sebia

## PROFESSIONAL ALERT SYSTEM

# PROCEDURE FOR THE COLLECTION OF ALERTS

### INTRODUCTION

The company has subscribed to the alert system, **ethicorp. com**.

This system is part of the company's ethical approach, which aims to establish and maintain a culture of integrity, transparency and propriety.

The purpose of this procedure is to recall the legal framework for alert systems, the rights, guarantees and duties of whistleblowers and facilitators, and the principles and operating methods of the system.

It is complemented by precise instructions for use of the system as well as by dedicated training courses.

### Article 1. LEGAL FRAMEWORK FOR THE IMPLEMENTATION OF THE WHISTLEBLOWING SYSTEM

**Law n°2016-1691 of 9 December 2016**[1] on transparency, the fight against corruption and the modernisation of economic life, known as the Sapin II Law, was revised by **Law n°2022-401 of 21 March 2022** aimed at improving the protection of whistleblowers, which gave rise to **Decree n°2022-1284 of 3 October 2022** relating to the procedures for collecting and processing whistleblower reports.

The revised Sapin II law includes **two** additional **provisions** requiring the establishment of reporting systems:

- Article 8, I. B: "*The **following are required to establish an internal procedure for collecting and processing alerts**, after consultation with the social dialogue bodies and under the conditions laid down by decree in the Council of State*
  *1° Legal persons governed by public law employing at least fifty staff members, with the exception of municipalities with fewer than 10,000 inhabitants, public establishments attached to them and public establishments for inter-municipal cooperation which do not include among their members any municipality exceeding this population threshold.*
  *2° State administrations.*
  *3° Legal persons under private law and enterprises operated in their own name by one or more natural persons, employing at least fifty employees.*
  *4° Any other entity falling within the scope of the European Union acts mentioned in Part I B and Part II of the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting violations of Union law.*"
- Article 17, II: *"The persons mentioned in I*[2] *shall implement (...) an **internal whistleblowing system designed to enable the collection of reports** from employees concerning the existence of conduct or situations contrary to the company's code of conduct*.

In accordance with the Recommendations of the French Anti-Corruption Agency[3] , it is possible to set up a single technical system for collecting alerts common to both provisions.

---

[1] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033558528

[2] Article 17, I: *"the chairmen, managing directors and managers of a company employing at least five hundred employees, or belonging to a group of companies whose parent company has its registered office in France and whose workforce comprises at least five hundred employees, and whose turnover or consolidated turnover is greater than 100 million euros"*

[3] https://www.economie.gouv.fr/files/files/directions_services/afa/2017_-_Recommandations_AFA.pdf

The implementation of alert systems is also governed by:

- The European Parliament's **General Data Protection Regulation (GDPR)** of 14 April 2016.
- Law No. 78-17 of 6 January 1978 on **information technology, files and freedoms** (revised in accordance with the provisions of the RGPD).
- The **Recommendations of the French Anti-Corruption Agency** (AFA)[4] .

**Important: Any person who obstructs, in any way whatsoever, the transmission of an alert is punishable by one year's imprisonment and a fine of €15,000 (€75,000 for legal persons).**

### Article 2. DEFINITION OF WHISTLEBLOWER - OPENING OF THE SYSTEM

Article 6 of the revised Sapin II Law defines the whistleblower:

> *"A whistleblower is a natural person who reports or discloses, without direct financial consideration and in good faith, information concerning a crime, an offence, a threat or harm to the general interest, a violation or an attempt to conceal a violation of an international commitment duly ratified or approved by France, of a unilateral act of an international organisation taken on the basis of such a commitment, of the law of the European Union, or of the law or regulations. Where the information was not obtained in the course of the professional activities mentioned in Article 8(I), the whistleblower must have had personal knowledge of it.*

Thus, the whistleblower must be:

- A **natural person** - this cannot be a legal person, i.e., a company, an association or even a trade union.
- **Without direct financial compensation** - in France whistleblowers are not paid.
- **In good faith** - the whistleblower must not act maliciously or with vengeance by spreading information that he or she knows to be false or erroneous.
- Where the information was not obtained in the course of professional activities, the whistleblower must have personal knowledge of the information, i.e., he or she must have **personally witnessed** the facts (or been the victim) - the whistleblower may not simply spread a rumour.

