WHISTLEBLOWING PROCEDURE

CONTENTS

I. GLOSSARY

AFA: French Anticorruption Agency ("Agence Française Anticorruption")

GTCP/GTCS: General Terms & Conditions of Purchase / General Terms & Conditions of Sale

CNIL: French Data Protection Authority ("Commission Nationale de l'Informatique et des Libertés")

Code: refers to Exail Group *Anticorruption Code of Conduct.*

Collaborator: means collectively, for each Entity: (i) employees, whether they work full time, part time, on a fixed-term or permanent contract, under a thesis agreement, on a work-study contract or apprenticeship; (ii) staff on freelance agency contracts; (iii) temporary staff and trainees; (iv) self-employed managers and persons with equivalent responsibilities.

Ethics Committee: refers to the committee whose members and tasks are described in chapter IV.2 of this procedure.

Corruption: see chapter IV of the Code.

Management: refers to any member of the management of an Entity, i.e. having a Director level in Exail organisation and/or being statutorily part of a governance body of an Entity.

Entity: refers indiscriminately to Exail Holding SAS and/or any company controlled (directly or indirectly) by it, in France and abroad, as well as the secondary establishments and other offices of these companies.

Exail or **Exail group**: refers collectively to all the Entities.

Sapin II Law: refers to Law no. 2016-1691 of 9th December 2016 on transparency, the fight against corruption and the modernisation of economic life, amended by Law no. 2022-401 of 21st March 2022 aimed at improving the protection of whistleblowers, known as the Waserman Law, which gave rise to Decree no. 2022-1284 of 3rd October 2022 on the procedures for collecting and processing whistleblower reports.

Referents: designates the internal referents responsible for receiving, handling and processing alerts, as explained in chapter IV.1 of this procedure.

GDPR Regulation or **GDPR**: refers to Regulation (EU) 2016/679 of the Parliament and of the Council of 27th April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Trade Compliance Committee or **TCC**: refers to the committee whose members and tasks are described in chapter IV.3 of this procedure.

II. FRAMEWORK FOR THE INTERNAL WHISTLEBLOWING SCHEME

As further explained in detail in the *Memo on the Protection of Whistleblowers under French Law*, annexed to this procedure (but only available in French), the Sapin II Law requires certain companies and groups of companies to set up an **internal whistleblowing system:**

- Articles 6 to 16 require a whistleblower protection system to be put in place, which must be formalised in a procedure for collecting and processing whistleblowers reports;
- Article 17 requires the implementation of "*an internal whistleblowing system designed to enable the collection of reports from employees concerning the existence of conduct contrary to the company's code of conduct*".

In accordance with Article 5 of Decree no. 2022-1294 of 3rd October 2022 and the AFA Recommendations, it is possible to set up a single system for collecting alerts common to both provisions.

Subject to these obligations and in line with its ethics and compliance policy, which aims to establish and perpetuate a culture of transparency and integrity, Exail Group has set up an internal whistleblowing scheme, as explained in this procedure.

It therefore sets out the principles and measures in place within Exail Group for **the collection and processing of whistleblowing reports** made to Exail by employees, external and occasional collaborators and any other persons concerned, in accordance with the legal provisions applicable in France to whistleblowers.

The internal whistleblowing scheme is an integral part of the anticorruption system deployed within Exail Group in accordance with the AFA Recommendations. As such, it has 2 main objectives:

- enable all Collaborators to report any behaviour or situation contrary to the Code, in order to put an end to it and, if necessary, sanction the person(s) responsible;
- contribute to updating the Group's anticorruption system, in particular its risk mapping, to strengthen measures to prevent and detect corruption.

It should be noted that throughout the rest of the procedure and its appendices, the terms "alert", “report” and "whistleblowing" will be used interchangeably with the same meaning.

This procedure is supplemented by the following documents, which constitute annexes:

- the *Memo on the Protection of Whistleblowers under French Law* (available in French only);
- the *Guide on Ethicorp Platform* ;
- the *Ethicorp User Manual* ;
- the *List of Referents* (for internal use only) ;
- the model of *Ethics Charter* (for internal use only).

