

Protection of whistleblowers for criminal offences or irregularities which have come to their attention in an employment relationship

Index

1. What is the whistleblowing	2
2. The legislation	3
2.1 Legislative Decree 24/2023 – Subjective scope	4
2.2 Legislative Decree 24/2023 - Terms	4
2.3 Legislative Decree 24/2023 - Definitions	4
3. Purpose of the document	6
4. Analysis of the context	6
5. Scope of the alert	7
6. Process of reporting wrongdoing	7
6.1 Content of the alert	7
6.2 Subject of the alert	7
6.3 Operating modes and signalling channels	7
6.4 Management of reporting	11
6.5 The anonymous reports	11
6.6 Verification of the validity of the alert	11
6.7 Protection of the whistleblower	12
6.8 Protection of privacy	13
6.9 Responsibilities of whistleblowers and other entities	13
7. Other channels	14
8. Information, instructions and communications	14
9. Sanctions	14
9.1 Collaborators and external consultants	15
9.2 Partners, customers and suppliers	15
9.3 General rules	15

1

Figures index

<i>Figure 1</i> Screen of the corporate website - Link Whistleblowing to access to the platform "WallBreakers"	8
<i>Figure 2</i> Module with QR-Code for platform access "WallBreakers"	8
<i>Figure 3</i> Home Page "WallBreakers" platform	9
<i>Figure 4</i> Questionnaire of the "WallBreakers" platform	10
<i>Figure 5</i> Success Sending Report and Receipt Code "WallBreakers" platform	11

Whistleblowing Procedure
19/01/2024

LAWER S.p.A - Via Amendola, 12/14 - 13836 Cossato (BI) Italy | Tel. +39 (0)15 9899511 | Telefax +39 (0)15 9842211

E-Mail sales@lawer.com | CF e P. IVA/TVA/VAT N° IT 00500780028 | Rag. Soc. Trib. Biella N° 7404

1. What is the whistleblowing

The term "whistleblower" refers to the employee of the company or also to other parties (e.g. a supplier's employee, shareholders, partners, etc.), which reports violations of national or European Union regulatory provisions affecting the private interest, of which they became aware in the workplace. Reporting ("whistleblowing"), in the intentions of the legislator is a manifestation of civic sense through which the whistleblower contributes to the emergence and prevention of risks and situations detrimental to the company to which it belongs. Revelations or complaints can be of various kinds: violation of a law or regulation, threat of a public interest such as corruption and fraud, serious and specific situations of danger to public health and safety, etc. The primary purpose of the report is therefore to bring to the attention of those identified the possible risks of irregularities that have become known. Therefore, reporting is an important tool for prevention. The justification for whistleblowing, therefore, can be found in the possible greater control of corruption and abuse of power and can help promote accountability and ethics in the company. Within this framework, the issue of the protection of whistleblowers, on the one hand, and the verification of the truth of information, on the other hand, arises. Therefore, a balance between protecting whistleblowers and protecting the company from distorted use of the tool is necessary to minimize the risk of reputational damage. In any case, it is necessary to guarantee the reporting agent and any other parties involved in several ways, pending the management of the file, maximum confidentiality, and protection of personal data. It is also essential that the structure has an organizational system and procedures that can ensure compliance with the provisions of the legislation or update existing ones.

2. The legislation

The D. Lgs. 10 March 2023 n. 24 transposes, in Italy, the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23/10/2019, concerning the protection of persons who report violations of European Union law.

Main changes:

- the extension of the pool of the recipients of the obligations;
- the extent of individuals who can report wrongdoing (in addition to employees, also collaborators, trainees, volunteers, self-employed, contractors and suppliers);
- the extension of potentially illegal conduct deemed worthy of reporting;
- the integration of the classic reporting channel (internal to the institutions) with an external reporting channel entrusted to the Anti-Corruption Authority (A.N.A.C.);
- strengthening the protection of whistleblowers with rules and guarantees aimed at preventing them from being discouraged from reporting for fear of the consequences or, if they have reported violations, they are penalised.