It is under these conditions that the whistleblower will benefit from the full protections guaranteed by the law (see below the article "**Protections for whistleblowers**". Otherwise, in particular in the case of bad faith, spreading rumours or defamatory facts, he or she will be liable to sanctions.

The right to lodge an alert is legally open:

- To staff members,
- To persons whose employment relationship has ended, where the information was obtained in the course of that relationship,
- To persons who have applied for a job in the entity concerned, where the information was obtained in the course of that application.
- To shareholders, partners and holders of voting rights in the general meeting of the entity.
- To the members of the administrative, management or supervisory body.
- To external and occasional collaborators.
- To contractors of the entity concerned, their subcontractors or, in the case of legal persons, to members of the administrative, management or supervisory bodies of such contractors and subcontractors,
- As well as to the staff members of co-contractors and subcontractors.

[4] See above

### Article 3. WHO TO ALERT?

The whistleblower has **three distinct channels** for reporting while benefiting from the protections granted by law to this status:

- **Internal reporting**: the whistleblower chooses to report internally to his/her hierarchy or via the ethicorp.com platform,
- **External reporting**: the whistleblower may address his or her alert to a competent authority (listed by decree), to the Defender of Rights, to the judicial authority or to any competent institution, body or agency of the European Union, either after an internal alert or directly, when he or she considers that it is not possible to remedy the violation effectively by an internal alert or that he or she is not exposing himself or herself to a risk of reprisals
- **Public disclosure**: The whistleblower may finally make the alert public, either for the whistleblower who obtained the information in the course of his or her professional activities in the event of imminent or obvious danger to the public interest, or if the external alert has not been followed by any appropriate measure within the set time limits, in the event of serious and imminent danger or when referring the matter to the competent authority would put the whistleblower at risk of reprisals or would not allow for the situation to be remedied effectively.

**In order to provide the highest guarantees of impartiality and independence, the company has chosen ethicorp. com as its referent, accessible at https://www.ethicorp.com/sebia .**

This platform for receiving and processing alerts is entirely managed and administered by **lawyers**, independent regulated professionals who are bound by strict ethical and disciplinary obligations, particularly with regard to confidentiality and professional secrecy.

**ethicorp. com** thus has, through its positioning, the competence, the authority and the means sufficient to carry out its missions.

### Article 4. WHAT TO REPORT: THE FACTS OF THE ALERT

In accordance with the law, an alert may relate to:

- A **crime or misdemeanour**
- A **threat or harm to the public interest**
- A **violation or an attempt to conceal a violation**
    - **An international commitment regularly ratified or approved by France.**
    - **Or a unilateral act of an international organisation taken on the basis of such a commitment.**
    - **Or European Union law, statute or regulation.**
- **Failure to comply with the Anti-Bribery Code of Conduct** (where section 17 of the Act applies).

**The alert may relate to events that have occurred or are very likely to occur.**

**Some examples:**

- Misuse of corporate assets
- Hygiene violations
- Bleaching
- Unfair competition
- Conflicts of interest
- Private bribery
- Public corruption
- Obstructionist offences
- Embezzlement
- Discrimination
- Scam
- Favouritism
- Fraud against the president / supplier
- Tax evasion
- Bullying
- Sexual harassment
- Computer intrusion
- Protection of personal data
- Radicalisation and terrorism
- Sectoral regulations (insurance, mutual insurance, social security)
- Industrial risk
- Employee safety and accidents at work
- Breach of confidentiality - secrecy
- Violence - aggression
- Flights

- etc.

In case of doubt, it is better to use the system than to take the risk that a serious and underestimated fact will not be revealed. Lawyers working through **ethicorp.com** have the necessary expertise to examine the alert and assess its appropriateness.

