

Whistleblowing Policy

APPROVED BY THE BOARD OF DIRECTORS ON 20 December 2023

Drafted by: Legal Function - Compliance

Contents

- 1. Introduction 3**
- 2. Recipients, purpose, protected subjects and scope 3**
- 3. Roles and Responsibilities in the Management of Reports 4**
- 4. Online Platform for Reporting 4**
- 5. Content of Reports 4**
- 6. Management of Reports 5**
- 7. Additional Reporting Channels 5**
- 8. Safeguards: processing of personal data, confidentiality, prohibition of
retaliation and support measures 6**
- 9. Responsibility of the Whistleblower 7**
- 10. Data Protection and Archiving of Reporting Documents 7**

1. Introduction

This Policy is intended to establish the rules and procedures for reporting (“**Report**”) unlawful conduct, either commission or omission, of which a person has become aware in a work context, which constitutes or may constitute a violation of laws and/or regulations (national or of the European Union) in any case applicable to FAI SERVICE S. Coop. (the “**Company**” or “**FAI SERVICE**”) and/or its subsidiaries (“**Group**”), as well as of the internal control system, procedures and corporate rules in force within the Group, including the Code of Ethics and the Organisational and Management Model according to Italian Legislative Decree no. 231/01 adopted by FAI SERVICE (the “**Model**”).

This Policy constitutes the reference for the companies of the Group, without prejudice to any specific laws governing the same subject matter at local level that conflict with it.

The principles of this Policy do not impair or limit in any way the obligations to report to the competent Judicial, Supervisory or Regulatory Authorities in the countries in which the companies operate, nor the obligations to report to any control bodies that may be set up in each Group company.

2. Recipients, purpose, protected subjects and scope

The recipients of this Policy (hereinafter referred to as “**Recipients**”) are:

- top management and members of corporate bodies of FAI SERVICE and the Group companies;
- employees of FAI SERVICE and Group companies;
- suppliers, partners, consultants, shareholders and, more generally, stakeholders of FAI SERVICE and the Group companies (hereinafter “**Third Parties**”).

The purpose of this Policy is to regulate the process of receiving, analysing and processing Reports from anyone sent and/or transmitted, even in anonymous form.

Reports may concern, in general, all conduct, acts or omissions that may constitute unlawful conduct and, in particular:

- reports of criminal conduct;
- reports of conduct in breach of laws or regulations, codes of conduct or other company provisions that may be subject to disciplinary sanctions;
- reports of conduct likely to harm the image of the Company and/or the Group;
- communications of alleged unlawful conduct pursuant to Italian Legislative Decree no. 231/01 or violations of the Model, where applicable.

The following reports are not admissible and manageable:

- general or personal grievances;
- communications whose content refers to private life, unless they are work-related in relation to possible offences or violations of internal rules.

The whistleblower is required to set out in a clear and, if possible, complete manner the elements useful to carry out the checks and investigations necessary to verify the validity and objectivity of the report, indicating, by way of example but not limited to:

- references as to the course of events (e.g. date, place), any information and/or evidence of what was reported;
- general information or other elements that make it possible to identify the reported person;
- details of any other persons who may report on the facts that are the subject of the Report;
- any private interests linked to the Report.

Although the Company, in accordance with the Code of Ethics, considers Reports transmitted non-anonymously to be preferable so that appropriate checks and consequent measures can be more effectively carried out, anonymous Reports are also encouraged, provided they are suitably substantiated.

3. Roles and Responsibilities in the Management of Reports

The person in charge with the Report management process is FAI SERVICE's **Supervisory Board** (“**SB**”) which, depending on the nature, character and/or complexity of the Report, may rely on the support and cooperation of the competent internal company departments (such as, for example, the legal department, the personnel department, the administrative department) and/or external consultants to carry out the relevant preliminary investigation.

In the event that the Report involves the SB or a member thereof, the management of the Report will be carried out by the FAI SERVICE Board of Directors, which will take appropriate advice.

4. Online Platform for Reporting

Reports should be submitted **electronically** by accessing the “*Whistleblowing Policy and Reporting Platform*” section of the corporate website, or by clicking directly on: <http://Segnalazioni.lumesia.com> (the “**Portal**”).

Only members of the SB, through automatic receipt notification mechanisms, will be able to read and download the Reports.

Access to the Portal is subject to the “no-log” policy: even if access to the platform for sending Reports is made from a computer connected to the FAI SERVICE company network, it cannot be traced by the company information systems, to protect the anonymous whistleblower.

The Portal access page contains further practical information on the correct use and operation of the platform.

Without prejudice to the above with reference to the reporting methods, it should be noted that any Reports received by persons other than the SB must be forwarded by the recipient to the SB, again through the Portal, **as soon as possible**.

All Reports, regardless of the method of receipt/uploading, will be registered in the Portal, which will be the database summarising both the essential data of such Reports and their management (tracked by workflow), also ensuring the archiving of all attached documentation, as well as that produced or acquired in the course of analysis activities.