Outline of successive legal provisions



2.1 Legislative Decree 24/2023 – Subjective scope

Private Sector

Subjects who have employed, in the last year, the average of at least 50 employees on permanent or fixed-term contracts; subjects falling within the scope of the European Union acts referred to in parts I.B and II of the Annex, even if in the last year they have not reached the average of 50 employees (financial services, prevention of money laundering, terrorism, transport safety, environmental protection).

Different subjects with an Organization and Management Model ex Legislative Decree 231/01, even if in the last year they have not reached the average of 50 employees (in this case, if they have less than 50 employees, the subject of the reports is limited).

2.2 Legislative Decree 24/2023 - Terms

There are deadlines for adjustment and establishment of the reporting channel depending on the type of institution and the number of employees.

For those who were previously required to adopt the procedure continue to apply the previous rules (art. 54 bis of Legislative Decree 165/2001 and art. 6 of Legislative Decree 231/2001) until the adoption of the new procedure and in any case:

- until 15 July 2023 for the public sector and private entities with more than 250 employees
- until 17 December 2023 for companies up to 249 employees

2.3 Legislative Decree 24/2023 - Definitions

For convenience below is a table with the main definitions derived from the measure in force (Art. 2 of Legislative Decree 24/2023).

Addressees of the new private law	see the paragraph "Subjective scope" of the Legislative Decree 24/2003
Violations	<ul style="list-style-type: none"> ▪ administrative, accounting, civil or criminal offences ▪ infringements of European legislation on public procurement, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety and animal health and welfare, public health, consumer protection, privacy and personal data protection, network and information system security; infringements of competition law and State aid ▪ acts or omissions relating to the internal market (e.g. competition, State aid)
Information on infringements	Information, including well-founded suspicions, concerning infringements committed or which, on the basis of factual evidence, could be committed in the organisation with which the reporting person or the person who makes a complaint to the judicial or accounting authority has a legal relationship in the business context, as well as elements concerning conduct aimed at concealing such violations
Reporting	Written or oral communication of information on infringements
Internal reporting	The communication, written or oral, of information on violations, submitted through the internal reporting channel
External reporting	The communication, written or oral, of the information on the violations, introduced through the external signaling channel (A.N.A.C.)
Public disclosure	Making information about infringements public through the press or electronic means or by means of dissemination that can reach a large number of people
Reporting person/whistleblower	The natural person who makes the public reporting or disclosure of information about breaches acquired within their business context
Facilitator	A natural person assisting a reporting person in the reporting process, operating within the same business environment and whose assistance should be kept confidential
Work context	Work or professional activities, present or past, carried out in the framework of the relationship referred to in article 3, paragraphs 3 or 4 of Legislative Decree. 24/2023 [employees, collaborators, members, shareholders, trainees, volunteers, freelancers, even during the probationary period and even if the relationship has ended], through which, regardless of the nature of such activities, a person obtains information on the infringements and in the context of which he or she could face retaliation in the event of a report or public disclosure or a complaint to the judicial or accounting authority
Person involved	The natural or legal person mentioned in the internal or external report or in public disclosure as the person to whom the infringement is attributed or as a person otherwise involved in the breach reported or disclosed publicly
Retaliation	Any behavior, act or omission, even if only attempted or threatened, carried out by reason of the report, of the complaint to the judicial or accounting authority or of public disclosure and which causes or may cause, directly or indirectly, unjust damage to the reporting person or the person who has made the complaint
Follow-up	The action taken by the entity entrusted with the management of the reporting channel to assess the existence of the reported facts, the outcome of the investigations and any measures taken
Feedback	Communication to the reporting person of information on the follow-up to the alert

3. Purpose of the document

This section provides operational guidance on how:

- identify the internal channel for the signalling
- report, then provide information on the subject, contents, recipients, methods and documents to be used for the transmission of alerts
- clarify the forms of protection recognized to the reporting and other subjects by our law.

The purpose of adopting this addition to the model is to:

- clarify the principles underlying the institution of whistleblowing;
- define the scope of the context;
- define the internal reporting channel;
- specify the management of alerts, through a well-defined procedural process;
- authorise one or more subjects to manage alerts, in compliance with the obligations of confidentiality and protection of personal data;
- define a training path for these subjects;
- represent the procedures adopted by the company/entity to protect the confidentiality of the identity of the reporting entity, the content of the report and the identity of any other parties involved in this process;
- define the requirements for the protection of personal data provided as part of the procedure;
- define the general information on the procedure adopted;
- to regulate any penalties applicable to infringements of the provisions.

