WHISTLEBLOWING POLICY

FOR HANDLING REPORTS OF CRIMES, OFFENCES OR IRREGULARITIES

1. Foreword

"Whistleblowing" means the reporting of any information concerning conduct (active or passive) and facts that - even if only potentially - do not comply with the law, the principles set out in the Code of Ethics of expert.ai S.p.A., the Organisational, Management and Control Model adopted by expert.ai S.p.A. pursuant to Legislative Decree 231/2001, internal procedures, or any other external discipline applicable to the Group as defined below, as well as offences falling within the scope of application of European Union or national regulatory frameworks (hereinafter referred to as "**Report(s)"**) that may damage the Group's integrity and of which one has become aware in the work context.

This Policy (the "**Policy"**), drafted in compliance with EU Directive 1937/2019 and Legislative Decree No. 24/2023 is intended to regulate the process of sending, receiving, analysing and processing Reports, made - including anonymously - by Group personnel (including top management and members of corporate bodies) and/or external contractors (hereinafter referred to as the "**Whistleblower**")[1].

This Policy shall take effect on 01/02/2021. Each subsequent update of the Policy cancels and replaces, from the date of its issue, all previously issued versions. The updating of this Policy is the responsibility of the internal compliance team or of designated consultants.

This Policy, as well as any updates to it, is subject to the approval of the Group's governing body. The Board of Directors is informed of the adoption of the Policy and of subsequent updates to it.

The Policy is made available on the company intranet in the Compliance - Whistleblowing section, as well as on the official website of expert.ai in the Corporate Governance section - expert.ai | expert.ai and on the Platform (as defined below).

2. Reporting Channels

In accordance with Art. 4 of Leg. Decree 24/2023, the Group has set up a specific internal reporting channel dedicated to the communication of the alleged violation, (as better explained below) to guarantee the effectiveness of the Report and at the same time to protect the Whistleblower's identity by means of a web platform chosen by the Group, and compliant with the recent legislation mentioned above (hereinafter the "**Platform"**). The platform will be easily accessible via a special link that will be sent to you individually by e-mail, as well as being published on the website: https://www.expert.ai.

[1] Subjects to whom the same protection as the Whistleblower is extended include facilitators, third parties connected with the Whistleblower who might risk retaliation in a work context, such as colleagues or relatives of the Whistleblower, and legal entities of which the Whistleblower is a controller under Art. 2359 of the Civil Code, for which they work or to which they are otherwise connected in a business context.

The Report will be duly received by the persons specifically designated to receive it and entrusted with the management of the process of analysing and processing Reports, such as the Chief People Officer (hereinafter referred to as "**Receiving Parties"**).

The process of assessing the Report is carried out by the Receiving Parties in full compliance with the principles established by the applicable regulations referred to above and in the manner described below in paragraph 6 "*The Process"*.

3. Scope of addressees

The recipients of this Policy are:

- Top Management and members of the Group's corporate bodies;
- all Group employees;
- those who, although not falling within the category of employees, work on behalf of the Group and are under the Group's control and management (e.g. temporary workers, workers with continuous cooperation contracts, trainees, interns (hereinafter, together with top management and members of the Group's corporate bodies, "**Personnel"**);
- partners, customers, suppliers, consultants, external contractors and, more generally, anyone who is a stakeholder of the Group (the "**Third Parties"**);
- the Personnel and Third Parties of the following companies Expert.ai S.p.A., Expert System Iberia SLU, Expert System France SA, Expert System Deutschland GMBH (jointly, all the companies to which this Procedure applies will be hereinafter referred to as the "**Group"**).

All the persons listed above may send Reports when the legal relationship:

- is in place;
- has not yet started, if the information was acquired during the selection process or at other pre-contractual stages;
- after its dissolution, if the information on violations was acquired in the course of employment or during the probationary period.

In addition, the protective measures provided for and described in Chapter 5 below are also extended to the following persons:

- Facilitators, i.e. persons who assist the Whistleblower in the Whistleblowing process, providing advice and support, and who work within the same work context as the Whistleblower (hereinafter "**Facilitator(s)"**);
- persons in the same work environment as the Whistleblower who are linked to him/her by a stable emotional or family link up to the fourth degree (persons linked by a network of relations arising from the fact that they work, or have worked in the past, in the same work environment as the Whistleblower);
- work colleagues with a regular and current relationship with the Whistleblower (persons who, at the time of the reporting, work with the Whistleblower and have a relationship with him/her that is characterised by such continuity as to determine a close relationship between the parties);
- entities owned by the Whistleblower (entities of which the Whistleblower is the sole or majority owner);

- entities for which the Whistleblower works (e.g. employee of a company providing a supply service for the Group);
- entities operating in the same business environment as the Whistleblower (e.g. partnerships between companies).