5. Content of Reports

The Portal provides a guided path for the whistleblower, through a series of open and closed questions, some compulsory, others optional, concerning facts, temporal context, economic size, personal information about the whistleblower (optional), further supporting elements, with the aim of skimming unaccountable or insignificant Reports from the outset. Reporting, as explained above, may also be done in a totally anonymous form.

At the end of the Report, the whistleblower will be issued a ticket through which he/she can later access his/her Report again and monitor its progress.

This will make it possible, should the whistleblower wish to do so, to request, where appropriate, further details or support for the Report itself, always with the utmost protection of the confidentiality and/or anonymity of the whistleblower.

6. Management of Reports

Once the report has been received, the SB will carry out the following activities:

- a) it sends the whistleblower an **acknowledgement of receipt** of the report **within 7 (seven) days** from the date of receipt;
- b) it may request additional information from the whistleblower, if necessary;
- c) it provides for appropriate verification of the Reports received;
- d) it provides feedback to the Report **within the following 3 (three) months**.

As set out in Article 3 above, depending on the nature, character and/or complexity of the Report, the SB may rely on the support and cooperation of the competent internal company departments (such as, for example, the legal department, the personnel department or the administrative department) and/or external consultants to carry out the relevant preliminary investigation.

There are three phases in the management process of Reports: reception, preliminary investigation and assessment.

Upon receipt of a new Report, the members of the SB analyse its contents. If the Report is irrelevant, the SB is entitled to disregard it and to inform the Whistleblower that it will not be further investigated (reception phase). If the SB deems it necessary to receive further information, it may request further details or support for the Report from the Whistleblower, via the Portal.

If, following the assessments carried out, the Report proves to be well-founded, the adoption of disciplinary measures against the reported person in accordance with the legislation applicable to the case in question will be assessed in agreement with the competent functions of the individual Group companies.

If the investigations carried out reveal situations of violations of the Model and/or the Code of Ethics, or if the SB has developed a well-founded suspicion that an offence has been committed, the SB shall promptly communicate the Report and its assessments to the President, the Managing Director and, at the first possible meeting, to the Board of Directors, as well as to the top management of the Group company(ies) that may be involved in the Report, unless the Report does not concern such parties.

The SB shall prepare an information report, to be annexed to its half-yearly report for the Board of Directors of the Company, in which it shall acknowledge the Reports received and the measures taken during the six months in question.

7. Additional reporting channels

Although the whistleblower is encouraged to make any Report through the Portal, in the cases and in the manner provided for by locally applicable legislation, Reports may be made to the competent local authorities, bodies or institutions.

A non-exhaustive list of external competent authorities is available below:

Country	Competent authorities	Link to site
Italy	Italian National Anti-Corruption Authority (“ANAC”)	https://www.anticorruzione.it/-/whistleblowing
Austria	Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung (“BAK”)	https://www.bak.gv.at/
France	Défenseur des droits	https://www.defenseurdesdroits.fr/fr
Poland	<i>To be identified</i>	<i>To be identified</i>
Spain	Autoridad Independiente de Protección del Informante	www.antifrau.cat www.antifraucv.es

Please also note that acts or facts relating to Lumesia Insurance S.r.l., which may constitute violations of the provisions of the Private Insurance Code, as well as of directly applicable European Union provisions, may be reported to IVASS.

8. Safeguards: processing of personal data, confidentiality, prohibition of retaliation and support measures

This Policy guarantees the protection towards the whistleblower and the reported person with regard to privacy (so-called Personal Data Processing) and, in particular, the confidentiality of the personal data of the persons involved is guaranteed in accordance with Italian and European legislation (Italian Legislative Decree 196/03, as amended by Italian Legislative Decree 101/2018, and EU Regulation 2016/679).

In particular:

- a) Reports may not be used beyond what is necessary to adequately follow them up;
- b) the identity of the whistleblower and any other information from which that information can be deduced, directly or indirectly, may not be disclosed, without the express consent of the whistleblower, to persons other than those responsible for receiving or following up reports and expressly authorised to process such data;
- c) in criminal proceedings, the identity of the whistleblower is protected pursuant to Article 329 of the Italian Code of Criminal Procedure; / in proceedings before the Italian Court of Auditors, the identity of the Whistleblower cannot be disclosed until the preliminary investigation phase is closed / in disciplinary proceedings, the identity of the Whistleblower cannot be disclosed where the allegation of the disciplinary offence is based on separate and additional investigations to the Report, whereas the Whistleblower's express consent is required where knowledge of his/her identity is indispensable for the accused's defence;
- d) the protection of the identity of the persons involved and of those mentioned in the Report is guaranteed, subject to the disclosures strictly necessary for the ascertainment of the necessary facts and/or for the consequent measures in the event of a positive finding, in the same way as for the protection of the whistleblower;
- e) in Whistleblowing procedures, the person concerned may be heard, without the identity of the Whistleblower being revealed, if known. On the other hand, the reported person has the right to be heard and to have access to the file of the Report, in the case of disciplinary proceedings initiated as a result of the Report. In such a case, however, the identity of the Whistleblower may only be disclosed if the charge is based, in whole or in part, on the Report, if knowledge of the Whistleblower's identity is necessary for the accused's defence, and if the Whistleblower has given his/her express consent to the disclosure of his/her identity, otherwise the Report cannot be used for the purposes of the disciplinary proceedings;
- f) personal data not necessary for the processing of a specific Report are not collected or, if accidentally collected, are deleted immediately.