6

This procedure takes into account the Guidelines of A.N.A.C., issued pursuant to art. 10 of Legislative Decree no. 24/2023.

4. Analysis of the context

This document applies to the reporting of violations, as defined above, within the working context.

The Company Lawer S.p.A. has at least 50 employees¹ and has NOT adopted the Organizational Model ex Legislative Decree 231/2001.

¹ For the purpose of calculating the average number of workers employed, reference was made to the average value of the employees (Data processing I.N.P.S.) at 31/12 of the calendar year preceding the current calendar year, contained in the Chamber Visure (v. Guidelines A.N.A.C.)

5. Scope of the alert

As required by law, the procedures will apply to infringements, if not excluded, provided for by the aforementioned legislation (see para. 2.3 above: Definitions).

The procedure does not apply, inter alia, to disputes or reports concerning individual employment relationships, or relating to relationships with superiors (Art. 1 of Legislative Decree no. 24/2023) therefore, by way of example, it does not concern issues concerning the operation of employment relationships, such as non-payments, recognition of level, company organization, time, etc.

Criminal law and trade union protection remain in place.

The following are also excluded:

- which do not affect the public interest
- out of the work context, as defined above.

In essence, irregularities in the management or organisation of the activity are no longer included among the infringements that can be reported.

6. Process of reporting wrongdoing

6.1 Content of the alert

The whistleblower must provide all the information necessary for the recipient or subjects, the recipients, to be able to carry out checks and investigations to verify the validity of the facts reported.

It is therefore necessary that the alert is as detailed as possible in order to allow the analysis of the facts by the competent entities to receive and manage the alerts.

For this reason it is planned to fill in a form that will guide the collection of useful information (see point 6.3 Figure 4).

6.2 Subject of the alert

The subject of the report is illegal conduct that the whistleblower has become aware of within the working context, as specified in paragraph 2.3 above: Definitions.

It must therefore be a question of facts which, in any event, are the result of elements which are in some way verifiable. Alerts based on mere suspicion or rumors shall not be taken into account.

6.3 Operating modes and signalling channels

Lawer S.p.A. has identified two reporting channels:

Channel 1: verbal reporting to the designated recipients at their offices

Channel 2 (preferential): it is a dedicated online platform, "WallBreakers" by PrivacyLab, accessible:

1. from the company website, at the bottom via the link "Whistleblowing" (<https://lawer.wallbreakers.it>) (see Figure 1)
2. framing from your Smartphone the "QR-Code" in the paper form placed on the company notice boards (see Figure 2).

This platform allows, once the various fields with the required information have been filled in, to send the report to the RECIPIENTS appointed by the company, ensuring the confidentiality of the identity of the reporter and the data entered.

