1. ENGLISH VERSION

2. ITALIAN VERSION

Information to be published on the Site

in the dedicated section "Whistleblowing"

Sipcam Oxon S.p.A.

Version	Date of issue	Object	Approved by	Effective from
V1	15/12/2023	Document Drafting	Responsabile Affari Legali e Societari	15/12/2023

Summary

Whistleblowing

Log in to the Service

Remember:

- to carefully keep the unique identification code of the report and the password issued by the Platform, as, in the event of loss, it cannot be recovered or duplicated in any way and access to the IT platform will no longer be possible.
- whereas a single channel must be used to submit the report/communication and to carry out subsequent integrations;
- whereas the use of the platform is the priority channel;
- that duplications of the same report should not be submitted.

1. The changes introduced by Legislative Decree no. 24/2023

What changes with the new discipline

In implementation of Directive (EU) 2019/1937, Legislative Decree no. 24 of 10 March 2023 concerning "the protection of persons who report violations of Union law and containing provisions concerning the protection of persons who report violations of national regulatory provisions" was issued.

The decree entered into force on 30 March 2023 and the provisions set out therein are effective from 15 July 2023.

- The decree applies to entities in the public and private sectors; with particular reference to the latter sector, the legislation extends the protections to whistleblowers who have employed, in the last year, an average of at least fifty employees or, even below this limit, to entities that deal with the so-called "employees". Sensitive sectors (services, products and financial markets and prevention of money laundering or terrorist financing, transport security and environmental protection) and those that adopt organisational and management models pursuant to Legislative Decree 231/2001.

- Only for private sector entities that have employed, in the last year, an average of employees, with permanent or fixed-term employment contracts, up to two hundred and forty-nine, the obligation to set up an internal reporting channel starts from 17.12. 2023.
- Until that date, the above-mentioned private entities that have adopted the 231 model or intend to adopt it continue to manage the internal reporting channels in accordance with the provisions of Legislative Decree no. 231/2001.

2. Entities required to comply with the rules

Private sector

The protection of whistleblowers operating in the private sector, provided for by Legislative Decree no. 24/2023, imposes the obligation to set up reporting channels for those entities in the same sector that meet at least one of the following conditions:

- have employed, in the last year, an average of at least fifty employees, with permanent or fixed-term employment contracts;
- they deal with some specific sectors (services, financial products and markets and prevention of money laundering or terrorist financing, transport security and environmental protection), even if in the last year they have not reached the average of at least fifty employees with permanent or fixed-term employment contracts;
- adopt the organisation and management models referred to in Legislative Decree 231/2001, even if in the last year they have not reached the average of at least fifty employees with permanent or fixed-term employment contracts.

Public sector

The obligation to set up internal reporting channels also applies to the following public sector entities:

- the public administrations referred to in Article 1, paragraph 2, of Legislative Decree no. 165 of 30 March 2001
- independent administrative guarantee, supervisory or regulatory authorities
- public economic entities, bodies governed by public law referred to in Article 3(1)(d) of Legislative Decree no. 50 of 18 April 2016
- public service concessionaires, publicly controlled companies and in-house companies, as defined, respectively, by Article 2, paragraph 1, letters m) and o) of Legislative Decree no. 175 of 19 August 2016, even if listed.

3. What you can report

Conduct, acts or omissions that harm the public interest or the integrity of the public administration or private entity and which consist of:

- administrative, accounting, civil or criminal offences;
- relevant unlawful conduct pursuant to Legislative Decree 231/2001, or violations of the organization and management models provided for therein;
- offences falling within the scope of EU or national acts in the following areas: public procurement; financial services, products and markets and the 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;
- acts or omissions affecting the financial interests of the Union;
- acts or omissions relating to the internal market;
- acts or conduct which frustrates the object or purpose of the provisions laid down in Union acts.

4. Choice of reporting channels

- internal (in the context of the work context);
- external (ANAC);
- public dissemination (through the press, electronic media or means of dissemination capable of reaching a large number of people);
- report to the judicial or accounting authority.

