever information about a natural person is handled either digitally (in a computer file) or manually (on paper).

The act defines the principles to be complied with when collecting, processing or storing personal data, and it guarantees individuals a certain number of data protection rights.

2. Personal data protection rights of employees

2.1 What are the basic principles of data privacy for employees?

- Lawful purpose of data collection

Personal data shall be collected or processed only for a specified and lawful purpose. Failure to adhere to said purpose may result in criminal sanctions.

Example: The purpose for which an IT application is being implemented must be specified clearly beforehand (e.g. to manage the hiring process, network security, time-tracking, etc.).

- Adequacy and relevance of data

Only the personal data that is adequate and necessary to the stated purpose may be collected or processed.

Example: A job applicant's family information, health records and social security number are not relevant to the recruiting process. This information can only be collected if it conditions the provision of specific benefits.

As reiterated in France's labour code, the collection of information about employees must not result in restrictions of individual rights and freedoms unless those restrictions are proportional to the stated purpose and justified by the lawful interest of the employer.

Example: A workstation cannot be placed under round-the-clock video surveillance unless there is a specific and duly substantiated safety risk to the employee working there.

- Limited retention of personal data

Information cannot be kept on file indefinitely. A specific retention period must be determined depending on the purpose of each file.

Example: Career management files may be kept as long as the employee remains with the company. Payroll files may be kept for up to five years. Recruitment files may be kept for a maximum of two years following the last contact with the job applicant. Video surveillance recordings may be kept for up to one month.

- Security and confidentiality of data

Employers have a data security obligation as data processors. They must take the necessary steps to ensure that data is kept confidential and is not divulged to unauthorised third parties.

Example: Every employee must have his or her own password, which must be changed regularly. Data access permissions must be precisely defined depending on each user's actual needs (read-only, read-write, delete). Computer terminals may also be set to require password re-entry after a short period of no activity.

Personal data may only be consulted by those who are authorised to do so as part of their role within the organization.

Example: Authorised members of the human resources department may access payroll information, network administrators may access internet login data, etc.

Data may nonetheless be shared with third parties provided those parties have special legal authorisation (labour inspectors, tax authorities, police, etc.).

- Respect for individual rights

-Right to be informed

Whenever an employee or job applicant's data is digitized, that person must be clearly informed as to (1) why his or her data is being requested, (2) whether the requested information is required or optional, (3) to whom the information will be provided and (4) how to exercise the rights guaranteed under the French data protection act to access, rectify/remove or refuse that information.

-Right to access and right to rectify/remove data

Individuals are entitled to demand that the party in possession of a file send them any information on them contained in that file. They are entitled to have any erroneous information either rectified or removed.

Example: Employees and job applicants are entitled, without reason and by sole virtue of a request submitted to this effect, to obtain from an employer a copy of any data it may have on them (recruitment and career history, compensation, reviews and assessments, disciplinary records, etc.). See below.

-Right to refuse the collection/recording/processing of data

Individuals are entitled to disallow, with lawful reason, the keeping of a digital record of their personal information, except where such a record is required under applicable law or regulations (payroll filings, official staff roster, etc.).

Example: In certain cases, a person may refuse to allow his or her professional contact information or photograph to be placed online.

2.2 What personal data are employers allowed to collect?

The only data that can be collected as part of the recruitment process is that used to assess the applicant's qualifications for the job (education, experience, etc.).

When someone is actually recruited, the employer may collect additional information. Besides the legally required information (for mandatory payroll filings, etc.), the employer may also collect information that is needed for:

• administrative purposes (driving licence, emergency contact, etc.)

• internal coordination purposes (optional headshots for staff directories and organizational charts, etc.)

• benefits provided by the employer (beneficiaries of the employee, etc.)

2.3 Who is allowed to access employees' personal data?

Access to employees' personal data must be restricted. Information on job applicants may be accessed only by individuals involved in the recruiting process.

Besides the authorities and institutions entitled to receive notification of changes in employment status (unemployment office, national health insurance, pension administrators and mutual insurers, etc.), employees' personal information is restricted to persons responsible for the administration of human resources.

Supervisors may access the information they need for the purposes of their work (performance reviews, compensation, etc.).

Staff delegates (*délégués du personnel*) have access to the data that is contained in the official staff roster (*registre unique du personnel*), such as name, nationality, position in the company, start date, etc.

Other staff representatives (works council, union delegates) may obtain certain information to facilitate the performance of their duties. For example, an employer may send its works council (*comité d'entreprise*) information about employees, provided those employees have been consulted and have not expressed a refusal. The works council may use this information to refine its offering of activities and services.

Union organisations may send employees emails with union-related information provided they have a prior agreement with the employer. Employees may request not to receive these emails at any time.

Access to personal data must be tracked.

Employers must ensure that information is kept secure and that only authorised persons are exposed to it. A record must be kept of actions taken by authorised persons when accessing personal data (who logged in to what, when and for what purpose).

2.4 How do employees exercise their right to access their personnel files?

Any current or former employee who can provide proof of identity is entitled to access his or her personnel file at the company.

What kind of data are employees allowed to access?

Current and former employees are entitled to access all of their personal data, whether it has been kept in digital format or in written or printed form.

This includes:

-recruitment records

-career history

-compensation

-reviews and assessments

-disciplinary record

Restrictions on access rights:

Current and former employees are not entitled to access data on another employee, nor are they entitled to consult data that is considered forward-looking (career potential, ranking) unless that data has been used to determine their pay rises, promotions, etc.

An employer may refuse any request for information that is deemed patently excessive. If the employee contests such a refusal, the burden is on the employer to demonstrate that the employee's request is excessive.

What are the steps to follow when exercising this right?

The right to access one's personnel file may be exercised either in person or in writing. Proof of identity is required.

The employer must respond immediately to all requests made in person and within two months if the request is submitted in writing. If the employer refuses the request, it must do so in a written letter explaining the reason for its refusal and explaining how and until when the employee may contest the refusal.

2.5 Have my personal data been sent to a subsidiary outside the EU?

Sopra HR Software employee data is kept on file at a subsidiary in Tunisia. This is referred to as "data transferred to a non-EU country" (or "third country" in EU parlance). In order to ensure that employees whose data is protected in the EU enjoy the same level of protection when their data leaves the EU, each of our subsidiaries has signed EU "standard contractual clauses". For the purposes of ensuring adequate data protection for employees, Sopra HR Software's BCRs now eliminate the need to enter into standard contractual clauses.

3. My obligations as an employee to protect the personal data of Sopra HR Software clients

3.1 Rules that every employee must obey

- Personal data may be accessed only as instructed by Sopra HR Software and its clients.
- All employees must comply with the operational and organisational procedures set up at Sopra HR Software to ensure data security and confidentiality
- More precisely:
    - Do not use the personal data to which you have access for any purposes other than those necessary for your work
    - Do not sell, assign, let or otherwise transfer the personal data to which you have access because of your work without the express prior consent of Sopra HR Software
    - Do not make copies of personal data without the express prior consent of Sopra HR Software (unless those copies are necessary for your work)
    - Inform Sopra HR Software immediately of any accidental or unauthorised access to personal data, and more generally any failure to comply with applicable data protection rules and regulations
    - Keep the information you process confidential

3.2 What are the penalties for breaking the rules listed in 3.1?

- Disciplinary action
- Civil liability (damages)
- Criminal liability