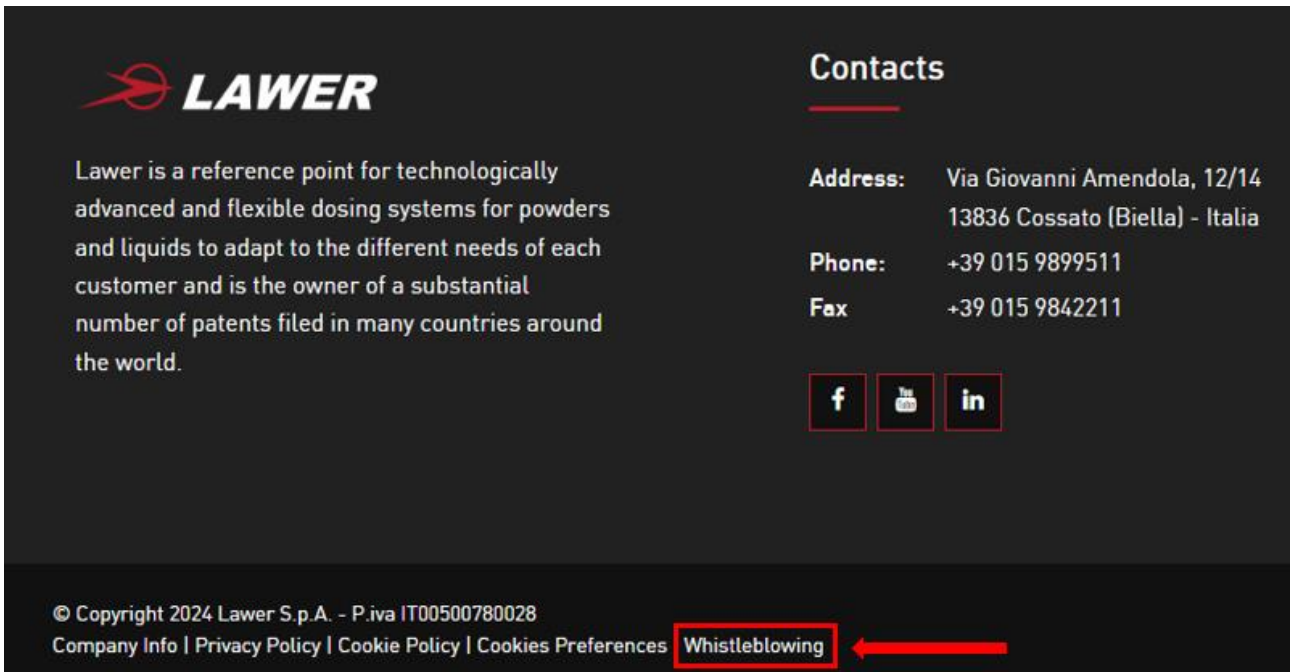


Figure 1 Screen of the corporate website - Link Whistleblowing to access to the platform "WallBreakers"



Figure 2 Module with QR-Code for platform access "WallBreakers"

**Lawer S.p.A. - Modulo Segnalazioni Condotte Illecite
(Direttiva Europea 2019/1937)**

- **CHI COME E COSA SEGNALARE:** Lawer SpA, secondo quanto regolato dal decreto legislativo 24/2023 (che ha recepito la direttiva europea 2019/1937, ampliando la portata delle segnalazioni, che possono riguardare non solo reati, ma anche violazioni di norme, codici etici o di condotta, e ha esteso l'obbligo di adottare canali di segnalazione interni ed esterni a tutti i datori di lavoro privati con almeno 50 dipendenti o che operano in determinati settori sensibili), si è dotata di una piattaforma per le segnalazioni che garantisce al segnalante il diritto alla riservatezza e la tutela contro le ritorsioni.
- **LA PIATTAFORMA INFORMATICA** permette al Personale di Lawer S.p.A. o a Terzi di inviare, anche in forma anonima, segnalazioni aventi ad oggetto comportamenti, rispetto ai quali si abbia il ragionevole sospetto o la consapevolezza che integrano illeciti o comunque condotte poste in essere in violazione di leggi o regolamenti.
- **IDENTITÀ DEL SEGNALANTE:** Lawer SpA incoraggia le segnalazioni in cui è individuata l'identità del segnalante in quanto rendono più agevole approfondire le circostanze relative alla segnalazione, tutelare il segnalante e, in generale, attivare i flussi informativi utili alla più efficace gestione della segnalazione. I dati personali del segnalante sono trattati nel rispetto della normativa vigente in materia di protezione dei dati personali (Regolamento EU 679/2016 e D.lgs. 196/2003, così come modificato dal D.lgs. n. 101/2018) e della legge n. 179/2017.
- **TUTELA:** Lawer SpA garantisce la piena tutela del segnalante, assicurando la riservatezza sulla sua identità e sui fatti oggetto di segnalazione. La piattaforma informatica costituisce strumento preferenziale per l'invio e la gestione delle segnalazioni, in quanto maggiormente idoneo a tutelare la riservatezza dell'identità del segnalante e assicurare adeguate misure di sicurezza delle informazioni. La piattaforma garantisce, infatti, con modalità informatiche, la segregazione tra il contenuto della segnalazione e i dati del segnalante o utilizza strumenti di crittografia. Lawer SpA garantisce, inoltre, che non siano adottati e posti in essere nei confronti del segnalante provvedimenti e comportamenti ritorsivi o discriminatori, per motivi collegati direttamente o indirettamente alla segnalazione, avverti effetti sulle condizioni del rapporto intrattenuto dal segnalante con Lawer SpA. È, altresì, tutelata la privacy dei segnalati nonché la reputazione dei terzi rispetto alle segnalazioni effettuate con dolo o colpa grave che si rivelino infondate.