### Article 5. CONFIDENTIALITY

In accordance with Article 9 of the Act of 9 December 2016, *"The procedures implemented to collect and process alerts, under the conditions mentioned in Article 8, shall guarantee strict confidentiality of the **identity of the authors of the alert, of the persons concerned by it and of any third party mentioned in the alert and of the information collected by all the recipients of the alert**."*

The following must therefore remain strictly confidential

- **The identity of the whistleblower**, who must be able to file his or her alert in complete peace of mind.
- **The identity of the person concerned** by the alert and of **any third party mentioned** in the alert.
- **The information gathered in the** context of the alert, i.e., the facts that are the subject of the alert.

The latter two elements (identity of the person concerned and of any third party mentioned in the alert and information gathered in the context of the alert) will in practice only be transmitted to the Ethics Committee and to the persons in charge of investigating the facts.

The CNIL specifies in its deliberation of 18 July 2019 concerning external data processors that "*The referent or service provider* [...] *undertakes in particular, by contractual means, not to use the data for purposes other than the management of alerts, **to ensure their confidentiality** [...]*"

Furthermore, the whistleblower cannot himself freely disclose the information that is the subject of the whistleblowing.

**Important** - Any violation of the confidentiality of the alert is punishable by **two years imprisonment**, and **a fine of 30,000 euros** (**150,000 euros** for legal persons)[5] .

**Possible anonymity of the whistleblower**

The CNIL (deliberation of 18 July 2019) recommends that the organisation should not encourage people who are to use the system to do so anonymously. However, their identity is treated as **confidential**.

As an exception to the principle of identifying oneself, the CNIL specifies that the alert of a person who wishes to remain **anonymous** may be processed under two cumulative conditions:

- **The seriousness of the facts mentioned is established and the facts are sufficiently detailed**, so it will be essential to be precise in the description of the facts.
- **Special precautions are** taken when dealing with alerts, in particular prior examination by the first recipient of the alert of the appropriateness of its dissemination, which is in principle the case with lawyers working via the **ethicorp. com** platform.

If these conditions are not met, the lawyers intervening via **ethicorp. com** may inform the whistleblower that he or she must identify himself or herself (exclusively to ethicorp. com and under guarantee of confidentiality) or that, failing this, the whistleblower's case cannot be processed.

[5] Article 9, II of the law of 9 December 2016

In practice, if the whistleblower provides his or her identity, only **ethicorp. com** will be informed, and **the identity will not be transmitted or revealed to the employer**. **ethicorp. com** will only transmit, under the strict conditions of the law mentioned *above*, the facts that are the subject of the whistleblower's report and the identity of the person concerned, to allow the internal investigation of the facts. The company has also contractually agreed with **ethicorp. com not** to request or attempt to seek the identity of the whistleblower.

Finally, to avoid any concerns, it is recommended not to use company equipment to log on to the **ethicorp. com** platform or to use your company email address to create your whistleblower account.

### Article 6. THE PROTECTIONS AND DUTIES OF THE WHISTLEBLOWER

In accordance with Article 10-1 and 12 to 13-1 of the revised Sapin II law, the whistleblower is **protected against any retaliatory measure**.

Article L. 1121-2 of the Labour Code:

> *"No person may be excluded from a recruitment procedure or from access to an internship or a period of vocational training, no employee may be sanctioned, dismissed or be the subject of a direct or indirect discriminatory measure, particularly with regard to remuneration, within the meaning of Article L. 3221-3, profit-sharing measures or the distribution of shares, training, reclassification, assignment, qualification, classification, professional promotion, working hours, evaluation of work, etc. 3221-3, profit-sharing measures or the distribution of shares, training, reclassification, assignment, qualification, classification, professional promotion, working hours, performance assessment, transfer or renewal of contract, nor any other measure mentioned in II of Article 10-1 of Law 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life, for having reported or disclosed information under the conditions provided for in Articles 6 and 8 of the same law. "*

