ANNEX 1 to the Group Whistleblowing Policy

WHISTLEBLOWING POLICY ITALY

1. INTRODUCTION

This Policy aims to integrate the contents of the InPost Group Policy called "Informativa sulle segnalazioni" with the peculiarities provided for by the Italian legislation transposing European Directive no. 2019/1937 on the discipline of Whistleblowing (the "Directive").

The Directive was implemented in Italy with Legislative Decree no. 24/2023, which entered into force on 30 March 2023 and is effective from 15 July 2023 (hereinafter, the "Decree").

With this document, **Locker InPost Italia S.r.l.** (hereinafter, "InPost Italia" or the "Company") intends to provide all recipients of the aforementioned legislation with clear information on the internal and external whistleblowing channels, on the procedures and conditions for reporting whistleblowing pursuant to the Italian legislation.

2. WHO CAN MAKE A REPORT

Reports can be made by all subjects who are and/or have been, even temporarily, in working relationships with InPost Italia despite not having the status of employees, as well as those who do not have a legal relationship with the Company yet or whose relationship has ended if, respectively, the information on the violations was acquired during the selection process or in other pre-contractual phases or during the course of the employment relationship.

More precisely, the subjects who can send a report are the following:
- employed workers;
- self-employed workers, freelancers and consultants, who carry out their work at the Company;
- volunteers and interns, paid and unpaid, who work for the Company;
- shareholders (natural persons);
- people with administrative, management, control, supervisory or representation functions, even de facto.

3. WHAT YOU CAN REPORT

The subject of the reports are behaviors, acts or omissions which damage the public interest and/or integrity of the Company and which consist of:

1. administrative, accounting, civil or criminal offences (additional to the hypotheses already indicated in numbers 3), 4), 5) and 6) of this list);
2. significant illicit conduct pursuant to Italian Legislative Decree 231/2001, or violations of the organization and management models provided therein, if adopted by the Company (additional to the hypotheses already indicated in numbers 3), 4), 5) and 6) of this list);
3. offenses that fall within the scope of application of European Union or national acts relating to the following sectors: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; 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;

4. acts or omissions detrimental to the financial interests of the Union;
5. acts or omissions concerning the internal market (including infringements of European Union competition and State aid rules, as well as infringements relating to the internal market linked to acts infringing corporate tax rules or mechanisms the purpose of which is to obtain a tax advantage which defeats the object or purpose of the applicable corporate tax legislation);
6. acts or behaviors that frustrate the object or purpose of the provisions set out in Union acts in the sectors indicated in numbers 3), 4) and 5) of this list.

The following cannot be reported:
• news that is clearly unfounded;
• information that is already totally in the public domain;
• information acquired solely on the basis of unreliable rumors.

N.B. Disputes, claims or requests linked to a personal interest of the reporting person which relate exclusively to their individual working relationships, or inherent to their working relationships with hierarchically superior figures, cannot be subject to whistleblowing reporting. Complaints excluded on the grounds that they relate to a personal interest of the whistleblower are not considered whistleblowing reports and, therefore, may be treated as ordinary reports which can be reported through the procedures set out in the relevant Group Policies.

Violation of any other internal or external regulation that applies to the Group, any generally accepted practice within the Group or any activity which is an abuse of any authorization procedures in the Group policies can be reported as provided for in the relevant Group Policy.

4. WHAT CONTENT A REPORT MUST HAVE

For the purposes of its admissibility, the report must be as detailed as possible and, therefore, is strongly recommended to indicate:
• the circumstances of time and place in which the reported event occurred;
• the description of the fact;
• personal details or other elements that allow the identification of the person to whom the reported facts can be attributed;
• documents that can provide elements of substantiation of the facts;
• other subjects potentially aware of the facts.

If what is reported is not adequately substantiated, whoever manages the reports can ask for additional information from the whistleblower.

Furthermore, it is advisable for anyone who intends to submit a report to specify that it is a report for which they intend to keep their identity confidential and benefit from the protections provided for whistleblowing (e.g.: by inserting the wording "*reserved to the people in charge of managing the Whistleblowing reports*"). This specification allows, where the report is erroneously addressed to an incompetent person, the timely transmission by the latter to the person authorized to receive and manage whistleblowing reports.