FAI SERVICE will not tolerate threats or retaliation of any kind against the Whistleblower and/or those who have collaborated in the activities of verifying the validity of the Report. Thanks to this Policy, FAI SERVICE guarantees the anonymity of whistleblowers, even in the case of their personal details are indicated, and reserves the right to take appropriate actions against anyone who carries out or threatens to carry out acts of retaliation against whistleblowers under this Policy. It is understood that FAI SERVICE or the individual Group companies within their competence may take the most appropriate disciplinary and/or legal measures to protect their rights, assets and image, against anyone who, in bad faith, has made false, unfounded or merely opportunistic Reports and/or for the sole purpose of slandering, defaming or causing prejudice to the reported person or other persons mentioned in the Report.

A list of institutions providing support measures for whistleblowers is provided by the competent authorities of each Member State.

The support measures consist of information, assistance and advice free of charge on how to report and on the protection from retaliation offered by national and EU legislation, on the rights of the person concerned and on the terms and conditions of access to legal aid.

The protections provided for in this Article also apply to:

- a) facilitators, i.e. natural persons assisting a whistleblower in the whistleblowing procedure, who are connected to the latter in terms of work;
- b) persons in the same work environment as the whistleblower who are linked to him/her by a stable emotional or family relationship up to the fourth degree;
- c) the whistleblower's work colleagues;
- d) entities owned by the whistleblower or operating in the same work environment as the whistleblower.

9. Responsibility of the Whistleblower

It is the responsibility of the whistleblower to make Reports in good faith and in line with the spirit of this Policy.

In cases of Reports made with wilful misconduct or gross negligence, the whistleblower is not protected by the measures provided for in Article 8 of the Policy and may be subject to disciplinary measures and/or reporting to the judicial authorities.

10. Data Protection and Archiving of Reporting Documents

Throughout the Report management process, the right to confidentiality of the identity of the whistleblower, of the person involved and of the person in any case mentioned in the Report, as well as of the content of the Report and of the relevant documentation, is preserved.

Therefore, the documentation relating to the Reports is also confidential. All documentation, whether on paper or computer, must be stored securely and in compliance with the rules in force within FAI SERVICE and the Group on the classification and processing of information and in accordance with the rules and regulations in force. This documentation must be filed by the SB and must only be accessible to the members of the SB or to persons expressly authorised by the same.

In particular, the documentation pertaining to each Report must be retained for as long as necessary for the processing of the Report and in any case no longer than the limit provided for by the applicable local regulations.

INFORMATION ON THE PERSONAL DATA PROCESSING OF THE WHISTLEBLOWERS

FAI Service S. Coop. (hereinafter, **FAI Service**) has adopted a whistleblowing procedure (the “**Whistleblowing procedure**”) aimed at encouraging, facilitating and managing the reporting of possible unlawful conduct within the company organisation, as well as reinforcing control over the effective application of and compliance with the applicable legislation, the Organisation, Management and Control Model and the Code of Ethics of FAI Service, as well as the provisions and principles identified in FAI Service's policies and procedures, including the Company Regulations with which FAI Service employees must comply, in accordance with the provisions of the applicable legislation and, in particular, Italian Legislative Decree no. 24/2023 (on the “*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national laws*” - hereinafter, also, the “**Whistleblowing Decree**”).

In order to comply with the regulatory provisions on whistleblowing, the Whistleblowing procedure has also been implemented by all FAI Service's subsidiaries listed in Annex 1 (hereinafter, the “**Subsidiaries**” and, together with FAI Service, the “**Group**”).

For more information on the Whistleblowing procedure, please consult the section “*Corporate Documents - Whistleblowing Policy and Whistleblowing Platform*” available at www.faiservice.com.

We also inform you that, pursuant to Regulation (EU) No. 2016/679 (the “**GDPR**”) and Italian Legislative Decree No. 196/2003, as most recently amended by Italian Legislative Decree No. 101/2018 (the “**Privacy Code**”), the information and personal data provided by you in the report made and collected under the Whistleblowing procedure you have initiated will be processed by the Group company to which you make the report, as the data controller (hereinafter, the “**Data Controller**”) in the manner and for the purposes indicated in this Privacy Notice (“**Privacy Notice**”).

