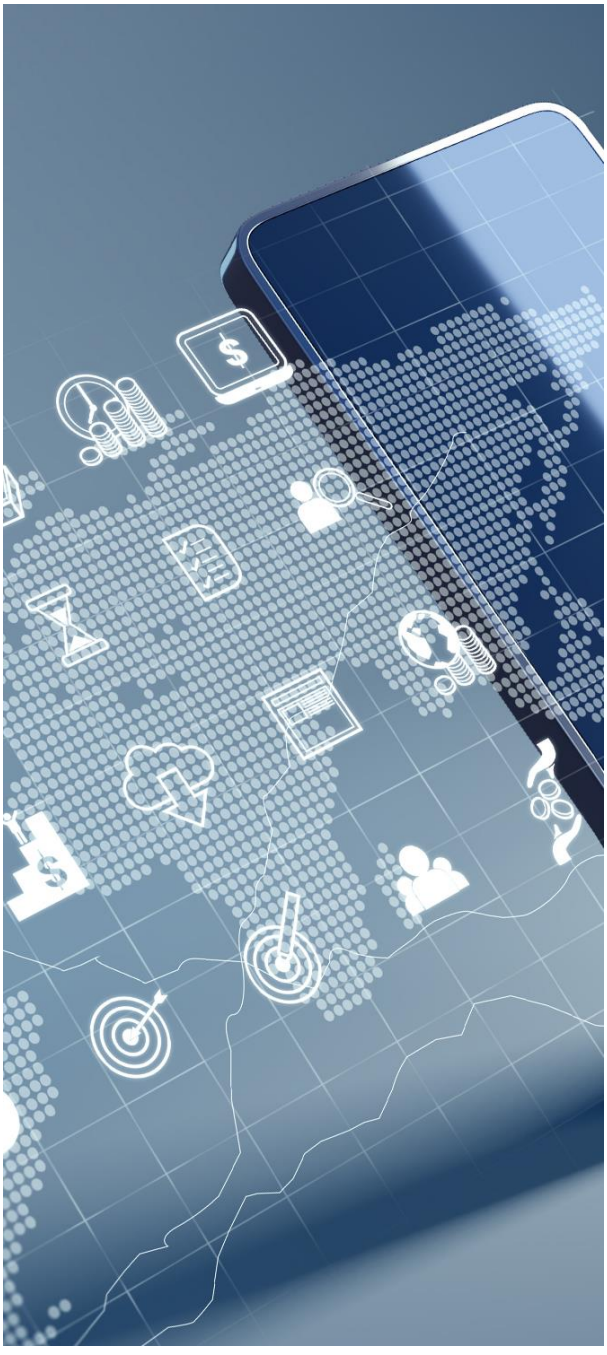
CUATRECASAS

New developments in Spain concerning data protection and labor relations

Legal Flash

June 10, 2021



The Spanish Data Protection Agency ("AEPD") has released a new guide on *data protection and labor relations* ("the Guide").

The Guide contains interpretative criteria that the AEPD and possibly the courts will apply to resolve conflicts that may arise, making it particularly valuable for all companies with a workforce.

This Legal Flash provides an executive summary of the 10 most controverted issues on the application of the data protection regulation in human resources, which the Guide aims to resolve.

1. Recruitment and social networks

- Companies can only process the personal data of employees and applicants they have sought through social networks, even if those individuals' profile on those networks is public, if there is a valid legal basis, the processing is related to professional activities, and it can be proven that the processing is necessary and relevant to the performance of the job.[1]

- Companies cannot send friend requests to employees or applicants to gain access to the content of their accounts, nor can they request any of the information these individuals share with other people on social networks.[2]

- With regard to job interviews, replies from applicants cannot be interpreted as consent to data processing. Therefore, any personal data collected through these means, whether directly or through deduction, cannot be subject to processing unless the company has a legitimate legal basis to process it. Otherwise, the company will be liable for an administrative offense and may be held in breach of fundamental rights.[3]

2. Collaboration between companies during the recruitment process (temporary employment agencies)

- Recruitment and placement agencies acting on behalf of clients will be considered data processors.
- When applicants are contacted before a specific job offer is made and an agency decides on the purpose and means of processing with no client instructions (at least initially), the agency will be acting as data controller.[4]
- Temporary employment agencies will act as data controllers as direct employers.

---

[1] One example would be a company following the LinkedIn account of a former employee with whom it had entered into a non-compete agreement to ensure the employee does not breach it.

[2] *Resolution 2/2017 of Article 29 Data Protection Working Party.*

[3] For example, if an employer asks an applicant during a job interview whether he or she intends to form a family or have children in the future and then collects that data, this could be considered a discriminatory act (judgment of the High Court of the Canary Islands, Labor Division (Santa Cruz de Tenerife), of April 7, 2014).

[4] Among other matters, this means that when agencies act as data controllers, they can only process the data of a particular applicant to enter into a contract with a particular client. Thus, once the position has been filled (and for which the agency was hired), the agency must destroy or return the processed data.