N.B. reports can also take place ANONYMOUSLY, where the chosen reporting channel allows it. Please note that an anonymous report which is also not adequately substantiated is likely to be considered non-admissible. In any case, anonymous reports will be registered by the report manager and the documentation received will be kept. In case the anonymous whistleblower is subsequently identified and has suffered retaliation, the protections provided for the whistleblower will be guaranteed.

5. WHAT ARE THE REPORTING CHANNELS

5.1 REPORTING CHANNEL INTERNAL TO THE COMPANY

Reports can be made through the following internal channels, the activation of which was adequately communicated to the trade union representatives in compliance with the art. 4 co. 1 of the Legislative Decree. 24/2023.

In written form:

Through the **SpeakUp reporting platform**, which also allows the whistleblower to make anonymous reports. The platform is accessible through the dedicated website (https://inpost.speakup.report/LockerInPostItalia), also reachable by scanning the following QR Code:

Signing in to SpeakUp requires neither the name nor the email address of the whistleblower, guaranteeing, if desired, the possibility of making anonymous reports. To track the status of the investigation, everyone can save their own unique "case number" and password (relating to the report). If the whistleblower wants to be contacted directly (outside the SpeakUp platform) by the people in charge of managing the report, the whistleblower can include his/her name and contact information in the report. In the event that the people in charge of managing the report have specific questions for the whistleblower, these will be visible once the latter accesses the report (using his/her case number and related password). Any status updates will also be visible by connecting to the portal.

In oral form:

Through the **SpeakUp voice messaging system**, reachable at the following freephone number:

800 147 694

After calling the number above, the whistleblower will need to enter the following 6-digit organization code:

100401

The system does not require the name and does not record neither the telephone number, nor the voice of the whistleblower, as the content of the report is automatically transformed into written text, thus guaranteeing the possibility of making anonymous reports.
To track the status of the investigation, everyone can save their own unique "case number" and password (relating to the report). The response of the report manager will be recorded by the system and will be available to the reporter in vocal format once the latter accesses the report (using his/her case number and related password) by calling the freephone number mentioned above.
If the whistleblower wants to be contacted directly (outside of the SpeakUp voice messaging system) by the people responsible for handling your report, he/she can include his/her name and contact information in the report.

Additional channels to be used only in case of conflict of interest:

Exclusively in the event that one (or more) of the subjects in charge of managing whistleblowing reports indicated in the following paragraph. 5.1.1 has a conflict of interest with respect to a specific report (as, for example, whistleblower or reported person), the report may be made - even anonymously - through the following channels.

In written form:
By registered postal mail to the following addresses:

- Locker InPost Italia S.r.l., viale Cassala, n. 30 - 20143 Milan, Italy (locally), or
- InPost sp. z o.o., ul. Pana Tadeusza 4, 30-727 Kraków, Poland (group level), to the attention of the Group Compliance Officer

To guarantee confidentiality, reporting through this method must take place using a "sealed envelope" system. In particular, the documentation must be divided into three separate envelopes, the contents of which must be divided as indicated below:

- Envelope no. 1: reporting data and copy of C.I.
- Envelope no. 2: reporting
- Envelope no. 3: with the wording *"Whistleblowing report reserved to [•]"*, indicating by choice one of the managers not in conflict of interest (Compliance Officer/General Counsel Italy or Head of Human Resources Italy or Legal Counsel Italy or Group Compliance Officer), in which Envelopes 1 and 2 must be inserted. If you intend to make an anonymous report, only Envelope 2 must be inserted.

In oral form:
Through a request for a **direct meeting** with one of the subjects in charge of managing whistleblowing reports indicated in the following paragraph. 5.1.1, identified at the choice of the whistleblower. In the request, the whistleblower must expressly declare that he/she wishes to confer exclusively with that specific manager who he/she believes does not have a conflict of interest. The meeting will take place within 15 days from the date of the request and in a suitable place to guarantee the confidentiality of the whistleblower. Subject to the consent of the reporting party, the meeting will be recorded using devices suitable for storage and listening. If, for any reason, it is not possible to proceed with the registration (for example, because the whistleblower has not given consent or the IT tools for recording are not available), a report will be drawn up which must be signed by the whistleblower and the manager. A copy of the report will be given to the whistleblower. This reporting method does not, by its nature, allow the anonymity of the whistleblower.

5.1.1 WHO MANAGES THE INTERNAL REPORTS RECEIVED BY INPOST ITALIA

The reports made through the internal channel are received by subjects adequately trained on the discipline of whistleblowing and appointed (through a formal act of appointment) for managing the reports, who, having carried out the preliminary checks better specified in section 5.1.2, transmit them to the subjects responsible for supervising, based on the specific circumstances, the reporting management.