Internal Reporting Channel

The internal report addressed to the Company's Whistleblowing Manager can be submitted in the following ways:

a) **Paper transmission of the report** (ordinary mail or registered mail with acknowledgement of receipt addressed to the person managing the report), which bears the wording "To the attention of the Whistleblowing Reporting Manager – personal confidential" by **postal service to the address of the registered office.**

b) **Delivery *by hand*** (i.e. in a sealed envelope addressed to the Reporting Manager, with the wording confidential personal) to the registered office.

c) **Submission through the IT platform** for the forwarding/acquisition and management of whistleblowing reports.

For the transmission and management of internal reports made in writing, Sipcam Oxon S.p.A. has opted to use the Whistlelink IT platform available at the web address https://sipcamoxon.whistlelink.com/, by filling in the form prepared for this purpose.

The platform allows you to fill in, send and receive the "Report Form" electronically.

Once the report has been submitted, the whistleblower will see a unique identification code and password that are required for subsequent access.

The notification of successful notification is automatically sent to the mailbox of the reporting manager.

The whistleblower can monitor the progress of the investigation only by accessing the IT Platform and using the identification code and password received.

As an alternative to internal reports made in writing through the IT Platform, reports may be made at the motivated request of the reporting person, through a direct meeting set within a reasonable time, according to this procedures.

The tools for transmitting and managing reports guarantee confidentiality:

- ✓ the reporting person;
- ✓ facilitator;
- ✓ the person involved or in any case of the subjects mentioned in the report;
- ✓ the content of the report and related documentation.

The management of the reporting channels is entrusted to:

- to a person specifically trained to manage the reporting channel, identified as Lara Giuffrida belonging to the function of Corporate Affairs Officer;
- to a person specifically trained to manage the reporting channel, identified as Giovanni Affaba belonging to the function of Head of Legal and Corporate Affairs;
- to a person specifically trained for the management of the reporting channel, identified as Gian Franco Soffiotto belonging to the Member of the Supervisory Body.

External reporting channel

Whistleblowers can use the **external channel (ANAC)** when:

- there is no mandatory activation of the internal reporting channel in the context of the work context, i.e. this, even if mandatory, is not active or, even if activated, does not comply with what is required by law;
- the reporting person has already made an internal report and the same has not been followed up;
- the reporting person has reasonable grounds to believe that, if he or she were to make an internal report, it would not be effectively followed up or that the report could lead to a risk of retaliation;
- the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;

Public Disclosure

Whistleblowers may directly make a **public disclosure** when:

- the reporting person has previously made an internal and external report or has directly made an external report and has not been responded to within the established deadlines regarding the measures envisaged or adopted to follow up on the reports;
- the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
- The reporting person has reasonable grounds to believe that the external report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as those where evidence may be concealed or destroyed or where there is a well-founded fear that the person receiving the report may be colluding with or involved in the violator.

5. Conditions for reporting

Reasonableness

At the time of reporting or reporting to the judicial or accounting authority or of public disclosure, the reporting person or complainant must have reasonable and reasonable grounds to believe that the information about the violations reported, publicly disclosed or reported is true and falls within the scope of the law

Modality

Public reporting or disclosure must be made using the channels provided (internal, external and public disclosure) according to the criteria indicated above under the heading "Choice of reporting channels".

6. Assessment of the public interest and personal interest of the whistleblower

Reports must be made

- in the public interest, or
- in the interest of the integrity of the public administration or private entity.

The reasons that led the person to report, denounce or publicly disclose are irrelevant to the protection of the person.

7. What happens after the report?

How to manage reports

Sipcam Oxon S.p.A. provides:

- give notice to the reporting person of the receipt of the report within 7 days from the date of its receipt, unless explicitly requested otherwise by the reporting person or except in the case in which Sipcam Oxon S.p.A. considers that the notice would undermine the protection of the confidentiality of the identity of the reporting person;
- maintain dialogue with the reporting person and request additions from the latter, if necessary;
- diligently follow up on reports received;
- carry out the investigation necessary to follow up on the report, including through hearings and the acquisition of documents;
- give feedback to the reporting person within three months of the date of the acknowledgment of receipt or, in the absence of such an acknowledgement, within three months of the expiry of the period of seven days from the submission of the report;
- communicate the final outcome of the report to the reporting person.