Article L. 1132-3-3 of the Labour Code:

> *"No person who has testified, in good faith, to facts constituting a misdemeanour or a crime of which he or she has become aware in the exercise of his or her duties, or who has reported such facts, may be subject to the measures mentioned in Article L. 1121-2.*
>
> *The persons mentioned in the first paragraph of this article shall benefit from the protections provided for in I and III of Article 10-1 and Articles 12 to 13-1 of Law No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life."*

Art. L. 1152-2 of the Labour Code

> *"No person who has suffered or refused to suffer repeated acts of psychological harassment or who has, in good faith, reported or testified to such acts may be subject to the measures mentioned in Article L. 1121-2.*

Retaliation against a whistleblower is also an offence of discrimination under Article 225-1 of the Criminal Code.

The whistleblower also benefits, in certain cases and under certain conditions, from **criminal and civil irresponsibility**.

Indeed, according to Article 122-9 of the Criminal Code:

> *"**A person who breaches a secret protected by law** shall not be criminally liable, provided that such disclosure is **necessary and proportionate to the safeguarding of the interests in question, that it takes place in compliance with the conditions for reporting defined by law and that the person meets the criteria for the definition of a whistleblower** provided for in Article 6 of Law No. 2016-1691 of 9 December 2016 on transparency, combating corruption and modernising economic life.*

> *Nor shall a whistleblower be held criminally liable if he or she **removes, misappropriates or conceals documents or any other medium containing information of which he or she has lawful knowledge** and which he or she reports or discloses under the conditions referred to in the first paragraph of this Article.*
>
> *This article shall also apply to the accomplice to these offences.*

By way of exception, the alert may not concern elements covered by national defence secrecy, medical secrecy or the secrecy of relations between a lawyer and his client, as well as the secrecy of investigations, instructions or judicial deliberations.

Moreover, Article 10-1 of the Sapin II Law provides, since the entry into force of Law n°2022-401 of 21 March 2022 aimed at improving the protection of whistleblowers[6] , for civil irresponsibility of whistleblowers who have chosen to make a public disclosure, under certain conditions:

> *"Persons who have reported or publicly disclosed information as provided for in Articles 6 and 8 shall not be civilly liable for damage caused by their reporting or public disclosure **if they had reasonable grounds for believing, at the time of reporting or public disclosure, that the reporting or public disclosure of the entirety of the information was necessary to protect the interests involved**.*

Article 6-1 of the Sapin II Law specifies that the status of whistleblower and the protections that flow from it also benefit[7] :

- Facilitators, i.e., any natural person or any non-profit legal entity (e.g., an association or a trade union) who assists a whistleblower in making a report or disclosure in accordance with the provisions of the Sapin II Law.
- Individuals who are related to the whistleblower and who are themselves at risk of retaliation.
- Legal entities controlled (within the meaning of Article L.233-3 of the French Commercial Code) by the whistleblower and with which he or she works or has a professional relationship.

This protection only applies if the whistleblower complies with the framework set out in Articles 6 to 8 of Law 2016-1691 of 9 December 2016.

**These whistleblower protections are accompanied by duties. The whistleblower will not be protected if he or she does not meet the legal definitions and in particular if he or she declares facts in bad faith and/or of which he or she would not have had personal knowledge when the information was not obtained in the course of his or her professional activity. He would then be exposed to civil and penal sanctions, notably for defamation or slander.**

### Article 7. THE RIGHTS OF THE PERSON WHO IS THE SUBJECT OF THE ALERT

The person concerned by the warning is entitled to respect for his or her strict confidentiality, particularly with regard to the fundamental principle of the presumption of innocence and the right to defence.

The elements likely to identify him or her may only be disclosed, except to the judicial authority, once it has been established that the alert is well founded. In other words, the company will conduct an internal investigation, bearing in mind that "*personal data must only be made accessible to persons authorised to know about it in the light of their duties*" (CNIL Deliberation of 18 July 2019), and/or will refer the matter to the judicial authority.

