New French guidelines on personal data processing for HR purposes

Hi everyone,

It's been a while since I wrote to you last. I hope you are all staying healthy! I'm back with a newsletter packed with new information since the French data protection authority (CNIL) just adopted its final guidelines on personal data processing for everyday human resource management purposes on April 15. This subject matter has always been a hot topic, perhaps even more so lately. Whether you or your own clients have French subsidiaries or need to draft your own guidelines, I hope you'll find this information useful for your privacy programs. At the end of this newsletter, I've also summarized the CNIL's recommendations for processing employees', agents', and visitors' personal data at the workplace and on telework systems during the COVID-19 pandemic.

Audience and scope of the guidelines

The guidelines are directed toward both private and public employers and cover all employee statuses. The CNIL reminds employers that they must follow both the GDPR and French labor laws. The guidelines cover the everyday processing of personal data in an HR context but exclude processing activities by trade unions, employee representative bodies, and occupational health services. They do not cover sensitive processing activities such as psychometrics, algorithmic processing for profiling purposes, big data processing activities, or processing activities aiming to control employees on an individual basis.

Purposes of processing

The CNIL states that data must be processed to meet a specific purpose and serve the employer's business purpose and activities, i.e.:

- recruitment
- administrative management of staff
- payroll management and the handling of related administrative formalities
- providing tools to staff
- work organization
- career and mobility monitoring
- training
- mandatory record keeping and relationships with employee representative bodies
- internal communication
- management of social benefits
- audits and the management of litigation and pre-litigation matters

Legal bases

For each HR activity, the CNIL lists the purposes of processing and the related legal basis. (The most common legal bases are complying with a legal obligation, performing a contract to which the data subject is a party or taking steps at the request of the data subject prior to entering into a contract, safeguarding the legitimate interests pursued by the employer, or performing a task carried out in the public interest. The data subject's consent can only be used in exceptional circumstances in an employer/employee relationship (e.g., for the recording of a promotional video). Here, the CNIL refers to the ex- Article 29 Working Party' opinion WP217.

Personal data concerned

The CNIL reemphasizes the principle of data minimization for each processing activity: The employer must only collect the data absolutely necessary for the related purposes and can only reuse data if it has a legal basis to do so.

The guidelines contain many examples of personal data collected for each HR purpose listed above. If you need specific examples of one of the purposes, please contact me directly. I'll just give one example, as I think it is very relevant to telework in light of current events: the provision of tools to staff where personal data is collected and processed based on the employer's legitimate interest for the following purposes:

- monitoring and maintaining computer equipment (examples of data collected: data for processing requests, data regarding the equipment provided and the date provided, data related to equipment maintenance and returns, budget allocation data)
- managing IT directories to ensure security and to make sure that software and networks work properly (examples of data collected: connection data, except for any data that would allow for the individual monitoring of the employees' activities)

- managing business e-mail systems (examples of data collected: address books, individual account data, except for any data that would allow for the individual monitoring of electronic messages sent or received by employees)
- setting up internal virtual private networks needed to transfer and collect data for the administrative management of staff (e.g., intranet) (examples of data collected: internal administrative forms, organization charts, data related to chat rooms and information rooms)

Data recipients

Personal data must only be accessed by employees on a need-to-know basis. When an employer decides to subcontract some HR activities, which may involve transferring some personal data, a data processing agreement must be executed (Art. 28 of the GDPR; see also the CNIL's Guide for Processors with examples of contractual clauses). Any transfer outside the EU must also comply with Chapter V of the GDPR.

Personal data collected for HR management purposes must also comply with Art. 5 of the GDPR: Data must be kept no longer than necessary only for the purposes for which the personal data are processed. The employer must decide on the data retention period before processing but can keep the data for a longer period in a separate archiving system to fulfill legal requirements set forth in the French Labor Code, the Social Security Code, and the Commercial Code. For example, the CNIL advises to keep pay stubs for one month only in an active database and for five years in a separate archiving system in order to comply with the French Labor Code (Art. L3243-4). Pay stubs may also be kept for fifty years in an electronic format (French Labor Code, Art. D3243-8).

Information to be provided to data subjects

Employers who act as controllers must comply with Art. 13 and 14 of the GDPR. The CNIL has published several templates to help employers fulfill this obligation. In addition, under the French Labor Code, employers must inform their employees individually in some cases and/or consult the relevant employee representative bodies.

Data subjects' rights

As data subjects, employees have the following rights: the right to object, the right of access, the right to rectification, the right to erasure (in some circumstances), the right to restriction of processing, and the right to data portability.

Data security

The CNIL refers to its 24-page security guide on its website and provides a detailed table of data security measures categorized as follows:

- Raising user awareness
- Authenticating users
- Access management
- Logging access and managing incidents
- Securing workstations
- Securing mobile data processing

- Protecting the internal network
- Securing servers
- Securing websites
- Ensuring continuity
- Archiving securely
- Supervising maintenance and data destruction
- Managing data processors
- Securing exchanges with other organizations
- Physical security
- Supervising software developments
- Encrypting, guaranteeing integrity, and signing

Data Protection Impact Assessments

Some data processing for HR management purposes does not require a DPIA:

- processing for HR management purposes at companies with a head count of less than a 250, except for profiling purposes
- processing for controlling physical access (except for the use of biometric devices and the processing of sensitive data or highly personal data)

Some data processing for HR management purposes requires a DPIA:

- processing for individual profiling for HR management purposes
- processing aimed at monitoring employee activity on an ongoing basis

Last but not least, and although this information is not in the guidelines, the CNIL has also issued recommendations to employers in light of the coronavirus crisis. These guidelines are consistent with the formal Statement on the processing of personal data in the context of the COVID-19 outbreak issued by the European Data Protection Board (EDPB):

1) **Processing personal data of employees, agents, and visitors at the workplace during the Covid-19 pandemic:**

The CNIL (as well as the Luxembourg Data Protection Authority) has drawn up two lists: DOs and DON'Ts with regard to good and bad practices:

DOs:

- DO raise awareness and invite employees/agents to report an exposure, if any, to the employer or the competent health authorities
- DO facilitate the communication of information
- DO encourage telework and the use of occupational health care services
- The employer may collect the date and identity of the person who may have been exposed to the virus and take organizational measures (by taking containment measures, arranging for telework, contacting the occupational health service, etc.) when a data subject reports information.

DON'Ts:

- DON'T take the employee's, agent's, or visitor's body temperature and report this information to the management
- DON'T ask employees or agents to fill out data sheets or health questionnaires

(For those of you located in the United States, I find it interesting to compare these recommendations to the ones issued by the EEOC in the U.S.)

2) Recommendations related to telework

- Draft a security charter for telework purposes, or at least minimum rules to be followed. If this document is intended to be used formally as the company's "internal rules" ("règlement intérieur"), some formal steps will need to be followed (French labor law requirements)
- Analyze the ongoing risks and take the required measures if the company's information system management rules need to be changed
- Install a firewall and antivirus and antimalware software on all employee workstations
- Set up a VPN on employee workstations
- For Internet services:
    - use protocols ensuring confidentiality and authentication of the recipient server
    - apply the latest security patches
    - apply double-factor authentication mechanisms
    - regularly monitor the access logs of services accessed remotely
    - prevent direct access to all server interfaces that are not secured

If you have any specific questions about the CNIL's guidelines or coronavirus guidelines, don't hesitate to drop me a line!

Stay safe!