

## PRACTICAL GUIDE THE INFORMATION TECHNOLOGY CHARTER

*This practical guide is for informational purposes only and is not a comprehensive presentation of the information technology charter. It does not constitute legal advice.*

Providing employees with communication tools can subject the company to certain risks. Introducing uncontrolled new technologies in a company may lead to a drop in productivity and may encourage technical risks (viruses, hackers, saturated networks, etc.) and legal risks (civil or criminal liability of the company and its executives).

The Information Technology Charter represents the most efficient ally for the company wishing to protect itself against the risks tied to using new technologies.

### ➤ PURPOSE

The development and adoption of an information technology charter is not mandatory, but the choice is left up to the employer.

The information charter informs employees about the laws and rules imposed upon them. It defines the rules of the game and allows sanctions for disregarding the rules.

### ➤ CONTENT

The employer has a lot of freedom in creating the information technology charter. The charter can thus address various topics, like for instance:

- Employees' Emails

The employer can choose to authorize the employee a reasonable personal use of the professional email address and can thus establish tools to monitor and ensure such usage.

In this case, the information technology charter informs the employee of the implementation of monitoring tools on the professional email address (measuring the frequency and size of messages, scanning attachments for viruses, filtering spam, etc).

The information technology charter may also state rules regarding the employee's personal email. Indeed, even though messages sent and received by the employee during the work day are presumed to be professional (*Cass. Soc., May 30, 2007*), and can consequently be freely consulted by the employer, the employee has a right, even during the work day, to privacy (*Cass. Soc. October 2, 2001, Nikon*). Consequently, the information technology charter may establish that messages expressly labelled as "PERSONAL" by the employee cannot be, in principle, monitored by the employer.

### ▪ Employees' Use of the Internet

The employer can choose to authorise reasonable personal employee use of the internet and implement monitoring tools to verify such usage (filtering non-authorized sites: pornography, child pornography, racism, revisionist, etc).

The information technology charter will notify the employee of the rules regarding internet use, like for instance bans on downloading software, joining discussion forums, accessing personal email accounts, watching movies or listening to music online, and of the monitoring means implemented.

The information technology charter may also inform the employee that internet use during the working day is presumed to be professional, thus permitting the employer to check it without the employee being present (*Cass soc. July 9,200*).

### ▪ Employee's Telephone Use

The employer that allows the employee reasonable personal use of the business's phone can establish tools and monitor and ensure such use (autoswitch). In this regard, the charter notifies the employee that an autoswitch has been implemented and of the rules regarding its use (monitoring the reasonable personal use of the telephone, monitoring the productivity of the employee, listening to employee telephone conversations). Here again, the information technology charter's purpose is to bring the employee's attention to the means of surveillance and control implemented.

### ▪ Geolocation: Tracking the Physical Location of the Employee

Under certain conditions, the surveillance of the employee can extend beyond the workplace. Indeed, today it is possible to use global positioning system technologies (geolocation) to, for example:

- Ensure the security of individuals or merchandise during transport,
- Better manage personnel and vehicles,
- Track and bill services,
- Monitor employees during the workday, when this cannot be accomplished by other means.

The information technology charter will thus inform the employee of the implementation of such monitoring, the rules regarding its usage, and most notably, that geolocation does not permit the collection of information regarding speeding, that the geolocation data will only be accessible to authorized personnel, and of the length of time the information will be stored.

## ➤ IMPLEMENTATION

The information technology charter can take on the form of a disciplinary device, as indicated by case law. Its implementation and the implementation of monitoring instruments or communication tools should consequently abide by the following requirements:

- **Preliminary Notification and Consultation by Institutions Representative of the Employees**

In accordance to the provisions of article L. 2323-13 of the Employment Code, the employer must notify and consult with the company committee prior to commencing the significant project of introducing new technologies in the company.

Additionally, the company committee should be informed and consulted, prior to the implementation of all means and techniques that monitor employee use of new technologies (*article L. 2323-32 of the Employment Code*).

Finally, in the case where the charter can be regarded as a disciplinary measure within the company, it should be subject to certification by institutions representing employees so that its provisions are opposable to the employees, notably in the case of a disciplinary procedure that may lead to dismissal.

- **Preliminary Notification of the Employees**

The information technology charter is above all a means of notifying the employees, entering the domain of legal obligations of the employer. This is why the charter should outline both the means of monitoring and the rules governing the use of new technologies.

Moreover, the employee must, before their implementation, be informed of the instruments used by the employer to monitor the employee's use of new technologies. Indeed, according to the provisions of article L. 1222-4 of the Employment Code, "no data may be collected regarding an individual employee through a device that the employee had no prior knowledge of."

- **Notifying the CNIL**

The tools implemented to monitor employee use of the means of communication at their disposal being susceptible to lead to processing and collecting of employee personal data, the employer must notify the CNIL of the monitoring and control tools that he plans to implement, according to the rules applicable to the processing of personal data.

*Ichay & Mullenex Avocats is a French law firm focusing on all legal issues related to the new technologies, the green business and the sustainable development in France and abroad. They are considered experts in intellectual property and Internet law, e-commerce, online gaming, data protection. Ichay & Mullenex Avocats also assists its clients on all issues related to financing, mergers & acquisitions, restructuring, etc. and advises them on their litigation and arbitration procedures.*