1. Identity and contact details of the Data Controller

The Data Controller is the Group company to which you send a report under the Whistleblowing procedure. Therefore, depending on who you decide to report an event or conduct to, the Data Controller may be FAI Service or one of its Subsidiaries.

For more information on the Group company acting as Data Controller for the report you submitted, please consult the list of Group companies in Annex 1 to this Policy.

2. Categories of processed data

The personal data processed as part of the Whistleblowing procedure will be your identification data as the reporting party (hereinafter also referred to as the “**Whistleblower**” or “**Data Subject**”), information concerning the conduct complained of, and any other data that you voluntarily submit during the Whistleblowing procedure depending on the type of report made or that are relevant on the basis of the reported event (hereinafter referred to as “**Personal Data**”).

In any case, only Personal Data that are strictly and objectively necessary to verify the merits of the report and proceed to its resolution are processed. Please note that reports can also be made anonymously, provided they are adequately documented.

In addition to the above, and exclusively where necessary to ascertain the reported conduct and to follow up on the report received, the Data Controller may also process special categories of personal data pursuant to Art. 9 of the GDPR or data relating to criminal convictions and offences pursuant to Art. 10 of the GDPR for reasons of relevant public interest as set out in the Whistleblowing Decree and in any event within the limits of what is permitted by the relevant legislation, including Articles 9 and 10 of the GDPR.

In any case, only Personal Data that are strictly and objectively necessary to verify the merits of the report and proceed to its resolution are processed. Should Personal Data be collected, even accidentally, that is manifestly not necessary for handling the report, such Personal Data will be deleted immediately.

3. Data processing purposes

The Personal Data of the whistleblower are processed for the following purposes:

- the application and management of the Whistleblowing procedure, including the verification of the facts that are the subject of the report, the resolution of the report, the preparation of the acknowledgement and the adoption of any relief or support measures for the whistleblowers, as well as to respond to questions and queries raised by the Data Subjects concerning corporate compliance (the “**Report Management Purposes**”);
- the fulfilment of obligations under the national and/or EU law, regulations or legislation, including the provisions of the Whistleblowing Decree (the “**Legal Purposes**”); and
- the exercise or defence of the rights of the Data Controller or the Group in judicial proceedings, as well as to ensure the proper management of the company, including through the implementation of FAI Service's internal policies and procedures such as the Whistleblowing procedure in order to minimise the risks of possible liability, damages or claims against FAI Service or its Subsidiaries (the “**Legitimate Interest Purposes**”).

4. Legal basis for data processing

The processing of Personal Data for the Report Management Purposes and Law Purposes is carried out pursuant to Article 6(1)(c) of the GDPR in order to manage and comply with applicable legal obligations in relation specifically to the Whistleblowing procedure and to provide feedback to reports received within the limits of the provisions of the Whistleblowing Decree. The processing of Personal Data for these purposes is therefore mandatory in order for the Data Controller to comply with the relevant legislation.

The processing of Personal Data for the Purposes of Legitimate Interest, on the other hand, is carried out pursuant to Article 6(1)(f) of the GDPR for the pursuit of the legitimate interest of the Data Controller who is fairly balanced with the legitimate interest of the Data Subject, as the processing activity of Personal Data is limited to what is strictly necessary for the exercise of the aforementioned rights. Processing for such Purposes of Legitimate Interest is not compulsory and Data Subjects may object thereto as indicated in this Privacy Policy. Should the Data Subject object to such processing, the relevant Personal Data may not be used for the Purposes of Legitimate Interest unless the Data Controller gives evidence of the presence of overriding compelling legitimate grounds or unless in case of the exercise or defence of a right pursuant to Article 21 of the GDPR.

In addition, any special categories of Personal Data referred to in Art. 9 of the GDPR or data relating to criminal convictions and offences pursuant to Art. 10 of the GDPR are processed for reasons of relevant public interest as set out in the Whistleblowing Decree and in any event within the limits of what is permitted by the relevant legislation, including Articles 9 and 10 of the GDPR.

The reports made by you shall under no circumstances be used by the Data Controller for discriminatory or retaliatory purposes against the Data Subjects.

5. Personal data processing methods

Personal Data is processed by manual or computerised means, suitable to guarantee their security, confidentiality and to prevent unauthorised access, dissemination, modification and misappropriation of data,

thanks to the adoption of appropriate technical, physical and organisational security measures, in compliance with the aforementioned legislation and the related confidentiality obligations and, in any case, in accordance with the purposes and methods set out in this Privacy Notice.

In particular, the IT systems adopted for the Whistleblowing procedure are configured in such a way as to prevent unauthorised access and ensure the complete confidentiality of the Personal Data provided, in compliance with the security measures deemed appropriate and adopted by the Data Controller.

