# CNIL Adopts New Rules on Service Quality Monitoring and BYOD

The French data Protection Authority (hereafter: "CNIL") recently released two documents reinforcing employees' rights to privacy in relation to (i) the recording of telephone conversations with customers, and (ii) the use of personal device for work purposes, the so-called Bring Your Own Device (hereafter: "BYOD").

In a Decision No 2014-474 of November 27, 2014, the CNIL issued a Simplified Norm in which it simplifies the registration requirements for the recording and use of telephone conversations between employees and customers, while ensuring employee's rights as follows:

(i) The recording may not be permanent or systematic, including for evidentiary purposes.

(ii) The purposes of the recording must be limited to employee training, employee evaluation and improvement of customer service.

(iii) Employees must be provided with a notice that describes the purposes of the processing, the categories of data processed, the recipients of the data, individuals' access rights and whether international data transfers take place.

(iv) Customers must be informed about their right to object before the end of the data collection.

(v) Companies may register their processing through a declaration of conformity by which they declare that they comply with the Simplified Norm. Where companies exceed the requirements of the Simplified Norm or process sensitive data, they will need to file a normal declaration.

On February 19, 2015, the CNIL released short guidance for the use of BYOD. Although the guidance is not binding, it represents the CNIL's current view. The guidance clarifies that BYOD may not replace a professional device as employers must provide their employees with the means necessary to perform their work.

Companies are advised to draft a specific security policy for the use of BYOD including provisions on:

(i) Identification of the part of the personal device that will be used for professional purposes and creation of a corresponding "security bubble".

(ii) Authentication measures for the control of distant access (electronic certificate or chip card).

(iii) Encryption of information flows (VPN, HTTPS).

(iv) Procedure for a security failure, including information of network administrator, provision of alternative device, and distant deletion of the professional data.

(v) Advanced security measures such as terminal locking with strong password and up-to-date antivirus protection.

(vi) Guarantees that the security measures may not prevent employees from using the device for personal purposes and that employers may not access the private information.

Finally, please note that companies do not need to register the use of BYOD separately from their general processing for HR management.

The Decision on service quality monitoring is available (in French) at:
http://www.cnil.fr/documentation/deliberations/deliberation/delib/326/

The guidance for the use of BYOD is available (in French) at:
http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/byod-quelles-sont-les-bonnes-pratiques/

Written by:

Jan Dhont
j.dhont@lorenz-law.com
+32 2 239 20 08

Delphine Charlot
d.charlot@lorenz-law.com
+32 2 239 20 06