Nulla da segnalare?

- **DESCRIZIONE DEL PROCESSO**
Le segnalazioni possono essere trasmesse agli enti preposti alla ricezione della segnalazione, alla gestione della stessa e qualora, a valle di una verifica preliminare, si avvino le attività istruttorie in caso di segnalazioni circostanziate verificabili.



Figure 3 Home Page "WallBreakers" platform

Lawer S.p.A. - Modulo Segnalazioni Condotte Illecite (Direttiva Europea 2019/1937)

Descrivi la tua segnalazione in dettaglio. *

Dove sono avvenuti i fatti? *

Quando sono avvenuti i fatti? *

Come sei coinvolto/a nel fatto segnalato? *

Hai delle prove a supporto della tua segnalazione? *

Hai segnalato i fatti ad altre organizzazioni o ad altri individui? *

Vuoi dirci chi sei?

Sì No

Nome *

Cognome *

Metodo di contatto alternativo *

Premendo il tasto INVIA darai seguito alla Tua segnalazione e verrà rilasciato un CODICE RICEVUTA che dovrai conservare in quanto SOLO attraverso questa piattaforma, identificandoti con quel codice potrai seguire l'avanzamento della Tua segnalazione. *

Ho compreso il metodo per seguire l'avanzamento della mia segnalazione.

Figure 4 Questionnaire of the "WallBreakers" platform

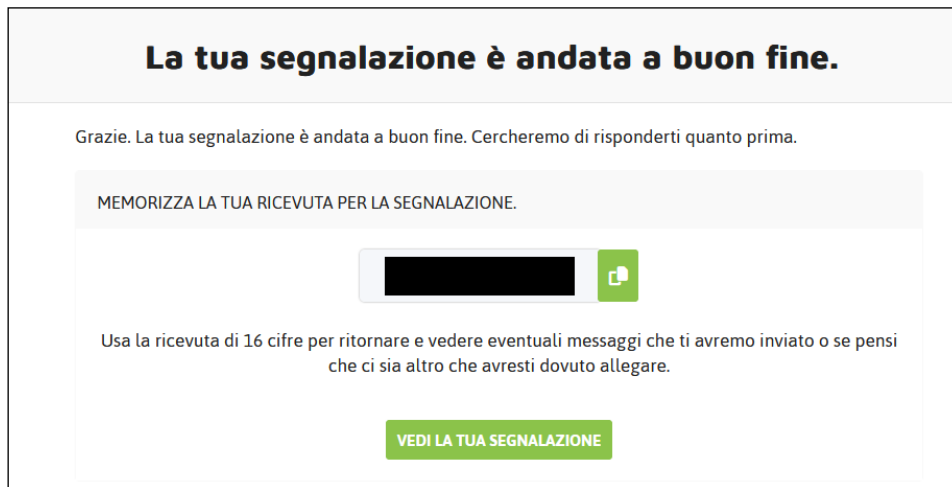


Figure 5 Success Sending Report and Receipt Code “WallBreakers” platform

6.4 Management of reporting

The persons identified by the company for the reception (RECIPIENT) and the management of the reports are Paola Rosati and Andrea Vallese.

At the time of opening the alert is given the possibility of omitting one of the two receivers.

The recipients are expressly trained on the content of the legislation and the methods required for the management and related communications.

The platform guides the management of the alert. The recipients:

- take charge of the report within 7 days from the date of receipt. Manually changing the status of the report, the signaller, through the platform, can understand and follow the progress of his "practice";
- maintain contact with the reporting person and may request additions from the reporting person, if necessary, exclusively through the platform;
- follow-up to the reports received, involving the persons responsible for carrying out the necessary investigations to determine whether they are illegal;
- provide feedback on the report within 3 months of the expiry of the 7-day period following the submission of the report; feedback shall also be provided if the report is not followed up or archived;
- on the channel, provide clear information on the procedures and conditions for internal reporting.