6. Categories of persons to whom Personal Data may be disclosed or who may become aware of it and transfer of Personal Data abroad

For the pursuit of the purposes identified above and, in any case, within the limits of the provisions of this Privacy Notice - also in consideration of the nature and/or gravity of the breach reported - Personal Data may be disclosed to other companies of the Group or to third parties, who will process them in their capacity as data processors pursuant to Article 28 of the GDPR, as well as to the competent entities and/or authorities, also for the purpose of carrying out investigations and/or subsequent judicial proceedings, which may be initiated as a result of the verifications carried out within the Whistleblowing procedure.

In particular, the reports and related Personal Data will be communicated to the FAI Service Supervisory Board for the pursuit of the above-mentioned purposes.

In any case, the persons in charge of receiving, examining, managing and acknowledging reports, as well as any data processors, are duly appointed by the Data Controller (or by FAI Service on its behalf), which provides adequate operational instructions, with particular reference to the adoption of security measures, in order to ensure the confidentiality and security of Personal Data. For a complete list of the designated data processors and persons in charge of processing, please contact the Data Controller by writing to the address given in [Annex 1](#).

Personal Data will not be transferred to countries outside the European Economic Area. In any case, where the Data Controller transfers Personal Data to countries outside the European Economic Area, the Controller will provide appropriate safeguards for the purposes of such transfer, such as the European Commission's Standard Contractual Clauses, in accordance with Articles 45 and 46 of the GDPR.

7. Personal data retention period

The Personal data will be processed for as long as is strictly necessary to pursue the purpose stated above. In particular:

- in case of unsuccessful reports, i.e. where there is no breach, the Personal Data is deleted immediately or at the latest within 2 months of the communication of the outcome of the Whistleblowing procedure; or
- in case of a successful report, i.e. where a breach is established, Personal Data is retained for 5 years following the communication of the final outcome of the Whistleblowing procedure, except where retention for a later period is required for litigation, requests by competent authorities or under applicable law.

In any case, at the end of the retention period, the Personal Data shall be deleted or irreversibly anonymised.

8. Rights of the Data Subject

Pursuant to Article 15 *et seq.* of the GDPR, the Data Subject may exercise the following rights, at any time and free of charge and in any case within the limits of the applicable legislation:

- (a) obtain confirmation of the existence or non-existence of Personal Data concerning him/her;
- (b) know the origin of the Personal Data, the purposes of the processing and its methods, as well as the logic applied to any processing carried out by means of automated decision-making processes;

- (c) Check the accuracy of the Personal Data and request the updating, rectification, amendment or - if he/she is interested - integration of the Personal Data concerning him/her;
- (d) obtain the cancellation, transformation into anonymous form or blocking of any data processed in breach of the law, as well as to oppose, for legitimate reasons, their processing;
- (e) withdraw their consent, where previously given;
- (f) request the Data Controller the restriction of the processing of Personal Data relating to him/her if:
 - the Data Subject contests the accuracy of the Personal Data, for the period necessary for the Data Controller to verify the accuracy of such data;
 - the processing is unlawful and the Data Subject objects to the deletion of the Personal Data and requests that its use be restricted;
 - the Personal Data is necessary to the Data Subject for the establishment, exercise or defence of legal claims, although the Data Controller no longer needs them for the purposes of the processing;
 - the Data Subject has objected to the processing pursuant to Article 21 of the Privacy Regulation, pending verification of whether the Data Controller's legitimate reasons prevail over the rights and freedoms of the Data Subject;
- (g) object, at any time, to the processing of their Personal Data for purposes of Legitimate Interest, except where the Data Controller has overriding legitimate reasons or the need to assert or defend a right in any legal proceedings;
- (h) request the deletion of Personal Data concerning the Data Subject without undue delay;
- (i) obtain an electronic copy of his or her Personal Data, when the Data Subject wishes to receive Personal Data relating to him or her or to transmit them to a different controller, in cases where the Controller processes Personal Data on the basis of a contract, of his or her consent, or where the Personal Data is processed by automated means.

The Data Subject also has the right to lodge a complaint with the Data Protection Authority, if the conditions are met.

Pursuant to Art. 2-*terdecies* of the Privacy Code, in the event of the death of the Data Subject, the aforementioned rights relating to the Personal Data may be exercised by the person who has an interest of his/her own, or is acting to protect the data subject as his/her agent, or for family reasons worthy of protection. The Data Subject may expressly prohibit the exercise of some of the rights listed above by his or her assignees by sending a written declaration to the address indicated in Annex 1. The declaration may be revoked or modified later in the same manner.

Without prejudice to the foregoing, pursuant to Article 2-*undecies* of the Privacy Code and Article 12 of the Whistleblowing Decree, the rights listed above may not be exercised if the exercise of such rights may result in actual and concrete prejudice to the confidentiality of the identity of the Data Subject who reports a violation of which he/she has become aware by reason of his/her employment relationship with the Data Controller or by reason of the functions performed for the latter. Moreover, if there is a real risk that the disclosure of information concerning the Whistleblowing procedure may jeopardise the verifications under way or, in general, the proper performance of the Whistleblowing procedure itself, feedback to the Data Subject may be provided after this risk has ceased to exist.