4. Scope of issues addressed

The Policy applies, in particular, to Reports concerning:

- administrative, accounting, civil or criminal offences;
- unlawful conduct relevant under Leg. Decree 231/2001 or violations of the Organisation and Control Model and of the Code of Ethics, or of the procedures in place at the Group, also with reference to activities and services of interest to the Group (including but not limited to: non-compliance with contractual clauses, libel and slander, threats, violation of privacy or confidentiality agreements, fraud, improper use of company equipment);
- conduct entailing the risk of an offence or crime being committed, even if not included among the predicate offences provided for in Legislative Decree 231/2001;
- alleged violations, incitement or inducement to violate laws or regulations, internal procedures, with reference to the activities and services of interest to the Group (e.g. non-compliance with contractual clauses, defamation, threats, violation of privacy or confidentiality agreements, fraud, improper use of company equipment);
- offences falling within the scope of Community or national law, indicated in the annex to Legislative Decree No. 24/2023, or of law transposing the European Union law set out in the annex to Directive (EU) 2019/1937, even if not indicated in the annex to Legislative Decree No. 24/2023, relating to the following areas:
    - public procurement;
    - financial services, products and markets and the prevention of money laundering and terrorist financing;
    - safety and conformity of products;
    - transport security;
    - environmental protection;
    - radiation protection and nuclear safety;
    - food and feed safety, and animal health and welfare;
    - public health;
    - consumer protection;
    - protection of privacy and protection of personal data and security of networks and information systems;
- acts or omissions detrimental to the financial interests of the European Union referred to in Article 325 of the Treaty on the Functioning of the European Union specified in the relevant secondary legislation of the European Union;
- acts or omissions relating to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including infringements of EU competition and State aid rules, as well as infringements relating to the internal market related to acts in breach of corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the purpose of the applicable corporate tax law;
- acts or conduct that frustrate the object or purpose of the provisions of European Union law in the areas mentioned above;

- suspicions concerning violations committed or which, on the basis of concrete elements, could be committed within the company organisation, or concerning conduct aimed at concealing such violations;
- complaints from third parties concerning alleged findings, irregularities and reprehensible facts;
- complaints concerning accounting issues, controls.

In order to circumscribe concretely the scope of application of this document, examples of reportable facts are provided below:

- ✓ violations of internal and external rules governing the Group's activities, including those contained in the Organisation, Management and Control Model of expert.ai S.p.A., as well as the principles and rules of conduct contained in the Code of Ethics;
- ✓ unlawful or fraudulent conduct by employees, members of the corporate bodies or third parties (suppliers, consultants, contractors) that may directly or indirectly result in financial and/or image damage for the Group;
- ✓ any commission of offences by employees, members of corporate bodies or third parties (suppliers, consultants, collaborators) committed to the detriment of the Group or which may give rise to the Group's potential liability.

Reports may also have as their subject matter

- the simple request, by the Whistleblower, for clarification of the correctness of his/her own or other people's conduct for the purposes of full compliance with the Code of Ethics (e.g. violation of corporate prohibitions and provisions, checks on the work of suppliers).

Reports must **not** concern complaints of a personal nature. Whistleblowers must not use the scheme for purely personal or retaliation purposes. Similarly, Whistleblower reports must not relate to contractual or trade union claims - unless they are based on the violation of laws, regulations, or procedures adopted by the Group - which, if anything, fall within the more general employment/contractual relationship or relations with hierarchical superiors or colleagues.

Reports concerning commercial complaints are also outside the scope of the Policy.

Reports must contain all the elements necessary to ascertain the merits of the facts that are the subject of the communication, in order to enable the Receiving Party to proceed with the necessary verifications (for more details see paragraph 6 below "The *Process*").

5. General Principles

This Policy is guided by the following general principles:

a) Protecting Whistleblowers

In accordance with the applicable legislation, the Group protects Whistleblowers against any retaliatory action or direct or indirect conduct by anyone arising from a Report

(regardless of whether the Report proves to be well-founded), such as, but not limited to: dismissal; suspension; demotion; loss of benefits; unjustified transfer; mobbing; harassment in the workplace; any other type of conduct leading to deteriorating or intolerable working conditions.

In particular, it is hereby noted that:

- Whistleblowers may - on their own or through their trade union - report to the National Labour Inspectorate, for measures within its competence, any discriminatory action they may suffer as a result of their Report;
- any retaliatory or discriminatory dismissal of a Whistleblower is null and void;
- also null and void are any change of duties within the meaning of Art. 2103 of the Civil Code, as well as any other retaliatory or discriminatory measure taken against the Whistleblower.

