SAPIN II: WHAT RECOMMENDATIONS SHOULD BE FOLLOWED FROM 2021 ONWARDS?

Date: 13 April 2021

French Data Protection, Privacy, and Security and Labor, Employment and Workspace Safety Alert

By: Claude-Étienne Armingaud, Christine Artus, Alexia Montagnon, Clara Schmit, Natacha Meyer

The French Law n°2016-1691 of 9 December 2016 relating to transparency, the fight against corruption, and the modernization of economic life, known as the "Sapin II" Act,[1] introduced to legal entities additional compliance requirements to address corruption in order for France to meet the highest European and international standards.

Sapin II has established a general principle of prevention and detection of corruption risks under the control of a national anticorruption structure, the French Anti-Corruption Agency (AFA), whose main mission is to help economic and public players in the process.

The AFA noted in its 2019 annual activity report[2] that anticorruption measures implemented by economic and public players were still incomplete.

On 12 January 2021, the AFA published new recommendations entered into force on 13 January 2021 (Recommendations, here in French).

The AFA specifies the practical procedures for implementing an anticorruption system structured around three foundational principles, namely:

- Governing body's commitment;
- Understanding the entity's exposure to probity risks; and
- Risk management.

WHO IS THIS ADDRESSED TO?

The AFA urges all entities to implement an anticorruption process, independently of the thresholds required under Sapin II. According to the AFA, an adaptation of these Recommendations remains necessary in light of the potential risks and activities of each entity. In concrete terms, each organization has an interest in protecting itself against the risks of probity breach and the resulting criminal risks.

Pursuant to Article 17 of Sapin II, relevant companies with at least 500 employees and recording a turnover exceeding EUR 100 million have the obligation to implement a program to prevent and detect corruption and influence peddling through eight internal preventive measures.[3] In these Recommendations, the AFA thus advises private companies subject to the prevention obligation of article 17 of Sapin II to include a wide range of criminal offences beyond corruption and influence peddling in their internal system and specifies that the actions to be implemented should be based on a genuine commitment by each company's governing body.

Governing bodies have a key role in the process of integrating anticorruption measures into risk procedures and policies and must be supported by nonexecutive bodies and compliance teams.

REINFORCEMENT AND FORMALIZATION OF THE ANTICORRUPTION SYSTEM

In order to encourage the various stakeholders to make up for the highlighted shortcomings and to abide by the established procedures, the key word in the AFA's Recommendations is “formalization.”

In this context, risk-mapping methods should be refined. Each company will have to draw up a risk map in the form of written and structured documentation, detailing the underlying methods used to draw it up, measures adopted to control the risks, and roles and responsibilities of each party involved.

The FA applies the same standards to internal whistleblowing systems, which are described for the first time in the Recommendations. Companies will therefore have to formalize their internal investigation procedure, providing at the very least the criteria required to trigger an alert and the methods used to carry out the investigation. Following the investigation, a report will have to be drawn up and a dedicated committee set up.

The integrity evaluation of third parties is not exempt from this formalization requirement. While this procedure is not new,[4] it must now be carried out within a formal framework, as it is specified that the determination of information and documents useful for the evaluation of third parties must be carried out by the company at the risk-mapping stage, taking into account the obligations prescribed by General Data Protection Regulation (GDPR).[5]

Following its willingness to truly involve corporate governing bodies in implementation of the anticorruption system, the AFA recommends that, in the context of human resources management, the recruiting process for the most exposed executives and staff should include an assessment of their “honorability.”

The applicability of GDPR to these procedures is all the more to be anticipated insofar as the AFA recommends identifying certain types of personal data relating to employees working on behalf of clients, suppliers, or intermediaries of the companies who are evaluating third parties.

Therefore, and as per GDPR's data minimization principle,[6] only the data strictly necessary to achieve the purposes of Sapin II may be collected and processed by the companies concerned. In the same way, physical, logical and organizational security measures shall be implemented to ensure the security and integrity of the data collected during the evaluation.[7]

Furthermore, individuals subject to an integrity evaluation will have to be informed[8] of the specifics of the processing operations pertaining to their personal data, as well as their rights regarding such data.[9] Finally, as the verification of the integrity of third parties may be carried out due to their presence or absence on sanction lists, the impacted stakeholders will need to implement special measures to ensure the protection of these special categories of personal data (known as “sensitive”) under GDPR.