In order to exercise the above rights, you may contact the Data Controller to whom you made your report at any time, by writing to the address given in Annex 1.

9. Amendments and updates

This Privacy Notice is updated to 30 November 2023.

In case of revision or updating of this document, also as a consequence of amendments or updates to the applicable legislation, the Data Controller shall inform you of the new features of the processing by publishing the updated text on the website www.faiservice.com and on the company notice board.

Annex 1

LIST OF DATA CONTROLLERS AND RELEVANT CONTACT DETAILS

<u>Company</u>	<u>Registered office</u>	<u>E-mail address</u>
FAI SERVICE S. COOP.	Viale Cassala 57, 20143 Milan (MI) (I)	privacy@lumesia.com
SAS EUROTOLL	35 Rue Camille Desmoulins 92130 Issy Les Moulineaux (F)	dpo@eurotoll.fr
TRACKY SERVICE ESPANA S.L.U.	c/Barreiros 1 of.107 Pol.Ind.Padrosa 17730 Llers (ES)	info@trackyservice.es
TRACKY SERVICE POLSKA SP. Z.O.O.	Rondo Daszynskiego 2b/26 00-843 Warszawa (PL)	info@trackyservice.pl
TRACKY SERVICE GMBH	Autobahnzollplatz a-9602 Thorl Maglern (AT)	info@trackyservice.at
LUMESIA INSURANCE SRL	Viale Cassala 57, 20143 Milan (MI) (I)	info@lumesiainsurance.com

**INFORMATION ON THE PERSONAL DATA PROCESSING
OF THE REPORTED PERSONS OR ANY THIRD PARTIES INVOLVED IN THE REPORT**

FAI Service S. Coop. (hereinafter, **FAI Service**) has developed a whistleblowing procedure (the "**Whistleblowing procedure**") aimed at encouraging, facilitating and managing the reporting of possible unlawful conduct within the company organisation, as well as reinforcing control over the effective application of and compliance with the applicable legislation, the Organisation, Management and Control Model and the Code of Ethics of FAI Service, as well as the provisions and principles identified in FAI Service's policies and procedures, including the Company Regulations with which FAI Service employees must comply, in accordance with the provisions of the applicable legislation and, in particular, Italian Legislative Decree no. 24/2023 (on the "*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national laws*" - hereinafter, also, the "**Whistleblowing Decree**").

In order to comply with the regulatory provisions on whistleblowing, the Whistleblowing procedure has also been implemented by all FAI Service's subsidiaries listed in Annex 1 (hereinafter, the "**Subsidiaries**" and, together with FAI Service, the "**Group**").

For more information on the Whistleblowing procedure, please consult the section "*Corporate Documents - Whistleblowing Policy and Whistleblowing Platform*" available at www.faiservice.com.

We also inform you that, pursuant to Regulation (EU) No. 2016/679 (the "**GDPR**") and Italian Legislative Decree No. 196/2003, as most recently amended by Italian Legislative Decree No. 101/2018 (the "**Privacy Code**"), the information and personal data provided as part of the Whistleblowing procedure and relating to the reported person (the "**Reported Person**") and/or any third parties involved in the report (hereinafter, jointly with the Reported Person, the "**Involved Parties**") will be processed by the Group company receiving the report, as the data controller (hereinafter, the "**Data Controller**") in the manner and for the purposes indicated in this document ("**Privacy Notice**").

1. Identity and contact details of the Data Controller

The Data Controller is the Group company to which a report is made under the Whistleblowing procedure. Therefore, depending on whom an event or conduct is reported to, the Data Controller may be FAI Service or one of its Subsidiaries.

For more information on the Group company acting as Data Controller for each report, please consult the list of Group companies in Annex 1 to this Policy.

2. Categories of processed data

The personal data processed as part of the Whistleblowing procedure are the identification data of the Involved Parties, information concerning the conduct complained of, and any other data transmitted during the Whistleblowing procedure depending on the type of report made or that are relevant on the basis of the reported event (hereinafter referred to as "**Personal Data**").

In any case, only Personal Data that are strictly and objectively necessary to verify the merits of the report and proceed to its resolution are processed. Should Personal Data be collected, even accidentally, that is manifestly not necessary for handling the report, such Personal Data will be deleted immediately.

In addition to the above, and exclusively where necessary to ascertain the reported conduct and to follow up on the report received, the Data Controller may also process special categories of personal data pursuant to Art. 9 of the GDPR or data relating to criminal convictions and offences pursuant to Art. 10 of the GDPR for reasons of relevant public interest as set out in the Whistleblowing Decree and in any event within the limits of what is permitted by the relevant legislation, including Articles 9 and 10 of

the GDPR.