The subjects responsible for managing and supervising the reports received by InPost Italia:
- Compliance Officer / General Counsel Italy
- Head of Human Resources Italy
- Legal Counsel Italy
- Group Compliance Officer, whose role is limited to supervising the activity carried out by the other managers and/or managing the report if: (i) one (or more) of the other managers is in conflict of interest; (ii) there is an interest at Group level.

If the internal report is presented to a person other than those identified above (e.g. to the hierarchical superior), where the whistleblower - previously informed of the possibility of being protected through the protection provided for by the legislation on whistleblowing - expressly declares that he wishes to benefit from whistleblowing protections or this desire can be deduced from the report (for example, from a reference to the relevant legislation), the report is considered a "whistleblowing report" and must be transmitted, within seven days of its receipt, to the competent internal person, giving simultaneous notice of the transmission to the whistleblower.

Otherwise, if the whistleblower does not expressly declare that he or she wishes to benefit from whistleblowing protections, said report is considered as an ordinary report.

5.1.2 HOW INTERNAL REPORTS RECEIVED BY INPOST ITALIA ARE MANAGED

Reception and management of reports will only be permitted to personnel expressly authorized to do so and in possession of the requirements of professionalism, reliability, autonomy -understood as impartiality and independence- and confidentiality in the management of reports and the related internal channels, required by law.

In the event that the report arrives via the local internal channels of InPost Italia, the following process will be followed:

- RECEIPT of the report: the receipt of the report is entrusted to the subjects in charge of managing the reports, who will issue the whistleblower with a notice of receipt of the report within 7 (seven) days from the date of receipt of the same and will also carry out an initial analysis of the contents, of the object, the evidence provided, the subjects involved, etc. and will inform the Group Compliance Officer, who will supervise the investigation and/or take part in it if there is an interest at Group level. If a report concerns one (or more) of the persons in charge for managing and/or supervising reports, this one will not be involved in the investigation process. If the report is made, by mistake, through a channel to which that manager has access, that manager's access to the channel will be interrupted for the duration of the investigation and he/she will not be given permission to become aware of the investigative documents. It is understood that, if the persons in charge for managing and/or supervising reports are involved in the facts being reported, the whistleblower can address the report, depending on the case, through the Group channels or the External channel at ANAC.

- MANAGEMENT of the investigation process: once the report has been received, the processability (compliance with the objective and subjective assumptions) and admissibility (subsistence of the content requirements) of the report received will be assessed. In the event of a positive outcome of this evaluation, the preliminary investigation activity will begin with the carrying out of any investigation that is deemed necessary. During the investigation, the persons involved in the report (e.g. the person reported), can be heard or, upon request, are heard, also through written observations and documents. Based on the evidence provided by the whistleblower and the findings of the investigation, a determination will be made whether further investigations are necessary.

- OUTCOME of the investigation: within 6 (six) weeks from the date on which the whistleblower made the report, the subjects in charge of managing the reports must provide adequately motivated feedback on the report (archiving or declaration of validity and transmission to the competent functions for follow-up, actions taken as a consequence of the report), which will be transmitted to the whistleblower in a form that reflects the one in which the report was communicated.
If it is not possible to give any response within (6) six weeks, the persons in charge of managing the whistleblowing reports must send the whistleblower an interlocutory response (information relating to the investigative activities that are intended to be undertaken and the progress of the investigation may be communicated), through the same channel used to submit the report, which also provides an indication of

when you will be informed of the Company's position on the report. In this last case, once the investigation has been completed, the results must be communicated to the whistleblower.

5.2 EXTERNAL CHANNEL AT ANAC

If one of the following conditions occurs, a report can be submitted via the external channel established at ANAC.

Whistleblowers can use the external channel if:

- internal channels are not active; or
- they are active, but do not comply with the provisions of the legislator regarding the subjects and methods of submitting reports; or
- the person has already made the internal report, but it has not been followed up; or
- the whistleblower has reasonable grounds to believe that if he/she made an internal report:
    - the same would not be followed up effectively; or
    - this could lead to a risk of retaliation. Or
- the whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

Reporting via the external channel established at ANAC can be done by accessing ANAC services portal at the following link: Whistleblowing - National Anti-Corruption Authority (https://www.anticorruzione.it/-/whistleblowing).