6.5 The anonymous reports

Alerts from which the identity of the reporting agent cannot be derived shall be considered anonymous.

When anonymous alerts are received via internal channels, they will be considered as ordinary alerts to be processed in accordance with the criteria set out in this procedure, as far as applicable, provided that the alerts are substantiated.

In cases of reporting, reporting to the judicial or accounting authority or anonymous public disclosure, where the reporting person has subsequently been identified and has been retaliated, protective measures for retaliation shall apply.

6.6 Verification of the validity of the alert

The task of the recipients is to make a complete assessment of the merits of the circumstances reported by the whistleblower in the report, in compliance with the principles of impartiality and confidentiality.

Once the eligibility of the alert has been assessed, they initiate an internal investigation into the reported facts or conduct in order to assess their existence.

Whistleblowing Procedure
19/01/2024

LAWER S.p.A - Via Amendola, 12/14 - 13836 Cossato (BI) Italy | Tel. +39 (0)15 9899511 | Telefax +39 (0)15 9842211

E-Mail sales@lawer.com | CF e P. IVA/TVA/VAT N° IT 00500780028 | Rag. Soc. Trib. Biella N° 7404

The person concerned may be heard by the recipients and his or her conduct may also be assessed by the submission of written observations and documents.

At the end of the investigation, the recipients shall provide feedback on the alert within the prescribed time limits, taking into account the measures taken or to be taken and the reasons for the choice made.

Feedback shall also be provided in the following cases:

- non-existence of the assumptions;
- manifestly unfounded by the absence of factual evidence capable of justifying the findings;
- established generic content of the report of wrongdoing such as not to allow the understanding of the facts or reporting of wrongdoing accompanied by inappropriate or inconsistent documentation.

Where the information is not sufficiently detailed, applicants may request additional information from the reporting agent via the portal. The request for additions suspends the time limits for the verification until the production or communication of the requested or until the beginning of the fixed deadline.

6.7 Protection of the whistleblower

The identity of the whistleblower is protected both during the acquisition of the report and in any subsequent context, except in cases where the identity must be recognised by law (e.g. criminal, tax or administrative investigations, inspections of supervisory bodies, etc.).

If the complaint is based, in whole or in part, on the reporting and the knowledge of the identity of the signaller is essential for the defence of the accused, the report can be used only in the presence of the signaller's express consent to the disclosure of his identity. In this case the necessary consent will be requested and acquired.

All entities that receive or are involved in the management of the report are required to protect the confidentiality of the identity of the reporting agent.

The identity of the persons involved and of the persons mentioned in the alert shall be protected until the conclusion of the proceedings initiated on the basis of the alert in compliance with the same guarantees provided for the reporting agent. Due to the principle of minimization, the data of persons not related to the report will be deleted.

No form of retaliation or discriminatory measure is allowed or tolerated with respect to the person making an alert (or to other persons protected: e.g. facilitator, family members, etc.), and the protective measures provided for in Art. 16/20 of Legislative Decree 24/2023.

Safeguards shall be granted if the reporting agent, at the time of reporting, of the complaint to the judicial or accounting authority or of public disclosure, had reasonable grounds to believe that the information on the infringements was true and fell within the objective scope of the legislation. In addition, reports and disclosures must have been made in accordance with the procedure for using the different channels.

Protection measures shall consist of

- prohibition of retaliatory actions, including, but not limited to, dismissal, assignment, relocation and any other action that has negative effects on employment contracts, as well as a series of other "punitive" actions, such as the request for submission to medical or psychiatric examinations;
- prohibition of discriminatory actions resulting in economic or financial damage, including loss of income or opportunities.

As stated by the A.N.A.C. Guidelines, there must be a close link between the reporting, public disclosure and the complaint and the unfavourable behaviour/act/omission suffered directly or indirectly by the reporting or reported person, to be considered retaliatory and, consequently, to be protected.

The protection measures shall not apply where the criminal liability of the reporting person for defamation or slander offences, or his civil liability, for the same reason, is established, including by a judgment in the first instance, in cases of intent or gross negligence. In such cases a disciplinary sanction shall be imposed.

6.8 Protection of privacy

The personal data collected in the reporting process will be processed in compliance with the relevant legislation (Regulation U.E. 679/2016 and Legislative Decree 196/2003).