The Group also acknowledges that, in the event of disputes related to the imposition of disciplinary sanctions, or to demotions, dismissals, transfers, or subjecting the Whistleblower to any other organisational measure having a direct or indirect negative impact on working conditions, following the submission of a Report, Legislative Decree 24/23 provides that the burden is on the employer to prove that the adoption of such measures is based on reasons unrelated to the Report.

b) Protection of confidentiality

All information received in the context of the Report will be treated confidentially by the Receiving Parties involved, in accordance with applicable law, so as to prevent third parties from becoming aware of it. The platform identified by the Group is designed to ensure that the confidentiality of the Whistleblower's identity is respected at all stages of the Policy. For more information on the processing of data carried out in the context of Reporting, please read the Privacy Notice at the end of this Policy and published on the Platform.

The Receiving Parties have received appropriate training to be able to act in full compliance with these principles. In addition, they received from expert.ai a specific authorisation pursuant to Art. 2 quaterdecies of Legislative Decree No. 196/2003 which commits them to complying with these specific confidentiality obligations.

The Receiving Parties may only share the information received to the extent that this is absolutely necessary for investigations and fact-finding.

The foregoing also applies to all those who, for whatever reason or necessity, may become aware of a Report and its contents, including the names of any persons involved.

As regards, in particular, the scope of disciplinary proceedings, the identity of the Whistleblower may only be disclosed in cases where the following requirements are met:

- the express consent of the Whistleblower;

- the disciplinary charge is based in whole or in part on the Report and the knowledge of the identity of the Whistleblower is indispensable for the defence of the accused, provided that the latter invokes and proves this circumstance at the hearing or by means of defence pleadings.

Therefore, subject to the above exceptions, without the Whistleblower's consent the identity of the Whistleblower and further information relating to the Report cannot be

shared with parties other than the Receiving Parties and the offices involved in the investigation of Reports.

In criminal proceedings, on the other hand, initiated against a person to whom the facts of a Report are attributed, the identity of the Whistleblower is covered by official secrecy until the closure of the preliminary investigation.

Should the judicial authority, for investigative purposes, wish to know the name of the Whistleblower, the competent corporate department shall disclose the Whistleblower's identity.

c) Protection from Reports Made Abusing This Policy

The Group guarantees adequate protection against forms of abuse of this Policy, such as unfounded reports, reports made with malice or gross negligence, or reports that are manifestly opportunistic and/or made for the sole purpose of harming the reported party or other persons, and any other case of misuse or intentional exploitation of this Policy, both during the investigation and after the end of the investigation. Submitting such Reports is a source of disciplinary liability for the Whistleblower.

If the Whistleblower's bad faith is established, the protection of confidentiality lapses and the person to whom the facts are attributed is informed of the Whistleblower's identity, in order to grant him/her the right to file a complaint for libel or slander.

d) Support measures

For the best handling of a Report, the Whistleblower can turn to Third Sector entities (the list of which can be found on the website of ANAC (Italian National Anti-Corruption Authority), which provide assistance and advice free of charge:

- on how to report;
- on the protection against retaliation recognised by national and EU legislation;
- on the rights of the person involved;
- on the terms and conditions of access to legal aid.

e) Limitations of liability

Whistleblowers do not incur any civil, criminal, administrative or disciplinary liability when disclosing information covered by the obligation of secrecy, with respect to:

- disclosure and use of official secrets (Art. 326 Criminal Code);
- disclosure of professional secrecy (Art. 622 Criminal Code);
- disclosure of scientific and industrial secrets (Art. 623 Criminal Code);
- breach of the duty of loyalty (Art. 2105 Criminal Code);
- infringement of copyright protection provisions;
- violation of data protection provisions;
- disclosure or dissemination of information about violations that harm the reputation of the person involved.

The limitation of liability also applies to conduct, acts or omissions on the part of the entity or person if they are related to the Report and strictly necessary to disclose the breach (and are not superfluous).
Exemption from liability operates only if certain conditions are met, such as:

- the acquisition of the information or the access to the documents took place in a lawful manner (e.g. the Whistleblower made copies of documents/acquired knowledge of the contents of another colleague's e-mail with the latter's consent);
- at the time of the Report, the Whistleblower had reasonable grounds to believe that the information was necessary to uncover the breach (the prerequisite is not met, for instance, in the case of vindictive or opportunistic purposes);
- the Whistleblower had reasonable grounds to believe that the information was true and fell within the scope of Reports, having also submitted a Report in the manner provided for in this Policy.

6. The Process

6.1 Sending a Report

Staff and Third Parties may send Reports, by accessing the Platform, the link to which is published on the expert.ai website and here Corporate Governance - expert.ai | expert.ai following the instructions, as soon as they become aware of events relevant to this Policy.