5.3 PUBLIC DISCLOSURE

A further reporting method provided for by the applicable whistleblowing legislation consists of public disclosure.

With public disclosure, information on violations is made public through the press or electronic means or in any case through means of dissemination capable of reaching a large number of people.

The public disclosure of violations must take place in compliance with the conditions set by the legislator so that the person who carries it out can benefit from the protections recognized by the Decree. The conditions for making a public disclosure, benefiting from the protection provided by the applicable provisions, are as follows:

- an internal report to which InPost Italia did not respond within the established deadlines was followed by an external report to ANAC which, in turn, did not provide feedback to the whistleblower within a reasonable time; or
- the whistleblower has already directly made an external report to ANAC, which, however, has not given feedback to the whistleblower regarding the measures envisaged or adopted to follow up on the report within a reasonable time; or
- the whistleblower directly makes a public disclosure as he has reasonable grounds to believe, reasonably, on the basis of concrete circumstances and therefore, not on simple inferences, that the violation may represent an imminent or obvious danger to the public interest; or
- the whistleblower directly makes a public disclosure because he or she has reasonable grounds to believe that the external report may involve the risk of retaliation or may not be followed up effectively.

If none of the aforementioned conditions apply, the author of a public disclosure will not be able to benefit from the protection measures provided for by the Decree.

5.4 REPORT TO THE JUDICIAL AUTHORITY

The legislation on whistleblowing also grants protected individuals the possibility of contacting the judicial Authorities to file a report of illicit conduct of which they become aware in a work context.

6. WHAT ARE THE PROTECTIONS PROVIDED FOR THE WHISTLEBLOWER

The following protections are guaranteed to the whistleblower and any other subjects involved:

• **CONFIDENTIALITY:** the identity of the whistleblower cannot be revealed to people other than those competent to receive or follow up on reports, without the prior express consent of the whistleblower. Protection concerns not only the name of the whistleblower, but also all the elements of the report from which the identification of the whistleblower can be derived, even indirectly. Furthermore, confidentiality is extended to the content of the report and the related documentation, to the identity of the people involved and the people mentioned in the report until the conclusion of the proceedings initiated due to the report, in compliance with the same guarantees provided in favor of the whistleblower.

• **PROTECTION OF PERSONAL DATA:** the processing of personal data relating to the receipt and management of reports is carried out by InPost Italia and, where strictly necessary in relation to the subject of the report, other companies of the InPost Group, as Joint Data Controllers, in compliance with European and national principles regarding the protection of personal data, providing appropriate information to the whistleblowers and the people involved in the reports, as well as adopting appropriate measures to protect the rights and freedoms of the interested parties. For further information, please refer to the Privacy Information attached to this procedure (Annex A), as well as to the Privacy Information that will be provided when using the internal reporting channels.
Pursuant to the provisions of art. 12, co. 3 of the Decree and as better specified in the Privacy Policy, the exercise of the rights provided for by the applicable provisions regarding the protection of personal data may be subject to limitations based on specific circumstances.

• **PROTECTION FROM RETALIATION:** the whistleblower is protected from any behavior, act or omission, even if only attempted or threatened, carried out as a result of the reporting, which causes or may cause unfair damage to the whistleblower. Protection from retaliation is also extended to the following individuals:

- to the facilitator (natural person who assists the whistleblower in the reporting process and operates within the same working context);
- to people from the same working context as the whistleblower, the person who filed a complaint or the person who made a public disclosure and who are linked to them by a stable emotional or kinship bond within the fourth degree;
- to work colleagues of the whistleblower or of the person who has filed a complaint or made a public disclosure, who work in the same working context as the person and who have a regular and current relationship with that person;
- to entities owned by the whistleblower or for which the same people work as well as to entities that operate in the same working context as the aforementioned people.

Protection requirements of the whistleblower from retaliation are as follows:

- the protections are granted when the whistleblower, at the time of the report, had well-founded reason to believe that the information on the violations was true and fell within the objective scope of application of the legislation on whistleblowing. Reports based on rumors or suppositions are therefore excluded from protection;

- the discipline/procedure for using the different reporting channels has been respected.

In the absence of even one of these conditions, the measures of protection provided by the Decree do not apply to those who report or make the public disclosure; in this case, depending on the circumstances, the protection granted to subjects other than those listed above could be excluded, due to the role assumed within the reporting/complaint process and/or the particular relationship that binds them to the whistleblower or whistleblower.