The person who is the subject of a warning (as a witness, victim or alleged perpetrator) must, in accordance with Article 14 of the GDPR, be informed by a warning within a reasonable period of time, which may not exceed **one month**, following the issue of a warning.

---

[6] LAW No. 2022-401 of 21 March 2022 to improve the protection of whistleblowers (1) - Légifrance (legifrance.gouv.fr)

[7] Article 2 of the law of 21 March 2022

However, according to Article 14-5-b of the RGPD, this information may be withheld when it is likely to "*seriously jeopardise the achievement of the purposes of the processing operation*". This could be the case, for example, where disclosure of the information to the data subject would seriously jeopardise the needs of the investigation, for example where there is a risk of destruction of evidence. However, the information must be provided as soon as the risk has been averted and must not contain information about the identity of the person who issued the alert or of third parties.

However, when a disciplinary sanction or litigation procedure is initiated against the person concerned as a result of the alert, the latter may obtain the communication of these elements by virtue of the rules of ordinary law (rights of defence in particular).

This possibility is nevertheless conditional on appropriate measures being taken to protect the rights and freedoms and legitimate interests of the data subject.

In accordance with the CNIL's decision, the information provided must mention the existence of the processing operation, its characteristics (in particular the purposes for which it is used, the types of data likely to be included, the types of persons likely to issue the alert or to be the subject of the alert, the main stages of the procedure triggered by the alert, the length of time for which the data is kept, etc.) and the rights available to the person concerned by the alert.

## Article 8. FILING, PROCESSING AND FOLLOW-UP OF THE ALERT - PRACTICAL ARRANGEMENTS

The **ethicorp. com** platform is accessible via the Internet at the secure address https://www.ethicorp.com. Except for maintenance, it is accessible 24 hours a day, 7 days a week, 365 days a year.

To avoid any privacy concerns, it is recommended that you do not use company equipment to connect.

**Creating a whistleblower account**

On the platform, the whistleblower will be invited to create a personal whistleblower account before being able to submit his or her alert.

To do so, he/she must fill in the Corporate Code that the company will have communicated to him/her (corporate code: @SILVER91). This code ensures that the alert is related to the company, as **ethicorp. com** does not deal with alerts relating to companies that are not members of its services.

The whistleblower will also have to provide his/her name and surname (unless he/she chooses to remain anonymous, under the conditions recalled in the "**Confidentiality**" article), as well as an email and a password.

It is recommended, again for reasons of confidentiality, not to use a business email address.

In any event, **ethicorp. com** will keep strictly confidential any element that could identify the whistleblower, including his/her email address.

After validating this information, the whistleblower will receive an email containing no confidential data, asking him/her to click on a specific web link to verify that the email entered really exists.

Once this process is complete, the whistleblower's account is active, and will allow the whistleblower to file, view and complete alerts, as well as communicate with **ethicorp. com**'s lawyers in complete confidentiality.

**Filing the alert**

The whistleblower, via his account opened on the **ethicorp. com** platform, can file his alert in complete confidentiality.

He/she is asked to describe, in free text, the facts and information he/she has personally witnessed.

He/she may attach documents to support the alert, if available.

In order to submit his alert, he finally validates his knowledge of a detailed warning reminding him of his rights and duties and the legal framework of an alert.

The whistleblower will immediately receive an acknowledgement of receipt of his or her alert, via an e-mail containing no confidential data and specifying the alert identifier.

At the same time, the alert is received by one of the lawyers involved via the **ethicorp. com** platform, who will ensure its analysis and processing.

The whistleblower will be informed on his or her whistleblower account of the basic steps in the follow-up of the whistleblowing: opening of an investigation, of a procedure, as well as possibly of its closure, for example if the facts are not characterised. This information will not, of course, give the whistleblower access to confidential information that would be obtained in the course of the investigation or the procedure that would follow the alert.

The whistleblower may at any time consult the status of his or her alert, as well as clarify or complete it, or even file another alert, by logging into his or her whistleblower account with the e-mail address and password that he or she will have entered when opening the account.