III. SCOPE OF THE WHISTLEBLOWING SCHEME

III.1 Subjects of an internal alert

The internal alert scheme concerns any report to Exail concerning:

- a felony, crime or misdemeanour ;
- a threat or harm to general interest ;
- a violation or an attempt to conceal a violation of:
  - an international commitment duly ratified or approved by France ; or
  - a unilateral act of an international organisation taken on the basis of such undertaking ; or
  - European Union law, statute or regulation ;
- a breach of Exail *Anticorruption Code of Conduct* ;
- a breach of any other code or charter in force within any Entity and formally incorporated into the Entity's internal regulations (in France) or any other document of equivalent scope (abroad).

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

On the other hand, facts, information and documents, whatever their form or medium, the revelation or disclosure of which is prohibited by provisions relating to national defence confidentiality, medical confidentiality, the confidentiality of judicial deliberations, the confidentiality of judicial investigations or proceedings and/or the professional confidentiality of lawyers (legal privilege), are excluded from the whistleblowing regime.

III.2 Entities concerned

Subject to legal obligations to consult social dialogue bodies, the internal alert scheme applies to all Entities established in France and, subject to legal and regulatory provisions applicable locally, to all Entities established abroad.

III.3. Persons concerned

As regards internal reporting of any behaviour or situation contrary to the Code, the internal whistleblowing scheme applies to all Collaborators.

More generally, to be eligible to the legal provisions protecting whistleblowers in France, the whistleblower must:

- be a natural person ;
- act without expecting direct financial compensation ;
- be acting in good faith ;
- be one of the following:
  - members of staff of any Entity ;
  - persons whose employment relationship with an Entity has ended, where the information was obtained in the course of that relationship ;
  - persons who have applied for a job within an Entity, where the information was obtained as part of that application ;
  - shareholders, associates and holders of voting rights in the general meeting of any Entity ;

- members of the administrative, management or supervisory body of an Entity ;
- external and occasional employees of any Entity ;
- co-contractors of any Entity, as well as their own subcontractors and, in the case of legal entities, the members of the administrative, management or supervisory bodies of these co-contractors and their subcontractors ;
- members of the staff of said co-contractors and their sub-contractors.

Furthermore, where the information was indeed obtained in the course of professional activities, the whistleblower may not have had mandatorily a personal knowledge of it, i.e. he/she may not have personally witnessed or been the victim of the facts. This would however not be possible in a non-professional context.

The scope of people who can benefit from the legal whistleblower protection scheme applicable in France is therefore broader than that of employees alone.

Finally, whistleblowers must not act maliciously or out of revenge by reporting information they know to be false or misleading.

It is under these conditions that the whistleblower will benefit from the full protection guaranteed by law (see chapters VIII and subsequent ones below). If they fail to do so, particularly in cases of bad faith, rumour spreading or defamation, they will be liable to sanctions (see chapter XIII below).

It should be noted that with regard to all of the persons listed above who are not Collaborators, it is and remains the responsibility of Exail co-contractors to inform them of the internal alert scheme in place, on the basis of the information made available to them by Exail (see chapter XIV below).

III.4. Reporting channels and disclosure

As explained in chapter IV of the *Memo on the Protection of Whistleblowers under French Law*, a whistleblower has three distinct channels for making his or her report while benefiting from the protections granted by law to this status:

- internal reporting ;
- external reporting ;
- public disclosure.

Exail Group internal whistleblowing scheme, which is the subject of this procedure, only covers the **internal reporting** channel. The term "report" or "alert" is therefore used here to mean only a report or an alert addressed to Exail.

For provisions relating to other channels, reference should be made to the applicable legal and regulatory provisions, as set out, for example, in the *Memo on the Protection of Whistleblowers under French Law* (in particular chapter IV).

IV. REFERENTS AND COMMITTEES

IV.1 Referents

The role of the Referents involved in the internal alert scheme is to:

- receive alerts addressed to them directly and/or indirectly, including via an internal hierarchical channel (see chapters V.1, V.3 and VI below) ;
- receive alerts transmitted via the ethicorp platform in accordance with the arrangements put in place (see chapter V.4 below) ;
- process alerts (see chapter VII below) ;
- convene or involve, where appropriate, the Ethics Committee (see chapter IV.2) or the TCC (see chapter IV.3) ;
- contribute to annual statistical reporting on the receipt, processing and follow-up of alerts received, and update the internal alert scheme as necessary, as directed by the Compliance Officer.

