**How to establish a whistleblowing system under the Belgian Whistleblower Act:**

**On 28 November 2022, the Belgian legislator incorporated the provisions of EU Directive 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law into Belgian law. This legislation is commonly referred to as the 'Whistleblower Act' and aims to safeguard individuals ('whistleblowers') who expose wrongdoing in their organisation. The Whistleblower Act imposes specific obligations on companies, including the establishment of an internal reporting channel.**

**1. Format.** Companies are required to establish an internal reporting channel, which can take various forms, including a secure email address, an online portal, telephone, a confidential meeting, or mail. The company's social partners must be consulted in this regard. Additionally, companies must designate a responsable person, who is independent, to receive and appropriately address notifications.

Keep in mind that if your company engages an external service provider for the implementation of the whistleblowing system, it must formalize the necessary agreement in accordance with Article 28 of the GDPR. The service provider, as administrator of the whistleblowing system, is to be regarded as a data processor. Your company, holding the legal responsibility for implementing the system, assumes the role of the data controller.

**2. Policy.** Employees must be informed about the whistleblowing system in advance, both at collective and individual level, to ensure that they have a clear understanding of how to use the internal reporting channel and the processing of their personal data. A whistleblowing policy which is easy to understand and accessible is therefore a must-have. Make sure to include the below information in your whistleblowing policy.

**3. Scope.** The policy must comprehensively outline the scope of the whistleblowing system, in alignment with the fundamental principles of necessity and proportionality. The protection granted to whistleblowers under the Whistleblower Act specifically applies to reports involving significant breaches of crucial EU legislation that could significantly impact public interest (e.g., competition law, legislation on financial services, and environmental protection).

While the scope of your whistleblowing system can extend beyond these types of breaches, it is important to consider the advice of the Article 29 Working Party (predecessor of the European Data Protection Board), emphasizing the subsidiary nature of such systems. Consequently, the system should be reserved for reporting sufficiently serious matters that may not be appropriately addressed or surfaced through regular monitoring procedures.

**4. Confidentiality.** The confidentiality of the identity of the whistleblower, the report and the identity of the person about whom the report is made must be safeguarded to the greatest extent possible. Under all circumstances, the identity of the whistleblower should not be disclosed without his/her consent, except when required for the protection of the right of defence. That being said, the person about whom the report is made should be informed as soon as possible of the existence of the report and of the allegations made against him/her.

**5. Anonymous reporting.** Companies may allow anonymous reporting. Based on the opinion of the Article 29 Working Party (predating the Whistleblower Act), anonymous reports had to remain the exception. The starting point was transparent reporting with the guarantee of confidentiality without reprisals. The Whistleblower Act now explicitly allows anonymous reporting, but companies with fewer than 250 employees are not obliged to receive anonymous reports.

**6. Legal ground for data processing.** The Whistleblower Act unfortunately does not explicitly define the legal basis for processing personal data. We assert that the most suitable legal basis for such processing is the performance of a task carried out in the public interest, as outlined in Article 6.1(e) of the GDPR. Such task stems from the legal obligations set out in the Whistleblower Act. If the whistleblowing system extends beyond these statutory obligations, companies are required to conduct a careful balancing test to ensure that reliance on their legitimate interests and those of others can be used as legal basis, as outlined in Article 6.1(f) GDPR. In these instances, special consideration is essential when handling sensitive personal data and criminal information. It is imperative to note that explicit consent from the whistleblower is mandatory for audio recordings of reports in all circumstances.

**7. Record keeping and retention period.** Companies must keep a record of each report received. Reports must be kept for the duration of the employment relationship with the whistleblower. In addition, the name, function and contact information of the whistleblower, other protected persons and the person about whom the report is made must be maintained until the reported violation is time-barred.

In principle, the personal data included in the file must be deleted as soon as possible after the investigation is completed. According to the Article 29 Working Party, this must be done within a period of two months. If legal proceedings or disciplinary measures are initiated, the personal data may be kept until the relevant proceedings and time limit for filing an appeal has passed. In any event, if the report proves to be unfounded, the personal data must be deleted immediately.

**8. Data protection impact assessment.** The CNIL and the DSK, respectively the French Supervisory Authority and the Conference of German Supervisory Authorities, consider that a data protection impact assessment is necessary for the implementation of a whistleblowing system. In any case, it is appropriate to involve at least the DPO in the implementation of the whistleblowing system.



Julie Mannekens


Anouk Focquet


Karolien Francken


Morgane Smets