**ethicorp. com**'s lawyers may need to contact the whistleblower to ask him/her to clarify his/her alert, to provide additional information, or to inform him/her of the follow-up. The whistleblower will then receive an email containing no confidential data, asking him/her to log in to his/her account to read the message intended for him/her.

The details of how the platform works, including a description of each step, are contained in the instructions for use that the employer makes available to employees and external and occasional collaborators.

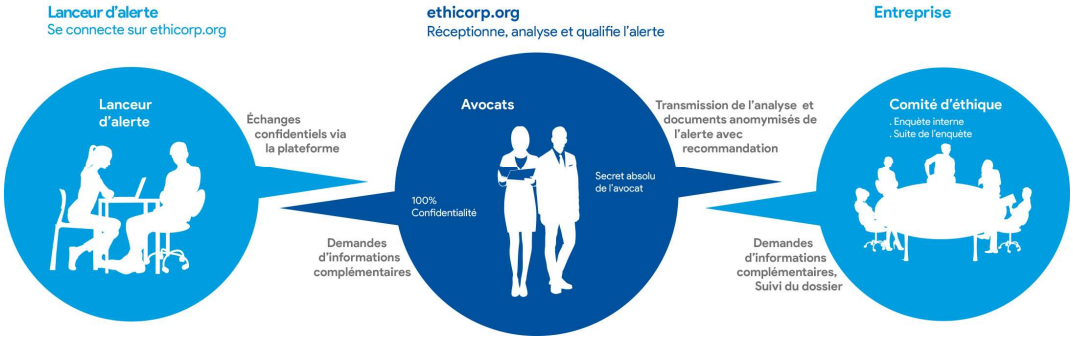
**Follow-up to the alert**

**ethicorp. com** provides an initial analysis of the alert, to ensure that it complies with the legal provisions, particularly with regard to the seriousness of the facts that may be reported.

If the alert corresponds to the legal provisions, it is transmitted (without mentioning the identity of the whistleblower) to the company's Ethics Committee, which will decide on follow-up measures: internal investigation, legal proceedings, etc.

In accordance with the CNIL's deliberation of 18 July 2019, "*personal data must only be made accessible to persons authorised to know it in the light of their duties*".

If the Ethics Committee or investigators require additional information, **ethicorp. com** will interface with the whistleblower to ensure strict confidentiality.




**Article 9. PROCESSING OF PERSONAL DATA**

The CNIL specifies (deliberation of 18 July 2019) "*that the data controller must ensure that only the data necessary for the purposes of the processing are actually collected and processed*"

*It is therefore the responsibility of the data controller to ensure that only relevant and necessary information with regard to the purposes of the processing is collected and/or stored in the alert system. This is generally the case for the following categories:*

- *Identity, functions and contact details of the sender of the alert.*
- *Identity, functions and contact details of the persons subject to the alert.*
- *Identity, functions and contact details of persons involved in the collection or handling of the alert.*
- *Reported facts.*
- *Elements collected in the context of the verification of the reported facts.*
- *Reports of verification operations.*
- *Follow-up to the alert.*

In accordance with the deliberation of the CNIL (18 July 2019) **ethicorp. com** is contractually committed not to use the data for improper purposes, to ensure their confidentiality, to respect the limited duration of data retention and to proceed with the destruction or return of all manual or computerised data carriers of a personal nature at the end of its service.

Article 8.I.C of the Sapin II Act provides that when the procedure for collecting and processing alerts is common to several companies in a group, a decree shall set "*the conditions under which information relating to an alert issued within one of the companies in a group may be transmitted to another of its companies, with a view to ensuring or supplementing its processing.*"

**Data retention periods**

The storage of personal data is subject to the provisions of the Law of 6 January 1978 and the EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (known as the General Data Protection Regulation - GDPR), in force since 25 May 2018.
In particular, personal data may only be kept for as long as is strictly necessary to fulfil the purpose for which they were collected.