Given Exail structure, size and organisation, it has been decided to appoint the people whose functions are set out in the table below as Referents.

These persons have, by virtue of their position or status, the competence, authority or legitimacy, as well as the sufficient means to carry out their missions. Exail General Management ensures their independence in carrying out these missions.

Functional area	Referents
Human Resources Referents	- Group HR Director - Business Areas HR Directors - Entity related sexual harassment and gender-based harassment Referents appointed by management and/or the personnel representatives
Legal & Compliance Referents	- Group General Counsel - Group Compliance Officer

Table 1 - Functional list of Referents

The most up-to-date contact details of the Referents are given in the *List of Referents,* which is accessible only to Collaborators.

The Referents are all signatories to the *Ethics Charter*, which stipulates in particular the reinforced commitments to confidentiality, integrity and impartiality that they undertake to respect in all circumstances in connection with the implementation of the internal whistleblowing scheme.

IV.2 Ethics Committee

At the request of at least one of the Human Resources Referents, an Ethics Committee will be set up without delay to deal with an alert in this area (see chapter VII below).

It should be noted that an Ethics Committee is not systematically set up. It is up to the Human Resources Referent(s) involved to decide whether and when to set it up, considering the context of the report and, first and foremost, the seriousness of the facts.

If an Ethics Committee has not been set up, the Referent(s) in charge of the processing will oversee the process directly (see chapter VII below).

An Ethics Committee may be set up as soon as the alert is received by the concerned Referent(s), or afterwards if necessary. Once an Ethics Committee has been set up, and provided that the alert is not subsequently declared irrelevant, it will handle the alert until it is closed.

An Ethics Committee is made up of:

- at least one member of Exail CODIR ;
- the Group HR Director ;
- one or more of the other HR Referents (including sexual harassment and gender-based harassment Referents), particularly when the report relates to their organisational reporting line ;
- the Legal & Compliance Referents as required ;
- any other person whose participation is necessary.

The composition of an Ethics Committee is validated by the member or members of Exail CODIR who sit on it and the Group HR Director.

In order to guarantee the impartiality of the internal whistleblowing scheme, no person may be a member of an Ethics Committee if he or she is involved in the whistleblowing and/or has a proven personal conflict of interest in connection with it.

The members of an Ethics Committee are all signatories to the *Ethics Charter*, which stipulates in particular the reinforced commitments to confidentiality, integrity and impartiality that they undertake to respect in all circumstances in connection with the implementation of the internal whistleblowing scheme.

IV.3 Trade Compliance Committee (TCC)

The Trade Compliance Committee or TCC is a permanent committee set up within Exail as part of the scheme for preventing and detecting corruption.

Its main tasks are: (i) to process the third-party assessment files sent to it in accordance with Exail Group *Third-Party Assessment Procedure*, (ii) to examine and process any alert sent to it by the Legal & Compliance Referents, in particular with regard to breaches of the Code, (iii) to monitor and supervise the proper implementation of the scheme for preventing and detecting corruption, including the internal alert scheme, and

(iv) to take any necessary measures relating to the effectiveness of the scheme, including the internal alert scheme.

The TCC is made up of:

- the members of Exail CODIR ;
- the Legal & Compliance Directors ;
- the Group Sales Directors.

In accordance with AFA Recommendations, any report relating to (i) facts likely to constitute breaches of the Code, (ii) behaviour that does not comply with internal procedures designed to prevent or detect the commission of such breaches or (iii) indications of the commission of facts likely to be qualified as Corruption, will be systematically and immediately sent by the relevant Referents to the TCC, which will process it (see chapter VII below).

For all other reports received by the Legal & Compliance Referents, however, the TCC is not systematically involved. It is up to the Legal & Compliance Referents to decide whether it is appropriate for the TCC to be directly involved in handling the alert, considering the context of the alert and, first and foremost, the seriousness of the facts. In such a case, the TCC may be involved as soon as the alert is received by the relevant Referents, or afterwards as required. Once involved, and provided that the alert is not subsequently declared irrelevant, the TCC will handle the alert until it is closed (see chapter VII below).