In particular, the principles underlying the company or entity and which are subject to specific training for authorised persons are the following:

- a) Processing data lawfully, correctly and transparently vis-à-vis data subjects ("lawfulness, fairness and transparency").
- b) Collect data only for the purpose of managing and following up reports, public disclosures or complaints made by subjects protected by Legislative decree 24/2023 ("purpose limitation").
- c) Ensure that data is adequate, relevant and limited to what is necessary for the purposes for which it is processed ("data minimisation"). Personal data that are manifestly not useful for the processing of a specific alert shall not be collected or, if collected accidentally, shall be deleted without delay.
- d) Ensure that the data are accurate and, where necessary, up-to-date; all reasonable steps must be taken to promptly erase or rectify inaccurate data relating to the specific report, public disclosure or complaint being handled ("accuracy").
- e) Keep the data in a form that allows the identification of data subjects for the time necessary for the processing of the specific alert and in any case no later than 5 years from the date of notification of the final outcome of the reporting procedure ("Restriction of storage").
- f) Carry out processing in a manner that ensures adequate security of personal data, including protection, by appropriate technical and organisational measures, against unauthorised or unlawful processing and against accidental loss, destruction or damage ("integrity and confidentiality"). In this context, which is characterised by high risks to the rights and freedoms of data subjects, the use of encryption tools within internal channels should normally be considered an appropriate measure to implement, from design and by default to the aforementioned principle of integrity and confidentiality. In any event, the security measures taken must be periodically reviewed and updated.
- g) Define a reporting management model in accordance with the principles of personal data protection. In particular, such measures must ensure that personal data are not made accessible, automatically without the intermediary of the data controller or authorised subject, to an indefinite number of subjects.
- h) Carry out, in the design phase of the signalling channel and therefore before the start of treatment, an impact assessment on data protection where the processing of alerts may pose a high risk to the rights and freedoms of individuals.

In relation to the above, the Data Controller, with reference to this procedure:

- has verified that the data relating to the alerts are accessible only to authorised entities;
- has specifically authorised and trained the person/persons in charge/s of the management of the alerts;
- at the time of reporting will then be made available to the reporting a special information (possibly in summary form with reference to other consultation methods for further information), concerning the processing of personal data (<https://www.privacylab.it/informativa.php?22035469771>.)
- carried out the impact assessment (DPIA), available and available in electronic format on the organization's PrivacyLab GDPR portal (<https://www.privacylab.it/>)
- has appointed, if necessary, a data controller pursuant to art. 38 of EU Regulation 2016/679 after evaluation;
- has updated the data processing register, available and available in electronic format on the organization's PrivacyLab GDPR portal (<https://www.privacylab.it/>)

6.9 Responsibilities of whistleblowers and other entities

Whistleblowing Procedure
19/01/2024

LAWER S.p.A - Via Amendola, 12/14 - 13836 Cossato (BI) Italy | Tel. +39 (0)15 9899511 | Telefax +39 (0)15 9842211

E-Mail sales@lawer.com | CF e P. IVA/TVA/VAT N° IT 00500780028 | Rag. Soc. Trib. Biella N° 7404

This procedure does not protect the whistleblower in case of libelous or defamatory reporting and there are specific sanctions imposed by the A.N.A.C.

7. Other channels

Are provided by the legislation other channels to which the signaler, in case of very precise assumptions, may turn.

1) External Channel (A.N.A.C.) (art. 6)

- it is not foreseen, within its working context, the mandatory activation of the internal reporting channel or this, even if mandatory, is not active or, even if activated, is not compliant;
- the alerter has already issued an internal alert and the alert has not been followed up (not if it failed);
- the alerter has reasonable grounds to believe that, if he made an internal alert, it would not be effectively followed up or would result in retaliatory action;
- the signaller has reasonable grounds to believe that the infringement may constitute an imminent or manifest danger to the public interest.