Article 9-III of the Sapin II Law provides, since the entry into force of the law of 21 March 2022, that:

> *"Alerts may be kept only for as long as is strictly necessary and proportionate for processing and for the protection of the authors, the persons concerned and the third parties mentioned in the alert, taking into account the time needed for any further investigations. However, data relating to alerts may be kept beyond this period, provided that the natural persons concerned are neither identified nor identifiable.*
>
> *When processed, personal data relating to alerts shall be stored in accordance with 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 (General Data Protection Regulation)."*

In accordance with point 7.1 of the reference framework established by the CNIL (deliberation of 18 July 2019):

> *"Data relating to an alert considered by the controller as not falling within the scope of the scheme, shall be destroyed without delay from the professional alert scheme or anonymised in accordance with Opinion 05/2014 on anonymisation techniques of the European Data Protection Committee (EDPS)[8] .*
>
> *Where no action is taken[9] on an alert falling within the scope of the scheme, the data relating to that alert shall be destroyed or anonymised by the organisation responsible for managing alerts within **two months of the** closure of the verification operations.*

[8] https://www.cnil.fr/sites/default/files/atoms/files/wp216_fr_0.pdf

[9] In accordance with the CNIL reference document of 18 July 2019, the term "*follow-up*" refers to any decision taken by the organisation to draw the consequences of the alert. This may include the adoption

*Where disciplinary or litigation proceedings are initiated against a respondent or the author of an unlawful alert, the data relating to the alert may be kept by the organisation responsible for managing alerts until the* ***end of the proceedings or the time limit for appealing against the decision.***

*With the exception of cases where no* ***action*** *is taken on the alert, the controller may keep the data collected in the form of an intermediate archive for the purpose of ensuring the protection of the whistleblower or to enable the establishment of continuing offences. This retention period must be strictly limited to the purposes pursued, determined in advance and made known to the data subjects.*

*Data may be kept for a longer period of time, in intermediate storage, if the controller is legally obliged to do so (for example, to meet accounting, social or tax obligations).*

The Commission recalls that decisions on the follow-up to professional warnings must be taken within a reasonable time after they have been issued.

It should be noted that the regulations on the protection of personal data do not apply to anonymised data, particularly as regards storage periods. Therefore, the data controller may keep anonymised data without time limits. In this case, the organisation concerned must ensure that the anonymised data are kept permanently.

In addition, in accordance with the deliberation of the CNIL of 12 February 2016:

*The data collected and processed in the context of* ***managing a pre-litigation*** *must therefore be deleted* ***as soon as the dispute is settled out of court or, failing that, as soon as the corresponding legal action is time-barred****.*

*Data collected and processed in the context of litigation must be deleted* ***when the ordinary and extraordinary remedies against the decision are no longer available****.*

*At the end of these periods, the data shall be securely deleted or, where appropriate, archived under conditions defined in accordance with the provisions of the heritage code relating to the obligations to archive public sector information for bodies subject to these provisions, on the one hand, or in accordance with the provisions of the Commission's deliberation No. 2005-213 of 11 October 2005 adopting a recommendation concerning the modalities of electronic archiving of personal data for bodies in the private sector, on the other hand*

*In this respect, the Commission considers that the decisions taken may be kept by the controller as a definitive archive because of their historical interest.*

**Respect for the rights of access and rectification**

Data subjects have the following rights, which they may exercise under the conditions laid down in the GDPR:

- Right to object to the processing of their data, subject to the conditions for exercising this right in accordance with Article 21 of the GDPR.
- Right of access, rectification and deletion of data concerning them.
- Right to restrict processing. For example, if the individual disputes the accuracy of his or her data, he or she can ask the organisation to temporarily freeze the processing of his or her data while it conducts the necessary checks.

---

or modification of the organisation's internal rules (internal regulations, ethics charter, etc.), a reorganisation of the company's operations or services, the pronouncement of a sanction or the implementation of a legal action.

When data subjects exercise their right of access, they may not, through the exercise of this right, obtain any data relating to third parties.

