Newsflash Sapin II: Last call for the implementation of professional whistleblowing systems in 2018

All private organizations with at least fifty employees and some public organizations must set up a professional whistleblowing system by 01 January 2018 in accordance with Law no2016-1691 dated 09 December 2016 (Sapin II Law) and Decree No. 2017-564 dated 19 April 2017. The necessary system is very simple in its principles, but there are numerous requirements.

Submitted	28 November 2017
Applicable Law	France
Topic	Crime, Fraud & Investigations > Anti-money laundering, Bribery & corruption, Corporate manslaughter Employment, Pensions & Incentives Data Protection & Privacy

Contact	Etienne Kowalski, Laurence Renard, Sarah Bailey

The requirements of the “Single Authorization” of the “National Commission for Data Protection and Liberties” (CNIL) have been modified to take into account the Sapin II Law[1], those organizations required to establish whistleblowing systems can do so in accordance with Law no2016-1691 dated 09 December 2016 (Sapin II Law) and Decree No. 2017-564 dated 19 April 2017.

What are the requirements for data processing?

The law regulates the data which can be processed, and the conditions of that processing.

Only data objectively formulated and necessary to the processing of the alert are treated. These are listed by the CNIL. The Unique Authorization also specifies for how long the data is allowed to be stored, depending on their nature.

The key word of the whistleblowing system must be confidentiality. Therefore, internal procedures for receiving and processing the alert must be strictly monitored.

Furthermore, the identity of the whistleblower or of a person subject to an alert may be disclosed only under very restrictive conditions.

If a company sets up a whistleblowing system that does not strictly comply with the Unique Authorization’s provisions, it will not be able to use it. The company will then have to request a specific authorization, which is a much more complex and time consuming process in practice.

The Unique Authorization also covers the applicable provisions of the transfer of personal data outside the European

Union.

The entry into force of the General Data Protection Regulation on 25 May 2018 should not significantly change the organization of the whistleblowing systems. However, it is likely that the treatments implemented for whistleblowing systems will be considered as of high risk for the rights and freedoms of people, thus falling within the scope of the impact assessments provided for in Article 35 of the General Regulation.

What are the organizational constraints?

There are many different frameworks which can be chosen to set up an internal whistleblowing system.

An alert is brought to the attention of the direct or indirect manager, the employer or a third party appointed by the employer. In any case, it is necessary to identify the recipient for alerts. This can be a third party, whose role can merely be to receive the alert, or can extend to dealing with the alert.

It may be useful for the organization itself to manage the examination and handling of the alert. Indeed, if the alert leads to an internal investigation, the composition of the internal investigation team must be thought through beforehand, and must be compliant with the policies of the company. It may be necessary to seek external advice.

Lastly, the employees themselves as well as external and temporary third parties must receive information about the implemented whistleblowing system collectively and at an individual level.

This information may occur retrospectively for a person who has not been told about the existing whistleblowing system (article 9).

Furthermore, the employee representative committee (soon to be "social and economic committee") must be consulted and informed before setting up the whistleblowing system.

Anyone who meets the definition of a whistleblower has a protective status within the company.

What are the risks for not setting up such system?

The Sapin II Law does not provide for a specific penalty if a whistleblowing system is not set up, or if the procedure does not comply with legal requirements.

However, if a whistleblowing system is not in accordance with the Law (no2016-1691 dated 09 December 2016) and the Decree (no2017-564 dated 19 April 2017), a company or its directors could be held liable for:

- obstacle to an alert (article 13 of the Law), penalized by one years' imprisonment and a fine of €15,000.00
- lack of confidentiality (article 9 of the Law), penalized by two years' imprisonment and a fine of €30,000.00, and
- lack of whistleblowing system for corruption (only if the company has more than 500 employees and more than 100 million euros of turnover, article 17 of the Law): the French anticorruption Agency may require the company to comply, issue a warning, and the Sanction Commission of the Agency may finally inflict a financial penalty (€200,000 for individuals, €1,000,000 for companies).

The French anticorruption Agency has included in its self-assessment questionnaire, put online in October 2017, the professional whistleblowing system as a tool to fight against corruption.

If a company does not set up a whistleblowing system, there is also a risk that the whistleblower will instead approach the administrative or judicial authorities, or even go public with their information.

Furthermore, if a company sets up a whistleblowing system that is not in accordance with the CNIL's Unique Authorization with regards to data processing and if it did not obtain a specific authorization to implement such system, it could be penalized for infringement of human rights resulting from data processing as set up in article 226-16 of the French Criminal Code, and penalized by five years' imprisonment and a fine of €300,000 for individuals, which may be increased to fivefold for companies.

---

[1] Deliberation no2017-191 dated 22 June 2017 amending Decision no2005-305 dated 08 December 2005 on the single authorization for the automatic processing of personal data implemented in the framework of professional whistleblowing systems (AU-004), published on 25 July 2017.

elexica Limited, CityPoint, One Ropemaker Street, London EC2Y 9SS