2) The reporting agent may carry out public disclosure if one of the following conditions is met (art. 15):

- has already carried out an internal and external signalling, or has carried out an external signalling directly and has not been reflected in the deadlines;
 - it has reasonable grounds to believe that the infringement may constitute an imminent or manifest danger to the public interest;
- it has reasonable grounds to believe that the external alert may involve the risk of retaliation or may not have effective follow-up due to the specific circumstances of the specific case, such as where evidence may be concealed or destroyed or where there is a reasonable fear that the person who received the report may be colluding with the offender or involved in the infringement itself.

Mode: by printing or electronic means or means of dissemination can reach a large number of people.

3) Report to the judicial or accounting authority.

Note: according to the provisions in comment:

- in priority way favored the use of the inner channel;
- only when the conditions of art. 6 of Legislative Decree no. 24/2023 are met, external reporting is possible;
- the use of public disclosure must be considered a kind of extreme remedy.

8. Information, instructions and communications

The channels and the methods and references for the reports will be made known through poster systems, to employees and collaborators, as well as with other systems accessible by all interested parties, such as the appropriate section of the website.

The authorised parties will be informed of specific operational instructions on the various aspects of the procedure, without prejudice to the training provided.

Any changes will be adequately communicated with the same systems.

9. Sanctions

In relation to the provisions of Legislative Decree 24/2023 are punishable persons who, however interested in the procedure, do not comply with the requirements provided and this procedure.

The violation of the principles and behavior indicated compromises the relationship of trust between the company and the perpetrators of the violation, whether they are directors, employees, consultants, collaborators, customers or suppliers or others and may give rise to sanctions of various kinds.

Whistleblowing Procedure

19/01/2024

LAWER S.p.A - Via Amendola, 12/14 - 13836 Cossato (BI) Italy | Tel. +39 (0)15 9899511 | Telefax +39 (0)15 9842211

E-Mail sales@lawer.com | CF e P. IVA/TVA/VAT N° IT 00500780028 | Rag. Soc. Trib. Biella N° 7404

The measures adopted, in relation to the gravity of the violations, the typology of the violated rule, the modalities of the facts, the possible precedents and every other circumstance, are borrowed by the C.C.N.L.

9.1 Collaborators and external consultants

The subjects, linked to the company by collaboration or consultancy relationships, that implement, in the exercise of their activity, behaviors contrary to the provisions contained in the procedure may be sanctioned with the interruption of the relative relationship, on the basis of specific express termination clauses, included in the contracts concluded with such parties.

In less serious cases depending on the type of infringement, the precedents, the context in which it was committed, the persons involved and any other circumstances, the Board of Directors, the President or the Chief Executive Officer may notify the offender of a warning.

9.2 Partners, customers and suppliers

The subjects, tied to the company by commercial relations, that implement, in the exercise of their activity, behaviors in contrast with the dispositions contained in the present procedure could be sanctioned, in the more serious cases according to the typology of the violation, of the previous ones, of the context in which it was committed, of the persons involved and of any other circumstance, with references, warnings or with the interruption of the relative relationship on the basis of specific clauses expressed in resolution, inserted in the contracts stipulated with such subjects.

9.3 General rules

As already indicated, the cases of infringement must be considered as examples without excluding the possibility of applying sanctions in relation to the gravity of the infringement.

The sanction system provided for here will be made known to the parties concerned first of all according to the provisions of the law as regards employees (billboard pursuant to art. 7 of Law 300/70) and in any case, for all, with appropriate means of communication, including personnel.

The following rules shall be taken into account when applying sanctions:

1. with respect to employees, including managers, the procedure referred to in art. 7 of Law 300/70
2. against any other person the violation must be challenged and the right to present justifications must be guaranteed before the adoption of the measure
3. in particular cases, the suspension of reports or functions may also be ordered, pending the decisions taken or pending the verification by the Judicial Authority or other Authorities. Moreover, such decisions are not a condition for the applicability of these sanctions
4. the application of individual measures will take account of the principle of proportionality in relation to the objective gravity of the fact or facts, the position of the subject, the intent of the conduct or the degree of fault, the causal contribution in case of multiple parties involved in the violation, the overall behavior and personality of the subject, the possible existence of precedents, the social and/or internal relevance of the behavior and any other relevant circumstances

In the case of a sentence, even of first instance, for the offences provided for by the Decree, the sentenced person must immediately notify the Sole Administrator or the Board of Directors and the Board of Statutory Auditors, as indicated above.