Reports may also be made anonymously; however, they are subject to evaluation only if adequately documented.

3. Data processing purposes

The Personal Data of the Data Subject are processed for the following purposes:

- the application and management of the Whistleblowing procedure, including the verification of the facts that are the subject of the report, the resolution of the report, the preparation of the acknowledgement and the adoption of any relief or support measures for the whistleblowers (the “**Report Management Purposes**”);
- the fulfilment of obligations under the national and/or EU law, regulations or legislation, including the provisions of the Whistleblowing Decree (the “**Legal Purposes**”);
- the exercise or defence of the rights of the Data Controller or the Group in judicial proceedings, as well as to ensure the proper management of the company, including through the implementation of FAI Service's internal policies and procedures such as the Whistleblowing procedure in order to minimise the risks of possible liability, damages or claims against FAI Service or its Subsidiaries (the “**Legitimate Interest Purposes**”).

4. Legal basis for data processing

The processing of Personal Data for the Report Management Purposes and Law Purposes is carried out pursuant to Article 6(1)(c) of the GDPR in order to manage and comply with the legal obligation relating to the Whistleblowing procedure and to provide feedback to reports received within the limits of the provisions of the Whistleblowing Decree. The processing of Personal Data for these purposes is therefore mandatory in order for the Data Controller to comply with the relevant legislation.

The processing of Personal Data for the Purposes of Legitimate Interest, on the other hand, is carried out pursuant to Article 6(1)(f) of the GDPR for the pursuit of the legitimate interest of the Data Controller who is fairly balanced with the legitimate interest of the Data Subject, as the processing activity of Personal Data is limited to what is strictly necessary for the exercise of the aforementioned rights. Processing for such Purposes of Legitimate Interest is not compulsory and Data Subjects may object thereto as indicated in this Privacy Policy. Should the Data Subject object to such processing, the relevant Personal Data may not be used for the Purposes of Legitimate Interest unless the Data Controller gives evidence of the presence of overriding compelling legitimate grounds or unless in case of the exercise or defence of a right pursuant to Article 21 of the GDPR.

In addition, any special categories of Personal Data referred to in Art. 9 of the GDPR or data relating to criminal convictions and offences pursuant to Art. 10 of the GDPR are processed for reasons of relevant public interest as set out in the Whistleblowing Decree and in any event within the limits of what is permitted by the relevant legislation, including Articles 9 and 10 of the GDPR.

5. Personal data processing methods

Personal Data is processed by manual or computerised means, suitable to guarantee their security, confidentiality and to prevent unauthorised access, dissemination, modification and misappropriation of data, thanks to the adoption of appropriate technical, physical and organisational security measures, in compliance with the aforementioned legislation and the related confidentiality obligations and, in any case, in accordance with the purposes and methods set out in this Privacy Notice.

In particular, the IT systems adopted for the Whistleblowing procedure are configured in such a way as to prevent unauthorised access and ensure the complete confidentiality of the Personal Data provided, in compliance with the security measures deemed appropriate and adopted by the Data Controller.

6. Categories of persons to whom Personal Data may be disclosed and transfer of Personal Data abroad

For the pursuit of the purposes identified above and, in any case, within the limits of the provisions of this Privacy Notice - also in consideration of the nature and/or gravity of the breach reported - Personal Data may be disclosed to other companies of the Group or to third parties, who will process them in their capacity as data processors pursuant to Article 28 of the GDPR, as well as to the competent entities and/or authorities, also for the purpose of carrying out investigations and/or subsequent judicial proceedings, which may be initiated as a result of the verifications carried out within the Whistleblowing procedure.

In particular, the reports and related Personal Data will be communicated to the FAI Service Supervisory Board for the pursuit of the above-mentioned purposes.

In any case, the persons in charge of receiving, examining, managing and acknowledging reports, as well as any data processors, are duly appointed by the Data Controller (or by FAI Service on its behalf), which provides adequate operational instructions, with particular reference to the adoption of security measures, in order to ensure the confidentiality and security of Personal Data. For a complete list of the designated data processors and persons in charge of processing, please contact the Data Controller by writing to the address given in Annex 1.

Personal Data will not be transferred to countries outside the European Economic Area. In any case, where the Data Controller transfers Personal Data to countries outside the European Economic Area, the Controller will provide appropriate safeguards for the purposes of such transfer, such as the European Commission's Standard Contractual Clauses, in accordance with Articles 45 and 46 of the GDPR.

7. Personal data retention period

The Personal data will be processed for as long as is strictly necessary to pursue the purpose stated above. In particular:

- in case of unsuccessful reports, i.e. where there is no breach, the Personal Data is deleted immediately or at the latest within 2 months of the communication of the outcome of the Whistleblowing procedure;
- in case of a successful report, i.e. where a breach is established, Personal Data is retained for 5 years following the communication of the final outcome of the Whistleblowing procedure, except where retention for a later period is required for litigation, requests by competent authorities or under applicable law.