In the absence of direct involvement by the TCC, the Referent(s) in charge of the treatment is(are) directly responsible for its progress (see chapter VII below).

In order to guarantee the impartiality of the internal whistleblowing scheme, no person may take part in the work of the TCC in connection with a whistleblowing escalated to it if he or she is involved in the report and/or has a proven personal conflict of interest in connection with it.

All members of the TCC are signatories to the *Ethics Charter*, which stipulates in particular the reinforced commitments to confidentiality, integrity and impartiality that he or she undertakes to respect in all circumstances in connection with the implementation of the internal whistleblowing scheme.

V. HOW TO LAUNCH AN ALERT

V.1 Soliciting the hierarchical channel

Before raising an alert, any Collaborator may, if he or she so wishes, contact his/her direct or indirect line manager and/or his/her supervisor, as applicable, who has a duty to assist and guide him or her as necessary (see also chapter XIV below).

However, if the Collaborator confirms his/her wish to lodge a report, he/she shall be directed **without delay** to the ethicorp platform or to a Referent, who are **the only channels** authorised to receive a report in order to guarantee the integrity of the process, in compliance with the applicable legal and regulatory obligations (see in particular chapter VIII).

V.2 Channels available for sending an alert

In order to ensure that the internal whistleblowing scheme is as effective as possible, while respecting the obligations of integrity, confidentiality and impartiality, two separate channels may be used by any concerned person to make a report:

1. Contact the internal **Referents** as explained in chapter V.3 below.
2. Use the outsourced **ethicorp** platform as explained in chapter V.4 below.

It should be noted that the ethicorp whistleblowing platform is only one of the two reporting methods that can be used, and failure to use it cannot result in any sanctions being taken against Collaborators.

The content of an alert and other provisions common to both reporting channels are explained in chapter V.5 below.

V.3 Sending an alert directly to the Referents

Referents can be contacted directly to transmit an alert via the following functional e-mail addresses, shared by the concerned Referents according to the associated functional areas:

- alert.hr@exail.com for all human resources issues;
- alert.compliance@exail.com for all other subjects.

All alerts sent via this channel must be in French or English.

In order to guarantee the effectiveness, integrity and robustness of the internal alert scheme when the Referents are contacted directly, it is recommended to use these shared functional addresses rather than their personal addresses.

However, as these functional addresses are shared by the Referents, if one of them is personally concerned by an alert, it is preferable to use the ethicorp platform to avoid any conflict of interest.

Finally, in the event that a Collaborator wishes to contact a Referent without going by e-mail, he or she may do so by using the *List of Referents*. The report may then be

received by telephone or, at the Collaborator's request and according to his/her choice, during a videoconference or a physical meeting organised no later than twenty working days after receipt of the request. In this case, the procedures for recording the alert will be defined in advance so as to guarantee compliance with the specific legal obligations associated with a verbal alert.

V.4 Sending an alert via the ethicorp platform

Exail has subscribed to the **ethicorp** whistleblowing platform, which provides the highest guarantees of impartiality and independence to people who wish to use it to report a problem.

The **ethicorp** platform can be accessed via the Internet at the secure address https://www.ethicorp.org.

This French platform for receiving and pre-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 positioning gives it the skills, authority and resources it needs to carry out its missions.

The use of the **ethicorp** platform is described in detail in the following documents, which are annexes to this procedure:

- *Guide on Ethicorp Platform* ;
- *Ethicorp User Manual*.

***In particular, the Guide on Ethicorp Platform* contains the corporate codes associated with Exail that are required to create an account on the platform, a prerequisite for filing an alert.**

V.5. Content of an alert and other common provisions

Regardless of the channel used, the alert must include :

- the identity, contact details (including a valid e-mail address) and, ideally, the professional status of the person who issued the alert, unless they choose to remain anonymous, under the conditions set out below ;
- the facts it wishes to report, with an appropriate level of detail ;
- information, documents and other evidence to support the alert, where available.

If the information required to support the alert cannot be sent by e-mail, appropriate collection procedures will be defined on a case-by-case basis with the addressee of the alert.

To avoid any confidentiality issues, we recommend that you do not use your company's equipment to connect. Similarly, for confidentiality reasons, we recommend that you do not use a company e-mail address.

