Compliance, internal whistleblowing channels and management of personal data

Consultation with the Spanish Data Protection Agency of 22 November 2021

Internal whistleblowing channels are playing an increasingly significant role in the area of compliance. Since 2010, the Criminal Code (article 31 bis) provides that legal persons may be exempted from liability (or, where appropriate, their liability may be mitigated) for certain offences committed by their directors, managers or employees, if they have adopted and effectively implemented appropriate "surveillance and control measures" prior to the commission of the offence. These measures are part of the so-called "crime prevention programmes" or "compliance systems". One of these measures is whistleblowing channels, which are used to report potential risks or breaches detected within the company.

According to the "Whistleblowing Directive" (Directive 2019/1937), private sector entities with over 50 employees as well as all public sector entities are obliged to have a whistleblowing channel. Although the deadline for implementing this Directive ended on 17 December and Spain has not yet done so, it is advisable that companies take the appropriate measures to comply with the provisions of this regulation, either by creating whistleblowing channels or, as the case may be, by adapting the existing ones to the new standards.

Whistleblowing channels and personal data

Rules, guidelines and directives have outlined how these channels should be organised. Organic Law 3/2018 on the Protection of Personal Data (article 24) regulates the processing of personal data through these channels. One key aspect is the period during which this data may be retained. According to the law, data must be deleted three months after it has been entered into the reporting system. However, in response to a query from the Spanish Compliance Association, on 22 November, the Spanish Data Protection Agency (AEPD) clarified that, if the complaint is considered well-founded and gives rise to a specific investigation, the data may be kept beyond this three-month period. However, in this case, the data must be retained in company's systems other than whistleblowing channels (e.g. at the compliance committee or the human resources management body).

The AEPD recalls that its guide on data protection in labour relations, dated May 2021, also analyses these and other relevant aspects. By way of example, the AEPD clarifies that it is essential that workers are informed about the existence of whistleblowing channels and the processing of the data involved in making a complaint. This information can be included directly in the employment contract or, for example, by means of information letters sent to the staff.