At the end of the retention period, the Personal Data shall be deleted or irreversibly anonymised.

8. Rights of the Data Subject

Pursuant to Article 15 *et seq.* of the GDPR, the Data Subject may exercise the following rights, at any time and free of charge and in any case within the limits of the applicable legislation:

- (a) obtain confirmation of the existence or non-existence of Personal Data concerning him/her;
- (b) know the origin of the Personal Data, the purposes of the processing and its methods, as well as the logic applied to any processing carried out by means of automated decision-making processes;
- (c) Check the accuracy of the Personal Data and request the updating, rectification, amendment or - if he/she is interested - integration of the Personal Data concerning him/her;

- (d) obtain the cancellation, transformation into anonymous form or blocking of any data processed in breach of the law, as well as to oppose, for legitimate reasons, their processing;
- (e) withdraw their consent, where previously given;
- (f) request the Data Controller the restriction of the processing of Personal Data relating to him/her if:
 - the Data Subject contests the accuracy of the Personal Data, for the period necessary for the Data Controller to verify the accuracy of such data;
 - the processing is unlawful and the Data Subject objects to the deletion of the Personal Data and requests that its use be restricted;
 - the Personal Data is necessary to the Data Subject for the establishment, exercise or defence of legal claims, although the Data Controller no longer needs them for the purposes of the processing;
 - the Data Subject has objected to the processing pursuant to Article 21 of the Privacy Regulation, pending verification of whether the Data Controller's legitimate reasons prevail over the rights and freedoms of the Data Subject;
- (g) object, at any time, to the processing of their Personal Data for purposes of Legitimate Interest, except where the Data Controller has overriding legitimate reasons or the need to assert or defend a right in any legal proceedings;
- (h) request the deletion of Personal Data concerning the Data Subject without undue delay;
- (i) obtain an electronic copy of his or her Personal Data, when the Data Subject wishes to receive Personal Data relating to him or her or to transmit them to a different controller, in cases where the Controller processes Personal Data on the basis of a contract, of his or her consent, or where the Personal Data is processed by automated means.

The Data Subject also has the right to lodge a complaint with the Data Protection Authority, if the conditions are met.

Pursuant to Art. 2-terdecies of the Privacy Code, in the event of the death of the Data Subject, the aforementioned rights relating to the Personal Data may be exercised by the person who has an interest of his/her own, or is acting to protect the data subject as his/her agent, or for family reasons worthy of protection. The Data Subject may expressly prohibit the exercise of some of the rights listed above by his or her assignees by sending a written declaration to the Data Controller to the address indicated in **Annex 1**. The declaration may be revoked or modified later in the same manner.

Without prejudice to the foregoing, pursuant to Article 2-undecies of the Privacy Code and Article 12 of the Whistleblowing Decree, the rights listed above may not be exercised if the exercise of such rights may result in actual and concrete prejudice to the confidentiality of the identity of the Data Subject who reports a violation of which he/she has become aware by reason of his/her employment relationship with the Data Controller or by reason of the functions performed for the latter. Moreover, if there is a real risk that the disclosure of information concerning the Whistleblowing procedure may jeopardise the verifications under way or, in general, the proper performance of the Whistleblowing procedure itself, feedback to the Data Subject may be provided after this risk has ceased to exist. In any case, the reported person will not have access to the identity of the whistleblower, but only to the substance of the report.

In order to exercise the above rights, the Data Subject may contact the Data Controller at any time, by writing to the address given in **Annex 1**.

9. Amendments and updates

This Privacy Notice is updated to 30 November 2023.

In case of revision or updating of this document, also as a consequence of amendments or updates to the applicable legislation, the Data Controller shall inform the Data Subject of the new features of the processing by publishing the updated text on the website www.faiservice.com and on the company notice board.

Annex 1

LIST OF DATA CONTROLLERS AND RELEVANT CONTACT DETAILS

<u>Company</u>	<u>Registered office</u>	<u>E-mail address</u>
FAI SERVICE S. COOP.	Viale Cassala 57, 20143 Milan (MI) (I)	privacy@lumesia.com
SAS EUROTOLL	35 Rue Camille Desmoulins 92130 Issy Les Moulineaux (F)	dpo@eurotoll.fr
TRACKY SERVICE ESPANA S.L.U.	c/Barreiros 1 of.107 Pol.Ind.Padrosa 17730 Llers (ES)	info@trackyservice.es
TRACKY SERVICE POLSKA SP. Z.O.O.	Rondo Daszynskiego 2b/26 00-843 Warszawa (PL)	info@trackyservice.pl
TRACKY SERVICE GMBH	Autobahnzollplatz a-9602 Thorl Maglern (AT)	info@trackyservice.at
LUMESIA INSURANCE SRL	Viale Cassala 57, 20143 Milan (MI) (I)	info@lumesiainsurance.com