In accordance with CNIL recommendation of July 2019, Exail does not encourage people who intend to use the scheme to do so fully anonymously. In any event, their identity will always be treated as confidential (see chapter VIII below).

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

- the seriousness of the facts mentioned is established and the facts are sufficiently detailed, so it is essential to be precise in describing 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 disseminating it.

If these conditions are not met, the recipient of the alert may inform the whistleblower that he or she must identify himself or herself or that the alert cannot be processed.

VI. HOW AN ALERT IS RECEIVED

VI.1 Acknowledgement of receipt

Regardless of the channel used, a written acknowledgement of receipt is sent by the recipient of the alert within seven working days of receipt of the alert, except in the case of an anonymous alert which has not been rejected and for which it would not be physically possible to contact the author.

Please note that this acknowledgement of receipt does not constitute acceptance of the alert.

VI.2 Admissibility

Whichever channel is used, the recipient of the alert will immediately carry out an initial analysis to assess the seriousness, relevance, nature and gravity of the alleged facts.

In addition, except in the case of a fully anonymous alert that has not been rejected, the recipient of the alert shall check that the conditions of eligibility for the legal protection of whistleblowers have been met (see chapters III.1 and III.3 above).

In order to confirm the admissibility of the alert, any necessary additional information may be requested from the author of the alert, depending on the channel used, except in the case of a fully anonymous alert for which it would be materially impossible to contact the author.

The author of the alert will be informed of the reasons why the addressee of the alert considers, where applicable, that the alert does not meet the conditions of eligibility. He/she will also be informed if his/her alert is rejected or if it will be processed anyway.

Once the admissibility of the alert has been analysed, if it appears to be founded, it is dealt with appropriately (see chapter VII below).

If the ethicorp channel is used, once the admissibility of the alert has been confirmed as explained above, the alert is forwarded via a summary note to the relevant Referent(s) (see chapter II of the *Guide on Ethicorp Platform*).

Conversely, if this initial analysis clearly shows that the alert is inaccurate or unfounded, it is immediately closed and no further action taken. The author of the alert is informed of the closure of the alert when it is closed.

VII. HOW AN ALERT IS PROCESSED

VII.1 Handling

Once a valid alert has been received, regardless of the channel used, at least one of the concerned Referents takes charge of handling it.

If an Ethics Committee is set up (see chapter IV.2 above) or if the TCC is involved (see chapter IV.3 above), the handling of the alert is steered by the Ethics Committee or the TCC.

VII.2 Confirmation of treatment

Where appropriate, if the information available at this stage does not allow a clear decision to be taken on the validity of the alert, further investigations will be carried out to confirm whether treatment should be continued.

In this respect, any additional information required may, if possible and relevant, be requested from the author of the alert, depending on the channel used.

If these investigations show that the alert is inaccurate or unfounded, it is closed. If, on the other hand, the investigations confirm that the alert is well-founded, it will be dealt with by means of an internal investigation.

VII.3 Internal investigation

The internal investigation will be conducted in order to precisely determine the accuracy and materiality of the facts reported in the alert. It will be conducted in an exhaustive, impartial, confidential and adversarial manner.

Within this framework, any necessary additional information may, if possible and relevant, be requested from the person who issued the alert, depending on the channel used.

In compliance with the applicable legal and regulatory provisions, in particular with regard to confidentiality, the presumption of innocence and the rights of defence (see chapter X below), interviews may be conducted as necessary with (i) the person or persons who are the subject of the alert, (ii) any third parties identified in the alert and (iii) any person who should be interviewed for the internal investigation to be effective.

All the interviews conducted will be recorded in written form in an appropriate manner.

As required, internal and/or external resources may also be called upon for their expertise in the context of the internal investigation. These persons will first sign the *Ethics Charter* or any equivalent document, stipulating in particular the reinforced commitments to confidentiality, integrity and impartiality that they undertake to respect in all circumstances in connection with their involvement in the internal investigation.

At the end of the internal investigation, a memorandum or summary report (depending on the nature, seriousness and extent of the facts) will be drawn up, attaching all the appropriate supporting documents.