Should a member of Personnel receive a Report from other parties (e.g. employees/third parties), without prejudice to the obligation of absolute confidentiality, he/she is obliged to transmit the Report on the Platform with any supporting documentation received, not retaining a copy of it and refraining from taking any independent initiative of analysis and/or investigation.

Failure to forward a received Report constitutes a violation of this Policy, with the application, in the event of proven bad faith of such conduct, of disciplinary sanctions.

6.2 Channels for Submitting a Report

A Report must be submitted, following access to the Platform, by filling in a special form and following the instructions therein. A Whistleblower may opt for anonymity or declare his or her identity, as he or she chooses.

In addition, it is possible to send a Report by paper mail (using the form at the end of this Policy) by placing it into two sealed envelopes, one containing the Report and the other with the data of the Whistleblower, if he/she does not wish to submit a Report anonymously. Both envelopes must be enclosed in a further envelope marked on the outside: *"Confidential-whistleblowing"*. The Report should be sent to the following address:

- FAO Francesca Petronio
  Viale Virgilio 48/H
  41123 Modena

Following the Report, the Receiving Parties will issue an acknowledgement of receipt of the Report to the Whistleblower, again via the Platform, within 7 (seven) days from the date of receipt of the Report.

Alternatively, at the request of the Whistleblower, the Report may be submitted by means of a face-to-face meeting with the Receiving Parties, set within a reasonable period of time; the Report, with the consent of the Whistleblower, is documented by the staff member in charge by means of a recording on a device suitable for storage and listening,

or by means of written minutes. In the latter case, the Whistleblower may verify, rectify and confirm the minutes of the meeting with his signature.

The Whistleblower may decide to be assisted by a Facilitator throughout the procedure.

It is also possible to submit a Report in oral form via the Platform.

6.3 Content of the Report

The Report must contain all the elements necessary to ascertain the truthfulness of the facts that are the subject matter of the communication, in order to allow the Receiving Parties to carry out the necessary verifications.

To this end, a Report should contain the following elements. It should be noted that even Reports lacking one or more of these elements will be taken into account, provided they contain sufficient elements to allow internal investigations to be pursued. In particular, a Report must contain:

(i) a clear and complete description of the facts that are the subject matter of the Report;
(ii) if known, the circumstances of time and place under which the reported facts were committed;
(iii) if known, the particulars or other elements allowing the identification of the person or persons who have carried out the reported facts (e.g. job title or the sector in which the activity is carried out);
(iv) an indication of any other persons who are aware of or may report on the facts that are the subject matter of the Report;
(v) any documents that may confirm the accuracy of the reported facts;
(vi) any other information that may provide useful feedback on the existence of the reported facts.

6.4 Preliminary verification

All Reports are subject to a preliminary analysis carried out by the Receiving Parties in order to verify the presence of useful data and information to allow an initial assessment of the merits of the Report, so as to identify the potential regulatory scope (e.g. Legislative Decree 231/2001, anti-corruption, money laundering, etc.).

The Receiving Parties will diligently follow up the Report and communicate with the Whistleblower, if necessary being able to request additional information from the latter via the Platform.

At the end of the preliminary verification, or in any case within a maximum period of 3 (three) months from the acknowledgement of receipt of the Report or, in the absence of such notice, within 3 (three) months from the expiry of the 7 (seven) day period from the Report, the Receiving Parties: close the Report, giving adequate reasons, if it emerges that there are no sufficiently circumstantiated elements or, in any case, that the facts referred to in the Report are unfounded; such closure is communicated to the Whistleblower;

- if the Report concerns facts and/or conduct that are not covered by this Policy, they close the Report, with the relevant reasons, and forward its contents to the competent corporate departments;
- if the Report requires further investigation, they proceed with the assessment of the Reports, as described below.

The Platform ensures that, should the Report concern one or more of the Receiving Parties, it will not be sent to the Receiving Parties but to another person who is not in a situation of conflict of interest.
Consequently, the entire process of handling such a Report (including the communication of the final outcome) will not be the responsibility of the Receiving Parties involved in the Report.

