

## LEGAL UPDATE

# Personal Data Protection: What Every Employer Needs to Know

April, 2026

The amendments introduced by Law No. 21,719 to Law No. 19,628 on the Protection of Private Life (the “Law”), which take effect on December 1 of this year, will have a significant impact on employers in the area of human resources. Employing entities will need to adjust their practices and pursue a meaningful shift in the way they manage personal data of candidates, employees and former employees.

It is important to bear in mind that many of the obligations established by this reform are not entirely new, given that the current law already contains basic data protection principles and data subject rights. However, the fundamental difference lies in the fact that, until now, there was no specialized authority in charge of overseeing compliance. The amendments to the Law create the Personal Data Protection Agency (the “Agency”), an autonomous body with broad powers to supervise, initiate sanctioning proceedings -whether ex officio or at the request of a party- and impose significantly more severe penalties than those contemplated under the current regulations. In practice, this means that employers who were already processing personal data without fully complying with the existing law will now face a real risk of oversight and sanctions.

### 1. The employer as data controller

Every employing entity qualifies as a data controller, meaning it is the entity that defines the purposes and means by which the personal data of individuals linked to its organization are processed. By virtue of this status, the employer assumes direct responsibility for the processing of its employees’ personal data throughout the entire employment lifecycle, from the recruitment process through termination. This responsibility also extends to the data of candidates who participate in a recruitment process but are not selected for the position. As a consequence, the employer must comply with all principles, obligations and rights established by the Law regarding personal data protection.

### 2. What constitutes personal data and sensitive data?

- Personal data is any information that allows a person to be identified, directly or indirectly. For example, a person’s name, national identification number, contact details, data associated with physical identity, among others.
- Sensitive data is personal data that includes information about ethnic or racial origin, union or trade association membership, health status, biometric data, sexual orientation and gender identity, among others. The processing of such data is similar to that of personal data in general, but it benefits from certain particularities that afford it greater protection.

### 3. Principles governing the processing of personal data that the employer must know

Data processing is governed by principles that apply to all human resources operations, the most relevant for these purposes being:

**a) Lawfulness and fairness:** Data may only be processed lawfully and fairly, and the employer must be able to demonstrate compliance. This means processing data only when supported by a lawful basis established by the Law.

**b) Purpose limitation:** Data must be collected for specific, explicit and lawful purposes, and may not be used for different purposes.

**c) Proportionality:** Only the data strictly necessary should be processed, and it should be retained only for the time required.

**d) Security and confidentiality:** Appropriate technical and organizational measures must be implemented, and those who access the data must maintain confidentiality, even after the termination of the employment relationship.

**e) Transparency:** Data subjects must have permanent access to clear information about how their data is processed.

### 4. Lawful bases: when may personal data be processed?

The Law establishes that the data subject's consent is the general rule for processing personal data. However, it also recognizes other lawful bases that allow processing without consent. Therefore, in practice, it is advisable to rely on consent only when none of the other lawful bases is applicable. Some of these lawful bases apply to all types of personal data, while others apply only to data that is not classified as sensitive.

The most relevant lawful bases for the employer are:

- Performance or compliance with a legal obligation, or where the law provides for the processing.
- Performance of a contract between the data subject and the controller, or pre-contractual measures taken at the request of the data subject (for example, the performance of an employment contract and recruitment processes).
- Satisfaction of the legitimate interests of the controller or a third party, provided that the rights and freedoms of the data subject are not adversely affected (for example, the employer's legitimate interest in installing surveillance cameras in its offices, where the nature of the services rendered makes it necessary and the employees' rights and freedoms are not affected).
- Exercise of rights and compliance with obligations in the employment or social security context, when carried out within the framework of the law.

## 5. Rights of employees over their data

Employees, as data subjects, have inalienable rights that the employer must facilitate through simple and, as a general rule, free-of-charge mechanisms:

- **Access:** To know whether their data is being processed and to obtain a copy thereof.
- **Rectification:** To correct inaccurate or incomplete data.
- **Erasure:** To request the deletion of data when it is no longer necessary or has been unlawfully processed.
- **Objection:** To object to certain processing activities.
- **Portability:** To receive their personal data in a structured electronic format and to request its transfer to another controller.
- **Restriction of processing:** To suspend processing while a rectification, erasure or objection request is being resolved.

Failure to respond, a late response or an inadequate response to the exercise of these rights exposes the employing entity to complaints before the Agency, which could result in sanctions.

## 6. Key considerations to bear in mind

**a) Transparency:** The company must publish and keep permanently available its data processing policy, complying with the disclosures required by the Law.

**b) Security:** Employers must implement appropriate technical and organizational measures to safeguard the confidentiality, integrity, availability and resilience of their information systems. Such measures may include, among others, pseudonymization and encryption of personal data. In the event of a security breach affecting employee data, the employer is required to report the incident to the Agency. Furthermore, when the breach involves sensitive data or other circumstances established by law, the employer must also notify the affected employees directly.