3. Whistleblowing procedures

- The legal basis for processing personal data collected through whistleblowing channels is reasons of public interest.
- The AEPD Guide underlines the fundamental need to previously inform whistleblowers and potentially accused persons that these systems exist and that data processing is carried out when an act is reported.
- Also, personal data stored in these systems may be transferred to a third party investigating the facts or to a third company investigating the reported act. The whistleblower and accused person must be notified of this data transfer.

- Reports may be made anonymously. Where a report is not anonymous, the whistleblower's privacy must be protected.

- Access to this data must be restricted to those in charge of internal monitoring and compliance, or to the designated data processor.

- In any case, data must be removed no later than three months from the date it was introduced in the whistleblowing system. There is no obligation to block the data unless the purpose for storing it is to leave evidence of the offense prevention template.

4. Working day register

- The legal basis for registering the working day is the legal obligation to keep a daily register of all employees' start and finish times.
- Workers must be informed of the existence of the register and the method used to register working hours. The Guide recommends that the working day register be as minimally invasive as possible. Also, it should not be accessible to the public or displayed in a visible location.

- Confidentiality of the data stored in the registry is essential. Access is only granted to persons authorized by law: workers involved, their legal representatives, and the

authorities if an investigation is carried out by the Labor and Social Security Inspectorate, for example, or if requested by a court.[5]

- It is explicitly stated that data collected through the working day register cannot be used for any other purposes, such as determining workers' location or tracking their geolocation. A remote working day register can be set up for workers that do not work at the company's premises through remote access to the corporate intranet or applications on digital devices.

5. Salary register

- In principle, the legal obligation to keep a salary register does not imply any data processing.

- However, in cases of professional groups or categories involving a reduced number of workers (e.g., management and senior positions) the Guide suggests implementing security measures, informing them of the processing (not of the information contained in the register) and the purpose, as well as ensuring the confidentiality of any information shared with the staff's legal representatives.[6]

- As regards consulting the salary register, companies must allow full access to the staff's legal representatives. If there are no legal representatives, workers are entitled to a restricted access.

6. Data transfers to other companies (company groups and outsourcing)

- Each of the companies making up a company group may be considered a data controller.

- In the case of outsourcing, the outsourcing company may transfer its staff's data to the main company, as long as there is a sound legal basis, deriving from the main company's subsidiary or joint and several liability.

---

[5] According to the Ministry for Labor's *Guide* on the working day register, "making this register information available does not entail the obligation to submit copies, unless agreed otherwise, and each individual worker should not be given an individual copy of his or her daily register, without prejudice to the worker being able access it for personal consultation. Neither should it be given to workers' legal representatives, which does not prevent them from being aware of workers' registers."

[6] In fact, the User Guide of the *Quantitative Analysis Tool per Gender of the Ministry for Equality* states that where only one person in an organization holds that position, that person's position should not be included for the purposes of disclosing his or her salary.

7. Video surveillance

- No consent is considered to have been granted for the processing of workers' personal data for video surveillance purposes to exercise the control functions of workers. In general, video surveillance systems can only be used when there is no other means available that would be less invasive of workers' privacy.

8. Geolocation

- Geolocation systems are can be used legitimately if they are installed on equipment belonging to the company (e.g., vehicles and digital devices).

- The Guide recommends that tracking systems be designed to register location data without providing all of the details to employers, and it confirms the unlawfulness of imposing an obligation on workers to provide personal means to facilitate geolocation (e.g., a personal cell phone).

9. Hiring a private investigator for surveillance

- Under labor law, companies are allowed to adopt control and surveillance measures of very different scope, including the possibility of hiring a private investigator. The AEPD highlights the need to act cautiously, always meeting the proportionality test, and that these investigations must respect workers' personal life.

10. Health surveillance

- With regard to health surveillance, personal data processing is justified by the existence of a contractual relationship and the company's obligation to fulfill its legal obligations.

- As well as drawing attention to the principles of confidentiality, information and proportionality, the Guide states that health surveillance may be mandatory under applicable legislation if a previous report is issued by the employees' legal representatives, and without the bargaining agreement being considered sufficient legal grounds, in the following cases:

  (I) When a medical examination is necessary to assess on an individual basis the effects of working conditions on workers.

  (ii) When a medical examination is necessary to assess whether a worker's state of health could pose a risk for other coworkers or persons related to the company.

(iii) When the company has the legal obligation to carry out this surveillance to ensure protection against specific risks and highly dangerous activities (occupational diseases).

- The medical examination must be linked to the conclusion on occupational fitness ("fit", "conditional fitness" or "unfit" for the worker's position), and the company cannot be given access to any other information, such as the specific medical diagnosis justifying that conclusion.

- With regard to Wearable technology, the AEPD specifies that, as a rule, it is forbidden to monitor health data using intelligent devices, such as bracelets and watches.

What happens now? Next steps

- Regulatory compliance with data protection legislation is particularly important in companies' day-to-day activities.

- Our team of lawyers specializing in labor and employment matters, data protection and new technologies advises companies to ensure full knowledge of all updates and how they affect labor relations, adapting employment contracts and company policies and procedures, and preventing potential penalties arising from non-compliance with the applicable legal regime and in cases of security breaches.

For more information on the contents of this Legal Flash regarding the interpretation of the AEPD's new Guide and how to implement it in the context of labor relations, please contact Cuatrecasas.