

Spanish Data Protection and Digital Rights Law Secures Employees' Right to Privacy

Para leer la Client Alert en español, [haga clic aquí](#).

The Spanish Digital Rights Act includes new rights and monitoring developments relevant to both employers and employees.

KEY FOCUS AREAS

- Digital disconnection rights
- Employees' and employers' rights relating to the use of digital devices
- Use of video cameras, sound recording devices, and geolocation devices
- Role of collective bargaining agreements
- Whistleblowing provisions

Background

The Organic Law 3/2018 on Protection of Personal Data and Guarantee of Digital Rights (the Spanish Digital Rights Act), which entered into force on 7 December 2018, repeals the previous Organic Law on Data Protection (LOPD) of 1999 and adapts the Spanish legal system to the provisions of the General Data Protection Regulation. The Spanish Digital Rights Act has also introduced new digital rights and other monitoring provisions that incorporate the latest EU and Spanish case law on this matter.

Digital Disconnection Rights

- For the first time in Spain, a statutory provision acknowledges the right of all employees (including those in management positions) to digitally disconnect outside working hours.
- This right will preserve an employee's resting time and personal and family privacy as a means to improve their work-life balance.
- Companies must establish an internal policy outlining how this digital disconnection right must be effectively exercised. However, before implementing such policy, companies must consult workers' representatives.

Use of Digital Devices

- The Spanish Digital Rights Act recognises an employee's right to protect their privacy when using company-issued digital devices.
- Companies are authorised to monitor the use of digital devices provided to employees for the following purposes only:
 - To control compliance by employees of their legal and statutory obligations
 - To confirm the integrity of the device itself
- Companies are obliged to establish a criteria for employees' use of digital devices, complying with minimum privacy standards in accordance with social customs and worker rights. Workers' representatives must be involved in the process of drafting such criteria and employees must be informed of its content.
- If devices are authorised for personal use, employees need to be informed of the authorised uses and companies have to establish measures to preserve worker privacy.

Use of Video Cameras, Sound Recording, and Geolocation Devices

- Companies may use video cameras for monitoring purposes provided that:
 - They guarantee employees' privacy and dignity rights
 - They expressly, clearly, and concisely inform both employees and workers' representatives that the company is using video cameras. In the event of a wrongful act, a company would fulfil this information obligation if a sign (with certain noticeable informative content) is located in a visible place.
- The use of sound recording devices, however, is more restrictive. Sound recording is only allowed for security and safety purposes and must comply with the principles of proportionality and minimum intervention.
- Companies must not place video cameras or sound recording devices in resting or leisure areas.
- The use of geolocation devices (e.g., Global Positioning System) must follow the same requirements as those for the use of video cameras. Companies are obliged to inform employees about their rights to access, rectify, restrict, process, and eliminate the data collected.

Role of Collective Bargaining Agreements

- Collective bargaining agreements (agreed between trade unions and employers associations at sector level or negotiated between employers and workers' representatives at company level) may establish additional guarantees with respect to processing personal data of workers and protection of digital rights.

Whistleblowing Provisions

- Companies may establish whistleblowing systems in which employees can report — anonymously, if necessary — any act or behavior in breach of company regulations, policies, or rules.
- Companies must preserve the identity and confidentiality of individuals affected by the information provided through the whistleblowing tool.
- As a general rule, access to data obtained from whistleblowing systems is limited to control and compliance functions. A company's human resources team can have access only when the process may result in disciplinary measures.

Data Protection Officer

- If the data protection officer (DPO) appointed is an employee, the DPO cannot be removed or sanctioned for the performance of his/her duties as DPO unless he/she acted intentionally or with gross negligence.

What Happens Next?

The Spanish Digital Rights Act is a significant development towards legal certainty on how employers can monitor employees' activity through company-issued digital devices, as well as on the use of video cameras, sound recording, and geolocation devices. The act is also a first step towards legalising the innovative right to digital disconnection for employees in Spain.

Some of the practical consequences of the Spanish Digital Rights Act remain unclear (sanctioning regime and effective role of workers' representatives), as well as whether additional guarantees will be implemented through collective bargaining agreements.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

[Naiara-Rodríguez Escudero](#)

Naiara.Rodriguez-Escudero@lw.com
+34.91.791.5110
Madrid

[Guillermo Ruiz de Salazar](#)

Guillermo.Ruiz-Salazar@lw.com
+34 91.791.5115
Madrid

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends.

The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's *Client Alerts* can be found at www.lw.com. If you wish to update your contact details or customize the information you receive from Latham & Watkins, visit <https://www.sites.lwcommunicate.com/5/178/forms-english/subscribe.asp> to subscribe to the firm's global client mailings program.