VII.4. Follow-up

Once the internal investigation has been completed, and on the basis of the summary note or report, the action to be taken on the alert will be formally decided and then implemented by the persons with the authority to do so, for each Entity concerned, i.e.:

- the measures to be taken, if necessary, to remedy the matter for which the alert has been issued ;
- whether to initiate disciplinary proceedings and/or legal action ;
- any further action to be taken in connection with:
    - the operation and/or organisation of any concerned Entity ;
    - any element of Exail anticorruption scheme, including the internal whistleblowing scheme ;
    - any other relevant information (e.g. internal regulations, charters and codes, procedures, memos, etc.).

Once all the actions have been formally decided, the alert is closed.

VII.5 Informing the author of the alert

Except in the case of fully anonymous alerts for which it would be physically impossible to contact the author, written feedback is given to the author of the alert as a minimum, depending on the channel used, as follows:

- Within a reasonable period of time not exceeding three months from the acknowledgement of receipt of the alert or, in the absence of such acknowledgement, three months from the expiry of a period of seven working days following the alert, the author of the alert shall be informed of the measures envisaged or taken to assess the accuracy of the allegations and, where appropriate, to remedy the subject of the alert, as well as the reasons for such measures.
- The author of the alert is informed when the alert is closed, even if it is ultimately closed without further action.

VIII. CONFIDENTIALITY

In accordance with Article 9 of Sapin II Law, the following must remain strictly confidential:

- the identity of the whistleblower, who must be able to report in complete peace of mind ;
- the identity of the person concerned by the alert and that of any third party mentioned in the alert ;
- information gathered as part of the alert, i.e. the facts that are the subject of the alert.

In practice, these last two elements (identity of the person concerned and of any third party mentioned in the alert, as well as information gathered in the context of the alert) will only be known to those responsible for gathering and then processing the alert, for the purposes of the alert and under a strict obligation of confidentiality.

Access to this information is forbidden to persons who are not authorised to know it in accordance with the provisions of this procedure. For this reason, it is imperative that reports which may have been sent directly to other employees are forwarded to the Referents without delay.

Aside from authorised persons, information that could identify the whistleblower may only be disclosed with the whistleblower's consent.

However, they may be communicated to the judicial authorities if the persons responsible for collecting or processing the alerts are required to report the facts to the judicial authorities. The whistleblower is then informed unless this information could compromise the legal proceedings. Written explanations are attached to this information.

Furthermore, the whistleblower may not himself freely disclose the information that is the subject of the whistleblowing, except in the strict context of public disclosure (see chapter III.4 above).

IX. WHISTLEBLOWER PROTECTION

In accordance with articles 10-1 and 12 to 13-1 of the revised Sapin II Law, whistleblowers are **protected against any retaliatory measures**.

For example, no one may be excluded from a recruitment procedure or from access to an internship or a period of professional training, and no employee may be punished, dismissed or subjected to a discriminatory measure for having reported a whistleblowing (see chapter VII of the *Memo on the Protection of Whistleblowers under French Law*).

Retaliation against a whistleblower also constitutes an offence of discrimination, in accordance with article 225-1 of the French Criminal Code (see also chapter XIII below for associated sanctions).

In certain cases and under certain conditions, whistleblowers are also exempt from criminal and civil liability.

Of course, this protection only applies if the whistleblower complies with the framework set out in articles 6 to 8 of the Sapin II Law.

On the other hand, whistleblowers will not be protected if they do not meet the legal definitions, and in particular if they report facts in bad faith and/or of which they had no personal knowledge when the information was not obtained in the course of their professional activity.

This being said, the use of the scheme **in good faith** will not expose the user to any disciplinary sanction, even if the facts subsequently prove to be inaccurate or do not give rise to any follow-up.

X. RIGHTS OF PERSONS AFFECTED BY A REPORT

Any person who is the subject of a report is entitled to strict confidentiality, in particular with regard to the fundamental principle of presumption of innocence and rights of defence. Identifying information may not be disclosed, except to the judicial authority, until it has been established that the whistleblowing is well-founded.

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

However, in accordance with Article 14-5-b of the GDPR, this information may be deferred where it is likely to "*seriously jeopardise the achievement of the purposes of such processing*". This could, for example, be the case where disclosure of this information to the person concerned would seriously compromise the needs of an investigation, for example where there is a risk of evidence being destroyed. However, the information must be provided as soon as the risk has been averted and must not contain any information relating to the identity of the person who issued the alert or any third parties.