6.5 Evaluation of Reports

Where, as a result of the preliminary analysis, useful and sufficient elements emerge or are in any case inferable for an assessment of the merits of the Report, without prejudice to the right of defence of the person to whom the facts referred to in the Report relate, the Receiving Parties shall:

a) initiate specific analyses and carry out the verifications deemed necessary for the purposes of ascertaining the facts reported, by means of appropriate activities, including the hearing of the persons who may report on the facts that are the subject of the Report, availing themselves of the competent structures (possibly also by means of audits or through specialised third party companies) and involving the corporate departments concerned by the Report that may be informed of the facts that are the subject matter of the Report;
b) obtain internal Group documents where relevant to the ascertainment of the facts that are the subject matter of the Report;
c) proceed to hearing the person to whom the reported facts relate when this does not prejudice the performance of the activities and protections afforded to the Whistleblower under paragraph 5;
d) terminate the investigation at any time, if, in the course of the investigation, it is established that the Report is unfounded, without prejudice to the provisions under g);
e) make use, if necessary, of experts from outside the Group specialised in carrying out investigations, or experts in specialised legal matters related to the subject matter of the Report;
f) agree, with the management of the department concerned by the Report, on any action plan necessary to remove any control weaknesses detected, also ensuring the monitoring of the implementation;
g) agree with the departments concerned on possible initiatives to be taken to protect the Group's interests (e.g. legal action, suspension/cancellation of suppliers);
h) request the initiation of disciplinary proceedings against the Whistleblower, in the event of Reports that prove to be unfounded and in relation to which the Whistleblower is found to have acted with malice, informing the SB where necessary;
i) request the initiation of disciplinary proceedings against those who have violated the Whistleblower protection measures, informing the SB where necessary;

j) take appropriate measures, if the Report refers to Personnel and is well-founded, and the Receiving Parties shall promptly inform the SB of such measures, where necessary;
k) submit for assessment by the Board of Directors and the Board of Statutory Auditors the results of the investigation into the Report, if it refers to members of the Board of Directors or the Board of Statutory Auditors and is well-founded, so that the most appropriate measures may be taken against such Reported Persons. It will be the responsibility of the Board of Directors and the Board of Auditors to inform the Supervisory Board of such measures in a timely manner, where necessary;
l) submit to the competent division the results of the investigation into the Report, if it relates to third parties with whom business relations exist and it is well-founded, so that the most appropriate measures may be taken against such reported parties (e.g. termination of the contractual relationship). It will be the responsibility of the relevant division to inform the Receiving Parties of such measures in a timely manner.

Minutes of each hearing must be drawn up and signed by all those who attended the hearing (including the declarant party).

The Receiving Parties inform the Reported Person of the facts against him/her so that he/she can defend him/herself and exercise his/her rights. The Reported Person will be informed confidentially and securely and given instructions on how to exercise his or her rights.

However, the Receiving Parties may decide, if they have reliable and materially verifiable evidence, to take precautionary measures, in particular to prevent the destruction of evidence relating to the Report, before informing the Reported Person of the process of analysing the Report.

The Reported Person has no right to know the identity of the Whistleblower.

Within the framework of disciplinary proceedings, the identity of the Whistleblower may not be disclosed if the disciplinary allegation is based on investigations that are separate and additional to the Whistleblowing, even if consequent to the Whistleblowing. If, on the other hand, the disciplinary charge is based, in whole or in part, on the Report, and knowledge of the identity of the Whistleblower is indispensable for the defence of the accused, that identity may be disclosed, but only with the express consent of the Whistleblower to the disclosure of his/her identity.

The request for consent shall be made to the Whistleblower in writing and shall contain an indication of the reasons for disclosing the confidential data.

In any case, no disciplinary proceedings (whether provided for in the employment contract and/or in the disciplinary system pursuant to Legislative Decree 231/2001) will be initiated against the Reported Person because of the Report received, unless and until there is concrete evidence concerning its content.

At the end of the assessment of the Reports, or in any case within a maximum of 3 (three) months from the date of issue of the acknowledgement of receipt of the Report or, in the absence of such an acknowledgement, within 3 (three) months from the expiry of the period of 7 (seven) days from the submission of the Report, the Receiving Parties will

provide feedback on the final outcome of the Report to be communicated to the Whistleblower via the Platform.

7. Periodic reporting

The Receiving Parties prepare a six-monthly account indicating the Reports

(i) received during the reporting period;
(ii) received in previous months, but not yet closed in the reporting period;
(iii) closed in the reporting period.

The Report shows the status of each Report (e.g. received, open, proposed for closure, closed, under assessment/audit, etc.) and any action taken. The Receiving Parties forward the Reports' account to: (i) the Chairman of the Board of Directors, (ii) the Managing Director, (iii) the Board of Auditors.

Where deemed necessary, the Receiving Parties shall promptly inform the Chairman of the Board of Directors and the Managing Director of events or information concerning specific Reports, in order to promptly share and implement the most appropriate actions to protect the company's assets, always in compliance with the relevant external and internal regulations.

The audits conducted on the basis of this Policy do not alter the prerogatives and autonomy attributed to the Board of Statutory Auditors and the Chief People Officer by law and by the company's internal regulations, who may therefore consider exercising their own autonomous powers of control upon receipt of the information addressed to them on the basis of this Policy and the Account of Reports.