**c) Privacy by design and by default:** From the planning stage of any process involving personal data, measures must be adopted to ensure that only the strictly necessary data is processed. This applies, for example, when designing job application forms, internal surveys or performance evaluation systems.

**d) Impact assessment:** When processing may pose a high risk to employees' rights, a prior impact assessment must be conducted. This is mandatory in cases of profiling with significant legal effects, large-scale data processing, systematic monitoring of publicly accessible areas, or processing of sensitive data when carried out on a lawful basis other than consent.

**e) Recruitment processes:** Data protection obligations also apply with respect to candidates. Once the process has concluded, data must be deleted when it is no longer necessary for the purpose that justified its collection. In order to store information gathered during the recruitment process and consider the candidate for a future opening, the candidate's consent must be obtained.

**f) Union membership:** The Law classifies union membership as sensitive data, which requires employers to place special emphasis on protective measures when managing this information, and means that only the lawful bases applicable to sensitive data may be used for its processing.

**g) Biometric and geolocation data:** The Law establishes specific regulations for both categories. Employing entities that use biometric attendance-tracking systems or that monitor the location of their employees must apply stricter security measures given the nature of the data.

**h) Former employee data:** The management of personal data does not end with the employment relationship. The Law requires that data be retained only for the time necessary to fulfill the purposes of the processing, after which it must be erased or anonymized. This obliges employers to define clear retention and deletion policies for former employee data, taking into account the statutory retention periods imposed by other regulations (for example, tax, social security or labor obligations). Additionally, specific regulations, such as those governing electronic attendance-tracking systems, set defined deadlines for employers to delete data once it is no longer necessary. It is advisable for employers to map the data retained after the termination of the employment relationship, identify the legal bases justifying its retention, and establish a periodic deletion schedule.

**i) Outsourcing of services and employee data:** The Law distinguishes two key figures when employee data is processed by third parties:

- **Mandate/processor:** This occurs when the employer entrusts a third party, for example, a *payroll* provider, a human resources management software vendor or a *pre-employment* screening service, to process data on its behalf and under its instructions. The third party does not acquire the status of data controller, because it acts as the employer's agent or processor and must use the data exclusively for the purposes of the engagement.
- **Transfer/assignment:** This involves transferring personal data to another controller, who will process it for its own purposes. In this case, the transferee acquires the status of data controller for all legal purposes. The transfer requires the data subject's consent, unless a legal exception applies, and must be documented in writing. In the human resources context, this figure may arise, for example, when employee data is shared with a related company that will use it for its own management purposes, or in a labor subcontracting scenario where the principal company requests data in exercise of its right to information.

**j) International transfers:** If the company transfers employee data to a parent company or subsidiaries abroad, it must rely on the regulations that allow such transfer. Accordingly, it must verify that the recipient country has adequate levels of protection or that appropriate safeguards are in place (contractual clauses, binding corporate rules or certifications), among others. Companies within the same group may rely on binding corporate rules approved by the Agency.

## 7. Infringement prevention model: an opportunity

The Law allows for the voluntary adoption of an infringement prevention model, the regulations for which must be incorporated into employment contracts, service agreements and/or the company's Internal Regulations on Order, Hygiene and Safety. Having a model certified by the Agency generates a positive reputational effect, as it is recorded in the National Registry of Sanctions and Compliance, and constitutes a mitigating circumstance when sanctions are determined. The compliance program must include, among other things, the appointment of a personal data protection officer, identification of the types of data processed and the associated risk activities, establishment of specific protocols to prevent infringements, implementation of internal reporting mechanisms and reporting to the Agency in the event of security breaches, and internal administrative sanctions and whistleblowing procedures for those who fail to comply with the system.

## 8. Sanctions

The Law establishes a three-tier sanctioning regime:

Level of Infringement	Sanction	Examples
Minor	Written warning or fine of up to 5,000 UTM (approx. USD 382,000).	Incomplete privacy policies; failure to respond in a timely manner to employee data requests.
Serious	Up to 10,000 UTM (approx. USD 764,000).	Processing without a lawful basis or consent; unauthorized data transfer; inadequate security measures.
Very Serious	Up to 20,000 UTM (approx. USD 1,528,000).	Fraudulent processing; deliberate breach of the confidentiality of sensitive data; knowingly processing minors' data in violation of the law.

In cases of recidivism, the Agency may impose up to three times the amount of the fine. For companies that do not qualify as small or medium-sized enterprises, recidivism in serious or very serious infringements may result in fines of up to 2% or 4% of annual revenue, respectively. Additionally, in the event of repeated very serious infringements within a 24-month period, the Agency may order the suspension of data processing operations for up to 30 days, renewable indefinitely. The Law also provides for civil liability for both pecuniary and non-pecuniary damages.



**B & E**

[www.bye.cl](http://www.bye.cl)