Similar attention will need to be drawn to personal data relating to disciplinary sanctions identified by private companies and public entities alike. The Recommendations clarify the regime applicable to disciplinary sanctions by providing, without much novelty, for the principle of gradation of sanctions. While the AFA calls on governing bodies to be strict and to sanction breaches of anticorruption measures, it also requires that the dissemination of these sanctions internally, as a reminder of the zero-tolerance policy, be carried out while preserving the anonymity of third parties at all costs.

Through the Recommendations, the AFA aims at reconciling the need to provide for limited retention of personal data[10] with the need for companies and public actors to be able to justify their decisions in the event of controls or audits. Finally, the same principles resulting from the application of GDPR will have to be respected within the framework of the implementation of whistleblowing systems by companies and public players, with a particular attention to the automated processing of such alerts.

Although the AFA is increasing its knowledge of the rules of the GDPR through its controls, it is unfortunate that the AFA did not consult the French Data Protection Authority (CNIL) to propose a turnkey compliance framework for impacted companies. Failing this, companies will have to determine themselves the operational methods that will best meet the dual compliance requirements vis-à-vis the AFA and the CNIL.

INVITATION FOR COMPLIANCE

These Recommendations are not binding or obligatory for the different entities but enforceable by the AFA in its control activities. The AFA will refer to the Recommendations for audits that will begin six months after their entry into force, i.e., as of 13 July 2021.

Following a recommendation of the Enforcement Committee,[11] the AFA specifies that entities which have indicated that they comply with the Recommendations will benefit from a compliance presumption, which can only be overturned by the AFA's demonstration of ineffective, incorrect, or incomplete implementation of the Recommendations. Otherwise, it will be up to the organization to demonstrate that the choices it made effectively allowed it to meet the regulatory requirements.

Each entity will also be invited to update its internal compliance procedures. Irrespective of the health crisis managements, integrating compliance tools has become a new challenge for 2021, since failure to comply with the Recommendations could be enforced in the context of an audit. The AFA is in line with the current trend of accountability frameworks, meaning that strict legal compliance is no longer sufficient. Such companies must also be able to document this compliance and the decisions taken to implement it.

In addition to the criminal sanctions resulting from acts of corruption, influence peddling, and similar offences, the AFA is able to adopt similar sanctions for failure to comply with the obligations arising from Sapin II following the submission of a request to its Enforcement Committee.

After the person concerned has been given the opportunity to present its observations, such commission may order the company to adapt its internal compliance procedures as per the recommendations it addresses to them within a period that must be shorter than three years.

The Enforcement Committee may also impose a financial penalty of up to EUR 200,000 for individuals and EUR 1,000,000 for legal entities and, finally, order the publication, distribution or posting of its decision. These sanctions remain without prejudice to possible additional sanctions by the CNIL regarding GDPR breaches, up to €20 million or 4 percent of companies' overall turnover (whichever is greater), even in cases where there was compliance with the Recommendations.

This invitation for compliance is a reminder of the European Union's willingness to standardize the different anticorruption measures of the member states. The implementation of the whistleblowing directive[12] by EU member states will need to be effective before 17 December 2021 and will bring some changes to Sapin II, notably by giving up the notion of a “disinterested act,” thus broadening the spectrum of prohibited retaliation

measures or authorizing public disclosure. The various private or public stakeholders will benefit from a grace period to update their anticorruption measures, beginning when the Recommendations are transposed.

K&L Gates' multidisciplinary labor and data protection law teams remain available for more information and to anticipate and implement your company's compliance.

FOOTNOTES

[1] Sapin II entered into force on 10 December 2016 (JORF n°0287 of Dec. 10, 2016).

[2] FRENCH ANTI-CORRUPTION AGENCY, ANNUAL ACTIVITY REPORT 2019 (July 7, 2020) (in French).

[3] As per Article 17, II of Sapin II, this obligation would require the implementation of a specific French Code of Conduct, an internal whistleblowing procedure, a risk mapping, integrity evaluation of third parties, internal or external accounting control procedures, training program for employees, disciplinary sanctions, and an internal control and audit process.

[4] Article 17, II, 4° of Sapin II.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter GDPR).

[6] Article 5 of GPDR.

[7] Article 32 of GDPR.

[8] Article 13 of GDPR.

[9] Article 12 of GPDR.

[10] Article 5 of GPDR.

[11] French Anti-Corruption Agency, Decision no. 19-01 Société S SAS and Mme C. (July 4, 2019).

[12] Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 on the protection of persons reporting violations of Union law, 2019 O.J. (L 305) 17.

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

CHRISTINE ARTUS
PARTNER

PARIS
+33.1.58.44.15.38
CHRISTINE.ARTUS@KLGATES.COM