8. Retention of Documentation

In order to ensure the management and traceability of the Reports and of the Policy, the Receiving Parties shall prepare and update all the information concerning the Reports and ensure the filing of all the related supporting documentation for a period not exceeding 5 (five) years from the date of the communication of the final outcome of the Policy, except in the case of proceedings before the judicial authorities for which it would be necessary to keep the documentation beyond that period.

9. The External Reporting Channel

The Whistleblower may also opt to make an external Report through the channels activated by the National Anti-Corruption Authority (ANAC) if, at the time of its submission, at least one of the following conditions is met:

- if the internal reporting channel is not active or, even if activated, does not comply with the regulations;
- if the Whistleblower has already made an internal Report and the Report has not been followed up;
- if the Whistleblower has reasonable grounds to believe that, if he or she makes an internal Report, it will not be effectively followed up or that it may lead to the risk of retaliatory acts;

- if the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

In any case, the terms of access to these channels and, in general, the rules on external reporting are set out in Leg. Decree No. 24/2023, to which reference is made, and are detailed by ANAC on its website and by means of special Guidelines that the Authority issues.

10. Public Disclosure

A further tool made available to the Whistleblower is the public disclosure of facts constituting violations that he/she has learned directly.

Although it is a separate system from the internal and external reporting channels, a publicly disclosing Whistleblower benefits from the protection provided for internal and external Whistleblowers if, at the time of public disclosure, at least one of the following conditions is met:

- the Whistleblower has previously made an internal Report and an external Report or has made an external Report directly, under the conditions and according to the procedures laid down in the legislation, and no reply has been received within the prescribed time limits on the measures envisaged and/or adopted to follow up on Reports;
- the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
- the Whistleblower has well-founded reasons to believe that the external Report may entail the risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the Receiving Party may be in collusion with the author of the violation or otherwise involved in the violation.

11. Sanctioning System

Penalties are provided for non-compliance with this Policy.

In particular, these are:

- disciplinary sanctions against the Whistleblower who has made Reports in bad faith and which turn out to be unfounded, if he/she is found guilty by a judgement (even of first instance) of criminal liability for the offences of slander or libel or for the same offences connected with the Report, or of civil liability for having intentionally or negligently reported false information;
- sanctions against the Receiving Parties or the persons in charge of the investigation in case of breach of the obligation to keep the identity of the Whistleblower and the content of the Report confidential;
- disciplinary sanction against the person to whom the facts that are the subject matter of the Report are attributed, in the event that the Receiving Parties, at the

outcome of the investigation, establish that the Report is well-founded, and internal disciplinary proceedings are initiated.

Any form of abuse, such as opportunistic Whistleblowing and/or Whistleblowing made for the sole purpose of harming the Reported Person or other persons, as well as any other case of improper use or intentional exploitation of Whistleblowing, shall also give rise to liability in disciplinary and other competent jurisdictions.

INFORMATION FOR THE PROCESSING OF PERSONAL DATA PURSUANT TO ART. 13 AND 14 OF REGULATION (EU) 2016/679 FOR WHISTLEBLOWING REPORTS

We inform you that, pursuant to Art. 13 and 14 of EU Regulation 2016/679 (hereinafter "**Regulation"** or "**GDPR"**), expert.ai S.p.A. with registered office in Rovereto (38068 - Trento, Italy), Via Fortunato Zeni, No. 8, VAT number 02608970360 (hereinafter "**expert.ai**"), Expert System Iberia SLU with registered office in Calle Poeta Joan Maragall, 3-5 Escalera Izquierda, Planta 1, Derecha 28020 Madrid (España), VAT number ES B66425513 (hereinafter "**Expert System Iberia"**), Expert System France SA with registered office in 15 - 17, rue Traversiere, 75012 Paris (France), VAT number FR81432265585 (hereinafter "**Expert System France"**), Expert System Deutschland GMBH with registered office in Theodor-Stern-Kai 60596 Frankfurt am Main (Germany), VAT number DE813075265 (hereinafter referred to as "**Expert System Deutschland**") are the Joint Data Controllers (hereinafter referred to as the "Joint Data Controllers**"**) of personal data collected in the context of reports of violations of national or European Union law that harm the public interest or the integrity of the Joint Controllers (hereinafter referred to as "**Whistleblowing Reports"**). The Joint Data Controllers have regulated their respective roles and responsibilities in an agreement drafted pursuant to Art. 26 of the Regulation, the essential content of which is made available on request by writing to privacy@expert.ai.

This document does not replace but supplements the further information already delivered previously (e.g. employees, suppliers, etc.) and therefore the information already provided there will not be repeated.