Similarly, an internal investigation initiated following a report of moral harassment does not necessarily require the employer to give the accused employee access to the case file. In a ruling handed down in June 2022, the French “Cour de cassation” stated that respect for the rights of defence and the principle of contradiction does not require, in particular, that in the context of an internal investigation designed to verify the veracity of conduct reported by other employees, the accused employee be given access to the case file and the documents collected, or that he be confronted with the colleagues accusing him.

However, if legal proceedings are initiated against the person concerned as a result of the alert, that person may obtain disclosure of the information in accordance with the rules of ordinary law (in particular the rights of defence).

However, this possibility is subject to appropriate measures being taken to protect the rights, freedoms and legitimate interests of any concerned person.

XI. PROCESSING OF PERSONAL DATA

Any personal data communicated in application of the internal whistleblowing scheme will be processed in accordance with the legal and regulatory provisions applicable to the protection and processing of personal data (see chapter IX of the *Memo on the Protection of Whistleblowers under French Law*).

The personal data collected and processed in the context of an alert are collected and processed for the sole purpose of complying with the obligations of the Sapin II Law and, more generally, with the legal and regulatory obligations applicable to Exail. In particular, only the personal data necessary to pursue the purposes of the associated processing will actually be collected and processed.

They will be recorded in a computerised file and may be forwarded as necessary to the persons involved in the collection and processing of alerts and, where appropriate, to the administrative and judicial authorities, always in compliance with the applicable legal and regulatory provisions.

The persons concerned by an alert have the following rights with regard to their personal data, which they may exercise in accordance with the conditions set out in the GDPR:

- right to object to the processing of their data, subject to the conditions for exercising this right pursuant to the provisions of Article 21 of the GDPR (the right to object may not be exercised in respect of processing necessary for compliance with a legal obligation to which the data processor is subject, in particular in respect of processing carried out and meeting the conditions of Articles 8 and/or 17 of the Sapin II Law) ;
- right of access, rectification (with regard to the purpose of the processing) and deletion of data concerning them ;
- right to restrict processing.

When a concerned person exercises his/her right of access, he/she may not, through the exercise of this right, obtain communication of any data relating to third parties.

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

The retention period for personal data is governed by the provisions set out in chapter XII below.

Any request relating to the processing of personal data via the internal alert scheme should be addressed to the Compliance Officer (see chapters IV.1 above or XIV below).

XII. DATA RETENTION AND DESTRUCTION

The storage of personal data is subject to the provisions of the Law of 6th January 1978 and the GDPR, in force since 25th May 2018. In particular, personal data may only be kept for as long as is strictly necessary to fulfil the purpose for which it was collected.

Article 9-III of the revised Sapin II Law also stipulates that: *"Alerts may only be kept for as long as is strictly necessary and proportionate for their processing and for the protection of their authors, the persons they concern and the third parties they mention, taking into account the time required for any further investigations."*

In accordance with point 7.1 of the guidelines established by CNIL in its deliberation of 18th July 2019, data relating to an alert will therefore be managed as follows:

- Data relating to an alert considered not to fall within the scope of the scheme is destroyed **immediately**.
- If no action is taken[1] on an alert falling within the scope of the scheme, the data relating to the alert is destroyed or made anonymous within **two months of the** end of the verification operations.
- When the alert is followed up at[1], other than in disciplinary or litigation proceedings, the data relating to the alert may be kept in the form of intermediate archives for the purposes of protecting the whistleblower or establishing ongoing offences. This retention period must be strictly limited to the purposes pursued, determined in advance on a case-by-case basis and brought to the attention of the persons concerned.
- When disciplinary or litigation proceedings are initiated against a person implicated or the author of an abusive alert, the data relating to the alert may be kept until the **end of the proceedings or the time limit for appeals against the decision.**
- Finally, data can always be kept for longer, in intermediate storage, if the data processor is legally obliged to do so (for example, to meet accounting, social or tax obligations).

For more information, see chapter IX.2 of the *Memo on the Protection of Whistleblowers under French Law*.

