Belgian DPA Clarifies Policy on Workplace Cyber-Surveillance

On May 2, 2012, the Belgian Data Protection Authority ("DPA") issued its long-awaited recommendation on cyber-surveillance in the workplace (Recommendation nr. 08/2012). This non-binding recommendation strives to clarify the Belgian rules governing access to the content of electronic communications at work, among other things.

Accessing electronic communications' content has historically been risky in Belgium. The Belgian 2005 Act on Electronic Communications requires a specific legal basis or prior consent of all the parties involved to access private electronic communications (typically e-mails). In addition, the threshold to qualify electronic communication as "private" is extremely low in Belgium: all electronic communication is considered private between those parties involved in the communication, and the employer is considered to be a third party to that communication, even if a professional e-mail account is used. Belgian case-law is rather polarized as to whether employers may access electronic communication, often taking the view that there are no sufficient clear legal grounds to access the content of e-communications and that an employee is not in a position to provide free consent to its employer.

In its game-changing recommendation, the DPA opines that the current legal framework provides a sufficient legal basis to access e-communication content in certain cases. However, the DPA takes the view that accessing such content is legally authorized based on the employer's general authority as set forth in the 1978 Employment Contract Act, rather than individual consent in any particular case. The DPA considers the employee's consent to access e-communication content unreliable as consent may not be "freely" given.

However, the DPA highlights that such access is only allowed if it is conducted in compliance with three principles: finality, transparency, and proportionality ("Principles"). *Finality* means that employers should have a specific, well defined and legitimate purpose to access content of electronic communications. *Transparency* means that employees must be informed of the monitoring practices of the employer. *Proportionality* implies that the employer cannot systematically access all electronic communication of its employees. Additional procedural rules (such as notice requirements, works council consultation and monitoring methodology) are specified in a Collective Labor Agreement ("CBA No. 81") and should of course be observed.

The DPA further proposes practical measures to comply with the Principles, such as:

- Employers should consider restricting employees' use of professional e-mail accounts for private purposes in their ICT policy. This should mitigate the risk that the employer interferes with employees' private communication. In case such restrictions are put in place, the employer may presume that all emails are professional. E-mails can then be opened provided that the Principles and the CBA 81 have been respected. This implies, for example, that an employer can access the e-mail account of an employee who is sick or on leave to follow up on an urgent matter, or in the context of a targeted control of compliance with the provisions of the employment contract. However, it must be noted that the DPA is of the opinion that in case employees have been prohibited to use their professional e-mail account for private purposes, they should be allowed to use an alternative e-mail address for private purposes at work.
- If employees are allowed to use their professional email account for private purposes, additional measures should be taken to mitigate the risk that the employer interferes with the private communication of its employees. This implies among other things that an employer should in a first phase monitor traffic data of emails, and access the content of private emails of their employees only if irregularities show up. If access is absolutely required, it is recommended to appoint a trusted third party to perform the task.

Overall, the recommendation signals the commitment of the DPA to confront challenges that arise for businesses in a practical way. Nevertheless, it is not yet clear whether courts will subscribe to and implement the DPA's position.

The full text of the recommendation is available here.

Jan Dhont and **Jonathan Guzy** of Lorenz Brussels.

Jan heads the Data Privacy Practice at Lorenz. He can be reached at j.dhont@lorenz-law.com (+32 2 239 2000). Jonathan specializes in data protection and privacy and can be reached at j.guzy@lorenz-law.com.