8. Protection of the confidentiality of reporting persons

- The identity of the whistleblower may not be disclosed to persons other than those competent to receive or follow up on the reports;
- The 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;
- The alert is exempt from access to administrative documents and the right of generalised civic access;
- The protection of confidentiality is extended to the identity of the persons involved and of the persons mentioned in the report until the conclusion of the proceedings initiated on the basis of the report, in compliance with the same guarantees provided for the reporting person.

9. Compliance with the legislation on the protection of personal data

- The processing of personal data relating to the receipt and management of reports is carried out by Sipcam Oxon S.p.A., as data controller, in compliance with European and national principles on the protection of personal data, providing appropriate information to reporting persons and persons involved in reports, as well as adopting appropriate measures to protect the rights and freedoms of data subjects.
- In addition, the rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679 may be exercised within the limits of the provisions of Article 2-undecies of Legislative Decree No. 196 of 30 June 2003.

- Internal and external reports and related documentation are kept for the time necessary to process the report and in any case no longer than 5 years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set out in European and national legislation on the protection of personal data.

The complete information regarding the processing of personal data can be accessed as follows:

- Privacy notice – reporting person (2) (art. 13 EU Regulation 2016/679)
- Privacy notice – Person concerned (2) (art. 14 EU Regulation 2016/679)

(1) Insert links to the respective policies

10. Retaliation

"Retaliation" means any conduct, act or omission, even if only attempted or threatened, carried out as a result of the report, the complaint to the judicial or accounting authority or the public disclosure and which causes or may cause unjust damage to the reporting person or to the person who filed the complaint, directly or indirectly.

Examples of retaliatory behavior:

- dismissal, suspension or equivalent measures;
- relegation or non-promotion;
- change of duties, change of place of work, reduction of salary, modification of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanctions, including financial sanctions;
- coercion, intimidation, harassment or ostracism;
- discrimination or unfavourable treatment;
- the failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the worker had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, in particular on social media, or economic or financial harm, including loss of economic opportunities and loss of income;

- improper listing on the basis of a formal or informal sectoral or industry agreement, which may result in the person not being able to find employment in the sector or industry in the future;
- the early termination or cancellation of the contract for the supply of goods or services;
- the cancellation of a licence or permit;
- the request to undergo psychiatric or medical examinations.

10.1 Competence to ascertain retaliation

- The management of communications of retaliation in the public and private sectors is the responsibility of ANAC, which may avail itself, as far as its respective competences are concerned, of the collaboration of the Civil Service Inspectorate and the National Labour Inspectorate.
- The declaration of nullity of retaliatory acts is the responsibility of the judicial authority.

10.2 Proof of retaliation

- ANAC must ascertain that the conduct (act or omission) considered retaliatory is consequent to the report, complaint or disclosure.
- Once the whistleblower proves that they have made a report in accordance with the law and that they have suffered retaliatory behaviour, the employer has the burden of proving that such behaviour is in no way related to the report.
- Since this is a presumption of liability, it is necessary that evidence to the contrary emerges in the adversarial proceedings before ANAC. To this end, it is essential that the alleged perpetrator provides all the elements from which to infer the absence of the retaliatory nature of the measure taken against the whistleblower.

10.3 Retaliation protection extended to others

Protection from retaliation is extended to other parties, in addition to the whistleblower:

- the facilitator (a natural person who assists the whistleblower in the reporting process and operates within the same work context);
- to persons in the same working context as the reporting person, 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 family bond within the fourth degree;

- to the work colleagues of the reporting person or of the person who has filed a complaint or made a public disclosure, who work in the same working environment as the person and who have a habitual and current relationship with that person;
- entities owned by the reporting person or for which the same persons work, as well as entities operating in the same working environment as the aforementioned persons.

11 Whistleblower Protection

11.1 Non-punishability of Whistleblowers

It is not punishable for disclosing or disseminating information about violations:

- covered by the duty of secrecy, other than the professional legal and medical obligation, or
- relating to the protection of copyright, or
- the protection of personal data, or

if, at the time of the report, complaint or disclosure, it had reasonable grounds to believe that the disclosure or disclosure of the information was necessary to make the report and the disclosure was made in the manner required by law.

11.2 Loss of protections

Protections are not guaranteed when the criminal liability of the reporting person for the crimes of defamation or slander or in any case for the same crimes committed with the complaint to the judicial or accounting authority or his civil liability, for the same reason, in cases of wilful misconduct or gross negligence, is ascertained, even with a first instance judgment; In such cases, a disciplinary sanction may be imposed on the reporting person.