1. Joint Data Controllers

The Joint Data Controllers of your personal data, i.e. the entities that define the manner and purpose of the processing of your personal data, are expert.ai, Expert System Iberia, Expert System France, Expert System Deutschland as defined above. For any information concerning the processing of personal data by the Joint Holders, please write to the following address: privacy@expert.ai.

The Joint Data Controllers have appointed a *Data Protection Officer* ("**DPO"**) who is available for any information concerning the processing of your personal data at dpo@expert.ai.

2. Categories and Types of Personal Data Processed

The personal data subject to processing could be, only if you decide to disclose your identity, your personal data (including but not limited to your first name, last name, e-mail address, etc.) as well as the identification data of the Reported Person and the names of other persons who may report on the facts that are the subject of your Whistleblowing Report. Moreover, in the context of the reports, data may be disclosed that fall under the so-called "special categories" of personal data within the meaning of Art. 9 of the GDPR (i.e. data disclosing racial or ethnic origin, religious, philosophical or other beliefs, political

opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or trade union nature, as well as personal data disclosing health and sex life) and so-called judicial data within the meaning of Article 10 of the GDPR (i.e. data relating to criminal convictions and offences). In general, please do not provide such categories of data of yourself or of third parties, unless this is strictly necessary for the purposes of Whistleblowing Report.

3. Purpose and legal basis of personal data processing

Your personal data will be processed, within the limits set out above, for the purpose of receiving, analysing and handling your Whistleblowing Report. The legal basis for such processing is a legal obligation, and in particular the provisions of Leg. Decree 24/2023, referred to in Art. 6(1)(c) of the Regulation. Any processing of personal data falling into the categories of special data or judicial data is carried out by the Joint Data Controllers in fulfilment of obligations in the field of labour safety and social security pursuant to Art. 9(2)(b) of the Regulation.

We point out that once the Whistleblowing Report has been handled, its contents may be further used for the legal protection of the Joint Data Controllers and for the necessary defence actions. In this case, the legal basis for the processing of such personal data is the legitimate interest of the Joint Data Controllers pursuant to Art. 6(1)(f) of the Regulation.

Whistleblowing could also be used to instigate disciplinary or sanctioning action in the event of pretextual, retaliatory or discriminatory conduct against the Reported Person or the Whistleblower. This processing is carried out on the basis of the applicable legal provisions (Legislative Decree No. 24/2023).

In the event of a Whistleblowing Report being submitted orally, it will be transcribed, subject to your express consent, which you may give using the form below. Please note that it is not compulsory to give your consent to the registration of the Whistleblowing Report and in the event of failure to do so, the Whistleblowing Report will still be handled, with its contents being transcribed. Please note that you can always check and confirm or rectify the content of the Whistleblowing Report transcript. The retention periods for such Whistleblowing Reports are the same as those indicated below.

4. Anonymity in Reporting

Please note that you may also send a Whistleblowing Report anonymously, which will nevertheless be taken into account and analysed. With regard to the identity of the Reported Person, the provision of his/her personal data is similarly optional, but the Whistleblowing Report may be disregarded if this is not materially possible.

Moreover, if you have expressly decided to disclose your identity when submitting the Whistleblowing Report, your personal data will only be processed by staff authorised to carry out such activities and who have committed to confidentiality. This is without prejudice to the sharing of the content of the Whistleblowing Report with the persons prescribed by law (see Section 5.d).

5. Recipients

Your personal data and, more generally, all personal data communicated with the Whistleblowing Report, together with the documentation supporting it, may be shared, to the extent strictly necessary, with the following parties bound to confidentiality "**Recipients"**):

a) Collegial Bodies of the relevant Contact Persons and only those persons strictly necessary to follow up the Whistleblowing Report who have committed themselves to confidentiality, including the **facilitator**, if any;

b) **any external legal advisors, as well as platform suppliers** with whom the Joint Data Controllers have signed contracts for the processing of data pursuant to Art. 28 of the GDPR and who, therefore, act as data controllers;

c) **entities, bodies or authorities** to whom it is obligatory to communicate your personal data by virtue of legal provisions or orders by the authorities.

6. Data Transfer

The Joint Data Controllers may transfer some of your personal data outside the European Economic Area. In such cases, the Joint Data Controllers assure you that such transfers will be supported by adequate safeguards (such as EU Standard Contractual Clauses) and/or other legal bases in accordance with applicable European legislation. More information is available from the Joint Data Controllers.