[1] In accordance with CNIL guidelines of 18th July 2019, the term "*follow-up*" refers to any decision taken by the organisation to draw consequences from the alert. This may involve the adoption or amendment of the organisation's internal rules (internal regulations, ethics charter, etc.), a reorganisation of the company's operations or services, the imposition of a sanction or the initiation of legal action.

XIII. PENALTIES

Any direct or indirect reprisal against a Collaborator who has reported an alert will not be tolerated and will result in disciplinary action, up to and including termination of the employment contract, in accordance with applicable law.

Sapin II Law also stipulates that 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 entities).

In addition, misuse of the internal whistleblowing scheme may expose the perpetrator to disciplinary sanctions and/or legal, civil and criminal penalties, in particular for defamation or slander.

Lastly, any breach of the confidentiality of the alert may also give rise to disciplinary action, up to and including termination of the employment contract, in accordance with applicable law.

This violation is also punishable by two years' imprisonment and a fine of €30,000 (€150,000 for legal entities).

All penalties will be applied in accordance with:

- the provisions of the internal regulations (in France) or any other equivalent text (abroad) of the company to which the person concerned belongs ; and/or
- the relevant legal and regulatory provisions.

XIV. INFORMATION AND AWARENESS RAISING

This procedure is:

- integrated in the internal rules of procedure (in France) and in the locally equivalent documents (abroad) of the Entities ;
- publicly available in Exail website(s) ;
- mentioned in Exail General Terms and Conditions (GTCP/GTCS) and contractual clauses ;
- evocated in Exail *Supplier and Partner Code of Conduct* ;
- available to Collaborators in Exail intranet site(s) ;
- communicated to all Collaborators on the occasion of its initial distribution as well as any significant modification ;
- communicated to each new Collaborator ;
- presented to Collaborators, in particular all new Collaborators, as part of awareness raising initiatives for all staff.

Any Collaborator requiring assistance in interpreting any of the provisions of this procedure may contact:

- his/her Manager ;
- the Human Resources Department of the Entity to which it reports ;
- the Legal & Compliance Department, for example at legal@exail.com or compliance@exail.com ;
- one of the Referents directly (see chapter IV.1 above).

XV. TO REMEMBER

As described in chapter II, Exail internal whistleblowing scheme has been set up in application of the legal and regulatory provisions applicable in France, in particular the Sapin II Law. It is an integral part of the anticorruption scheme deployed within Exail Group in accordance with AFA Recommendations.

Although the scheme needs to be known, understood and interpreted in its entirety, it is based on **six main points**:

1. The scheme specifies the scope and conditions of the legal whistleblowing regime, in particular as regards eligibility for whistleblower status (see chapter III).
    a. It is therefore directly applicable to all Exail Group Collaborators in France.
    b. Subject to the legal and regulatory provisions applicable locally, it also applies to Exail Group Collaborators of Entities established abroad.
    c. Lastly, it is open to other interested parties who are not Exail Collaborators, in accordance with the conditions set out above.
2. A specific internal organisation has been set up through the scheme to ensure that reports are collected and processed, via internal Referents and specific committees (see chapter IV).
3. The scheme spells out the practical procedures for launching an alert (see chapter V), via two possible channels: (i) the internal Referents or (ii) the outsourced ethicorp platform.
4. The scheme defines the basic principles and practical procedures for receiving and then processing an alert (see chapters VI and VII), including informing the person who issued the alert of the receipt, handling and closure of the alert.
5. The scheme confirms all the specific measures associated with an alert, in accordance with the applicable legal and regulatory provisions, with regard to:
    a. confidentiality (see chapter VIII) ;
    b. whistleblower protection (see chapter IX) ;
    c. the rights of persons affected by a report (see chapter X) ;
    d. the processing of personal data (see chapter XI) ;
    e. data retention and destruction (see chapter XII).
6. If the scheme is used in good faith and disinterestedly, the author is a priori protected, but an intentionally misleading alert and, more generally, misuse of the scheme may expose the author to disciplinary sanctions and/or legal proceedings (see chapter XIII).

XVI. APPENDICES

The following documents are annexes to this procedure:

- *Memo on the Protection of Whistleblowers under French Law* (in French only) ;
- *Guide on Ethicorp Platform* ;
- *Ethicorp User Manual* ;
- *List of Referents* (for internal use only) ;
- *Ethics Charter* template (for internal use only).