When the criminal liability of the whistleblower for crimes of defamation or slander is ascertained, even with a first instance sentence, or his/her civil liability, for the same title, in cases of malice or serious fault, the protection measures against the whistleblower do not apply and a disciplinary sanction is also applied to the whistleblower.

It should be noted that retaliation (e.g., dismissal, suspension, demotions, discrimination, etc.) must be communicated exclusively to ANAC, as the only body competent for its management and assessment.

7. FINAL PROVISIONS

This Policy has been approved and can only be modified in written form with a specific resolution of the Board of Directors of Locker InPost Italia S.r.l.

This Policy is available on the Company's website and intranet. The Company will also plan staff awareness and training initiatives on the whistleblowing system (such as, for example, specific communications, training events, newsletters, company emails, etc.).

For anything not provided for in this document, please refer to the provisions of the Group Policy on whistleblowing. In case of conflict between the two documents, the contents of this Policy will prevail.

ANNEX A

PRIVACY POLICY – WHISTLEBLOWER (D.LGS. n. 24/2023)
Information notice pursuant to Art. 13 of the EU Regulation 2016/679 ("GDPR")

1. WHO IS THE DATA CONTROLLER? HOW CAN I CONTACT HIM?

Locker Inpost Italia s.r.l., with registered office in viale Cassala, 30 – 20143 Milano, in person of its *pro-tempore* legal representative: Data controller's email: **privacy@inpost.it**.

2.CATEGORIES OF PROCESSED DATA

Personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can directly or indirectly be identified, in particular by reference to an identifier such as a name, an identification number, a location data, an online identifier or to one or more specific factors to the physical, physiological, genetic, mental, economic, cultural or social identity (C26, C27, C30).
The processed data will be those related to reports made by reporting individuals (so-called "Whistleblowers"), which may also include data related to third parties, namely the reported individuals and other subjects involved in the reporting, and will be processed in full compliance with and within the defined Whistleblowing Policy Italy adopted by the Data Controller.

Data related to reporting individuals, which may be provided by them, include:
-Name, surname;
-Company position or occupation;
-Contact details;
-The voice of the whistleblower, in case of a request for a direct meeting and with prior consent to recording;
-Other information provided by the whistleblower;
-Any Special Data (cf. art. 9 GDPR): personal data capable of revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data intended to uniquely identify an individual, data related to health or the sexual life or sexual orientation of the person;
-Any Data related to criminal convictions and offenses or related security measures (cf. art. 10 GDPR): personal data capable of revealing measures referred to in Article 3, paragraph 1, letters from a) to o) and from r) to u), of Presidential Decree November 14, 2002, n. 313, concerning the criminal record, the register of administrative sanctions dependent on crime, and related pending charges, or the status of the accused or under investigation under Articles 60 and 61 of the code of criminal procedure.
The data subjects of this processing are: subordinate workers of private sector entities; self-employed workers; workers or collaborators providing goods or services or carrying out works on behalf of third parties; freelancers and consultants; volunteers and trainees; shareholders and individuals with administrative, managerial, supervisory, oversight, or representative functions; job applicants and terminated workers.

3. PURPOSE OF PROCESSING, LEGAL GROUND, DATA RETENTION, NATURE OF CONFERRAL

PURPOSE OF PROCESSING	LEGAL GROUND	DATA RETENTION	NATURE OF CONFERRAL
A) Management of whistleblowing reports, specifically the collection of data for the submission of reports, that has come to light within the context of a legal relationship, pursuant to Article 3 of Legislative Decree No. 24/2023.	The processing is necessary to fulfil a legal obligation (pursuant to Legislative Decree No. 24/2023) which the Data Controller is subject to (C45), in accordance with art. 6, par. 1, lett. c), GDPR. The processing of "special" data is based on the fulfillment of specific obligations and the exercise of specific rights of the Data Controller and the data subject in the	For the time strictly necessary for the processing of the report and, in any case, not exceeding 5 years from the date of communication of the final outcome of the reporting procedure (Art. 14 of Legislative Decree No. 24/2023). In the event of ongoing legal proceedings, the aforementioned period is extended until the exhaustion of the degrees of judgment. Personal data that is evidently not useful for the processing of a specific report is not collected, or if collected	The provision of personal data by the whistleblower is necessary, while maintaining the right to make a report anonymously.

