



# France: Relevant legislation

We have identified the following key pieces of legislation which are applicable to employee IT monitoring in France. Note that there is other legislation which is applicable which we have not included in this document.

## French Civil Code (Article 9)

- 'Everyone has the right to respect for his or her private life'. A court can direct whatever steps may be necessary to put a stop to violations of this right.
- 'Private life' is defined as: love life, friendships, family circumstances, leisure activities, political opinions, trade union or religious affiliation and state of health.

## The Labour Code

- System monitoring must be:
  - justified by the nature of the task to be performed; and
  - proportionate to the intended purpose.
- In the event of a conflict between the Labour Code and a relevant collective bargaining agreement or employment agreement, the provisions more favourable to the employee apply.

## The 'right to log off'

- The right of the employee to log off, is the right not to use professional IT systems (smartphone, emails, etc.) during rest times (vacation, evening, week end, etc.). There are provisions in the French labour code which provide for an obligation on the employer to implement a right for employees to log off from IT systems in the following cases:
  - for Companies having more than 50 employees in France: these companies have an obligation to negotiate with their staff representatives on the employee's right to log off
  - for Companies having employees working under a lump sum remuneration in consideration for a fixed number of worked days ("forfait annuel en jours").
- Out of these two cases, there is no legal obligation for the employer to implement the right to log off.



- In the event of a claim, should an employer not have implemented a right to log off, an employee could claim payment of overtime or violation from the employer of his obligation to protect health and safety.
- There is no specific effect of the right to log off on IT monitoring of employees. When a company provides for such a right, it must implement all the effective tools to enable the employee to disconnect from IT systems during rest times: e.g. pop up message to prohibit sending emails after a certain hour in the evening or during week end, message at the end of an email indicating that there is no necessity to reply out of office hours, etc...

### **French Data Protection Act 1978**

- Regulated by the Commission Nationale de l'Informatique et des Libertés (CNIL).
- Employer must inform employees of monitoring – it must not be secret, disguised or unfair.
- Monitoring must not be excessive – case law and CNIL prohibit the permanent monitoring of employees at work, except in exceptional circumstances. Some monitoring may need to be reported to the CNIL.
- Right to privacy of employees prevent the employer from accessing the personal files/documents of the employee, if the employee has expressly identified these files/documents as personal.

# Principles deduced from case law

Monitoring must be:

- transparent (with prior notification to employees and staff representatives);
- fair;
- not excessive;
- legitimate;
- proportionate (for example, consider phone call metadata as opposed to content); and
- not contrary to the employee's right to privacy and freedom.

Intrusion by an employer into data an employee has marked as 'private' or 'personal' (or similar terms) is highly likely to be taken as an invasion of an employee's privacy.

## Social media

The same rules apply for monitoring social media as they do for other monitoring practices.

There has been distinction in case law made about 'public' comments versus more 'private' comments, only accessible to authorised users or 'friends'. The latter are unlikely to be deemed a public broadcast of (for example) defamatory or otherwise dismissible information, even when a 'friend' is another employee.

## Illegally gathered evidence

Many of the cases in our report focus on the lawful or unlawful nature of evidence used by employers through monitoring to sanction employees.

A strict position appears to be taken; such that a failure to comply with French legal requirements as to employee monitoring is likely to mean the evidence obtained cannot be used against the employee.

# The future

**GDPR:** The General Data Protection Regulation applies in France, as a member of the EU. It will make it necessary for employers to be proactive in ensuring compliance with the French Data Protection Act. See UK chapter or short report for more detail on the GDPR.

**Remote working/home office:** Likely to be growing obligations/constraints on the employer, such as the obligation to monitor the working hours of employees and compliance with their professional obligations balanced against respecting the employee's freedom and private life.

Organisations must be aware that legal considerations for employee monitoring will vary from organisation to organisation and specific issues will arise depending on the nature of the organisation undertaking monitoring and the risks it is trying to mitigate. Dentons UK and Middle East LLP (Dentons) prepared a report for NPSA on Employee IT Monitoring in March 2018 (the Report), to serve as a legal resource only, it is not a substitute for professional advice. This document provides a snapshot of some of the information contained in the Report and must not be read in isolation. Neither the Report nor this document are designed to provide legal or other advice and you should not take, or refrain from taking, action based on their content. The Report and this document are not a comprehensive report of all the information or materials that are relevant to this area of law, and do not address any particular concerns, interests, value drivers or specific issues you may have. This is a complex area of law that is changing rapidly. If you require assistance with a specific issue, you should seek legal advice from an appropriately qualified professional. Organisations planning to implement or review existing employee monitoring should seek their own professional advice. The Report (and therefore the information contained in this document) was current as of the date of the Report publication (being March 2018). Neither NPSA nor Dentons owe any duty to you to update the content of the Report or this document at any time for any reason. Please note the Report and this document do not represent the views of NPSA or Dentons. Neither NPSA nor Dentons UK and Middle East LLP accept any responsibility for any loss which may arise from reliance on the Report and/or this document.