The person concerned by the alert who exercises his right of access may not under any circumstances obtain information concerning the identity of the issuer of the alert.

In accordance with Article 21 of the RGPD, the right to object cannot be exercised for processing necessary to comply with a legal obligation to which the controller is subject (in particular concerning processing conducted by companies meeting the conditions of Articles 8 and/or 17 of the Sapin II Law).

On the other hand, when an organisation sets up an alert system on a purely voluntary basis, the right to object exists. Therefore, the data subjects will have to be informed of its existence and the controller will have to ensure that it is respected.

However, the exercise of this right is not automatic: the person exercising it must demonstrate the existence of "reasons related to his or her particular situation".

The controller will have to take the objection into account, unless it can be shown that:

- That there are legitimate and compelling reasons which override the interests and rights and interests of the data subject.
- Or the processing is necessary for the establishment, exercise or defence of legal claims

Finally, the CNIL (deliberation of 18 July 2019) specifies that the right of rectification, provided for in Article 16 of the RGPD, must be assessed with regard to the purpose of the processing.

This right of rectification is limited and may not allow the retroactive modification of the elements contained in the alert or collected during its investigation. When exercised, it must not make it impossible to reconstruct the chronology of any changes to important elements of the investigation.

This right may only be exercised to rectify factual data, the material accuracy of which can be verified by the data controller on the basis of evidence, without erasing or replacing the data, even if incorrect, originally collected.

For any request, please contact SAS ethicorp. com, 7 rue Royale, 75008 Paris, contact@ethicorp.com

### Article 10. DISSEMINATION OF THIS PROCEDURE - INFORMATION

In accordance with the decree of 19 April 2017, *"The body shall disseminate the procedure for collecting alerts that it has established by any means, in particular by notification, posting or publication, where appropriate on its website, under conditions that make it accessible to members of its staff or agents, as well as to its external or occasional collaborators. This information may be provided by electronic means.*

The Recommendations of the French Anti-Corruption Agency also recall that the various stages of the implementation of the whistleblowing system should include "*dissemination of the internal whistleblowing procedure to all staff by any means (management letter, posting, intranet site, hand-delivery, etc.) that ensures that each person concerned is aware of it and has access to it. In the case of a whistleblowing system that is common to the anti-corruption whistleblower and other legal systems, the procedure must also be distributed to casual employees. The company may decide to open its whistleblowing system to third parties. The company may choose to use its external communication tools to mention the existence of its whistleblowing system (e.g., its website, documents given to third parties, etc.);*"

Furthermore, the CNIL (deliberation of 18 July 2019) recommends that all persons potentially concerned by the system be informed prior to its introduction in the organisation.

This information specifies how the system works, in particular the stages of the procedure for collecting alerts, and in particular the recipients and the conditions under which the alert may be sent to them.

The controller expressly states that misuse of the system may expose the person to sanctions or prosecution but that, conversely, use of the system in good faith will not expose the person to any disciplinary sanction, even if the facts subsequently prove to be inaccurate or do not give rise to any follow-up.

The data controller reminds that the whistleblowing system is only one means of reporting among others (as can be the hierarchical channel), and that the fact of not using it cannot lead to any sanction against the staff members.

Finally, it is recommended that individual information be given to people as far as possible.

### Article 11. STAFF TRAINING

In accordance with the Recommendations of the French Anti-Corruption Agency:

- *"The company shall ensure that the persons in charge of managing the alert are trained, that the confidentiality of the handling of the alert is respected and that there is no conflict of interest; it shall also ensure the training of line managers. (§258)*
- *"The internal alert system is presented without delay to employees who have just joined the company. (§259)*
- The different stages of the implementation of the alert system should include
    - The "*presentation of the warning system as part of awareness-raising activities for all staff;*"
    - *Training of staff involved in collecting, managing and processing alerts, particularly on confidentiality obligations, and training of the most exposed staff*".

Done at Lisses, on December 1st, 2022.

Version as of [01 09 2022]