PURPOSE OF PROCESSING	LEGAL GROUND	DATA RETENTION	NATURE OF CONFERRAL
	field of labor law (Art. 9, par. 2, lett. b), GDPR. The processing of data related to criminal convictions and offenses, taking into account the provisions of Article 10 of the GDPR, is based on the legal obligation to which the Data Controller is subject (Art. 6, par. 1, lett. c).	accidentally, it is promptly deleted.	
B) Disclosure of the whistleblower's identity and/or any other information from which such identity can be directly or indirectly inferred to individuals other than those competent to receive and follow up on the report, in accordance with Article 12, paragraph 2, of Legislative Decree No. 24/2023.	The processing is based on the explicit consent of the data subject for the processing of its personal data (C42, C43).	Until the revocation of consent, unless the identity has already been disclosed to third parties.	The provision of the personal data by the whistleblower is optional. In case of lack, the Data Controller will not be able to disclose the identity of the whistleblower and/or any other information from which such identity can be inferred to individuals other than those competent to receive and follow up on reports, except in situations expressly provided for by Legislative Decree No. 24/2023 and after prior written communication of the reasons for the disclosure.

4. DATA RECIPIENTS

All the personal data may be disclosed to recipients acting as autonomous Data Controllers or Data Processors (art. 28 GDPR) and processed by persons appointed to, pursuant to art. 29 GDPR and acting under the authority of the controller or the processor, upon written letter of authorizations relating to purposes and means of processing. Personal data may be disclosed to recipients belonging to the following categories:
- the person or internal office, or external entity (including any Supervisory Body), entrusted with the management of the internal reporting channel; - third-party entities for the provision of the whistleblowing platform adopted by the Data Controller; - any judicial authorities and public authorities (including ANAC); - Data Protection Officer (DPO) / Privacy Officer for managing requests from data subjects.

5. DATA TRANSFERS

Personal data won't be transferred to countries outside the EEA.

6. AUTOMATED-MEAN PROCESSES?

Personal data will be subjected to traditional and manual, electronic or automated processing. Fully automated decision-making processes are not carried out.

7. DATA SUBJECTS' RIGHTS

You may freely exercise your rights at any time under the EU Reg. 2016/679 – GDPR – art. 15 and following, contacting Team for the management of reports through the same internal channel used to do a whistleblowing report. You have the right, at any time, to obtain confirmation from the Data Controller as to whether personal data concerning you are being processed (art. 15), request their rectification (art. 16) or erasure (art. 17), restriction of processing (art. 18). The Data controller communicates (art. 19) any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed to. The Data controller disclose the aforesaid recipients to any requesting data subjects. You may have the right to data portability (art. 20) in a structured, commonly used and machine-readable

format. You have the right to objects, at any time, to processing grounded on the legitimate interest of the data controller (art. 21); You have the right, at any time, to oppose to personal data processing without prejudice to the lawfulness of processing.
Without prejudice to any other administrative or judicial remedy, in case you consider your data processing in contrast with Reg. UE 2016/679, pursuant to article 15 lett. f) of Reg. UE 2016/679, you have the right to lodge a complaint with a supervisory authority in the Member State you habitually reside, work or in the place where the alleged violation has occurred (Garante Privacy https://www.garanteprivacy.it/).

According to Legislative Decree No. 24/2023, the Data Controller is obliged to ensure the confidentiality of the whistleblower: the identity of the reporting person and any other information from which such identity can be directly or indirectly inferred will not be disclosed, without the explicit consent of the whistleblower, to individuals other than those competent to receive or follow up on the report, except for the right of defense of the reported party and where required by law.

8. UPDATES
Data Controller retains the right to modify, update, add or remove some parts of this policy at any time. In order to facilitate the verification of any changes, the policy will contain an indication of the update date of the policy itself.

Last update: December 04th 2023

Data Controller
Locker Inpost Italia s.r.l.

***

Pursuant to Articles 13 and 6 of EU Regulation 2016/679 (GDPR),

I, the undersigned _____ city of residence_____
I declare that I have read the *Privacy Policy – Whistleblower (d.lgs. N. 24/2023)* of **Locker InPost Italia s.r.l.** above for purpose A).

Date _____ Signature _____

And I express my consent for purpose B) (identity disclosure):

□ I consent
□ I do not consent

Date _____ Signature _____