7. Data Retention

Whistleblowing Reports will be dealt with within three months from the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within three months from the expiry of the seven-day period from the submission of the Whistleblowing Report. Whistleblowing Reports and the related documentation are kept for the time necessary for the processing of the Whistleblowing Report and in any case no longer than five years from the date of the communication of the final outcome of the Whistleblowing Report procedure, in compliance with the confidentiality obligations set out in Article 12 of Legislative Decree no. 24/2023 and the principle laid down in Art. 5(1)(e) of the Regulation.

8. Data Processing Methods

The data will be processed using computer, manual and/or IT supports and/or tools, under a logic strictly related to the purposes of the processing and, in any case, guaranteeing the confidentiality and security of the data and in compliance with the Regulation. This is with particular reference to the Whistleblower's data, which will be protected by anonymity (unless the Whistleblower wishes to disclose his or her identity).

9. Your Rights

You have the right to ask the Joint Data Controllers at any time:

- **to access** to your personal data: we will provide the personal data we have on you, where applicable, the source of your data. This right is not actually exercisable by the person reported in a Whistleblowing Report;
- to make your personal data **portable**: where applicable, we will provide you with an excel file containing the personal data we have on you;
- **to rectify** your personal data if you believe they are incorrect or need to be updated;
- **to limit** the processing of your personal data: for example, if you consider that our processing is unlawful and/or that some processing carried out on the basis of our legitimate interest is inappropriate;
- **to delete** your personal data;
- **to object** to the processing of your personal data.

The response time under European law to which we are subject is 1 month from your request (extendable up to a further 2 months in cases of particular complexity).

Please note that pursuant to Art. 2 *undecies* Legislative Decree 196/2003, the rights referred to in Articles 15 to 22 of the Regulation may not be exercised by making a request to the Joint Data Controllers or by lodging a complaint pursuant to Article 77 of the Regulation where the exercise of such rights may result in actual and concrete prejudice to the confidentiality of the identity of the Whistleblower, such prejudice being assessed on a case-by-case basis, in concrete terms, and only where it is a necessary and proportionate measure. If the Joint Data Controllers make use of this limitation, you will be notified without delay in writing. We remind you that, in such cases, your rights may also be exercised through the Data Protection Authority in the manner set out in Art. 160 of Leg. Decree 196/2003 as amended and integrated.

You may exercise your rights by writing to the following e-mail address: privacy@expert.ai and to the physical address of the Joint Data Controllers listed above. You can always contact the DPO by writing to dpo@expert.ai.

In any case, you always have the right to lodge a complaint with the competent supervisory authority (Garante per la Protezione dei dati personali [Italian Data Protection Authority]), pursuant to Art. 77 of the Regulation, if you consider that the processing of your personal data is contrary to the legislation in force, or to take appropriate legal action (Art. 79 of the Regulation), subject to the limits of Art. 2 *undecies* of Leg. 196/2003 above.

***

CONSENSUS WORDING:

The undersigned, having read and understood the above privacy statement

[ ] consents [ ] does not consent

to the recording of the Whistleblowing Report submitted orally.

ANNEX:

FORM FOR REPORTING UNLAWFUL CONDUCTS

The report concerns the violation or suspected violation of the Code of Ethics or of the Organisation, Management and Control Model pursuant to Legislative Decree No. 231/2001 and/or the law of the European Union, as well as the Group's procedures/policies, or any other active or omissive conduct, whether proven or suspected, that may represent a breach of the obligations arising from the employment contract between the Group and its employees and/or assimilated personnel, or its contractors.

Whistleblowers are protected against any form of retaliation or discrimination in the professional sphere, and the confidentiality of their identity is guaranteed within the limits provided for by law or determined by the need to protect the Group.

Reports received and the appropriateness of follow-up action are assessed by hearing, if necessary, the Whistleblower and/or the person responsible for the alleged violation.

The use of the report made for mere retaliatory or emulative purposes shall be sanctioned.

AUTHOR OF THE REPORTED CONDUCT:
DETAILED DESCRIPTION OF THE BEHAVIOUR GIVING RISE TO THE ALERT:
DATA OF THE WHISTLEBLOWER (IN CASE OF A NON-ANONYMOUS REPORT):
First and last name:
Job title:
Contact (telephone or e-mail):
Date Signature

REVIEWS

VERSION	ISSUE DATE	COMMENT	SIGNATURE
V.01	01/02/2021	First issue	
V.02	15/12/2023	Second issue	
V.03		Third issue	

EXPERT.AI S.P.A.
Registered office: Via Fortunato Zeni, 8 – 38068 Rovereto (TN)
Administrative offices: via Virgilio 56/Q - 41123 Modena, Italy
Tel. +39 059 894011 – Fax +39 059 894099
VAT no. 02608970360 - Share capital € 689,017.58 fully paid up.
Registered with the Trento Register of Companies, no. 02608970360

www.expert.ai – info@expert.ai