11.3 Measures to support whistleblowers

- Support measures are provided in the form of information, assistance and advice free of charge on how to report and on the protection from retaliation offered by national and EU legal provisions, on the rights of the person concerned, as well as on the terms and conditions of access to legal aid.
- A list of Third Sector entities that provide support measures to reporting persons is established at ANAC. The list, published by ANAC on its website, contains the Third Sector entities that carry out, according to the provisions of their respective statutes, the activities referred to in Legislative Decree No. 117 of 3 July 2017, and that have entered into agreements with ANAC.

informazioni da pubblicare sul sito

nella sezione dedicata “Whistleblowing”

Sipcam Oxon S.p.A.

Versione	Data di emissione	Oggetto	Approvato da	In vigore da
V1	15/12/2023	Redazione documento	Responsabile Affari Legali e Societari	15/12/2023

Sommario

Whistleblowing

Scopri come segnalare un illecito di interesse generale nell'ambito del contesto lavorativo.

Accedi al Servizio

Ricorda:

- di conservare con cura il codice identificativo univoco della segnalazione e la password rilasciati dalla Piattaforma, in quanto, in caso di smarrimento, lo stesso non potrà essere recuperato o duplicato in alcun modo e l'accesso alla piattaforma informatica non sarà più possibile.
- che per presentare la segnalazione/comunicazione e per effettuare le successive integrazioni deve essere utilizzato un unico canale;
- che l'utilizzo della piattaforma è il canale prioritario;
- che non vanno presentate duplicazioni della stessa segnalazione.

1. Le novità introdotte con il D.lgs. n. 24/2023

Cosa cambia con la nuova disciplina

In attuazione della Direttiva (UE) 2019/1937, è stato emanato il d.lgs. n. 24 del 10 marzo 2023 riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali".

Il decreto è entrato in vigore il 30 marzo 2023 e le disposizioni ivi previste sono efficaci dal 15 luglio 2023.

- Il decreto si applica ai soggetti del settore pubblico e del settore privato; con particolare riferimento a quest'ultimo settore, la normativa estende le protezioni ai segnalanti che hanno impiegato, nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati o, anche sotto tale limite, agli enti che si

occupano dei cd. Settori sensibili (servizi, prodotti e mercati finanziari e prevenzione del riciclaggio o del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente) e a quelli adottano modelli di organizzazione e gestione ai sensi del decreto legislativo 231/2001.

- Solo per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, fino a duecentoquarantanove, l'obbligo di istituire un canale interno di segnalazione decorre dal 17.12. 2023.
- Fino a tale data, i suddetti soggetti privati che hanno adottato il modello 231 o intendono adottarlo continuano a gestire i canali interni di segnalazione secondo quanto previsto dal d.lgs. 231/2001.

2. Gli enti tenuti a rispettare la disciplina

Settore privato

La protezione dei segnalanti operanti nel settore privato, prevista dal D.lgs. n. 24/2023, impone l'obbligo di predisporre canali di segnalazione a carico di quegli enti del medesimo settore che soddisfano almeno una delle seguenti condizioni:

- hanno impiegato, nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato;
- si occupano di alcuni specifici settori (servizi, prodotti e mercati finanziari e prevenzione del riciclaggio o del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente), anche se nell'ultimo anno non hanno raggiunto la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato;
- adottano i modelli di organizzazione e gestione di cui al decreto legislativo 231/2001, anche se nell'ultimo anno non hanno raggiunto la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato.

Settore pubblico

L'obbligo di predisporre i canali di segnalazione interna grava altresì sui seguenti soggetti del settore pubblico:

- le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165
- le autorità amministrative indipendenti di garanzia, vigilanza o regolazione
- gli enti pubblici economici, gli organismi di diritto pubblico di cui all'articolo 3, comma 1, lettera d), del decreto legislativo 18 aprile 2016, n. 50

- i concessionari di pubblico servizio, le società a controllo pubblico e le società in house, così come definite, rispettivamente, dall'articolo 2, comma 1, lettere m) e o), del decreto legislativo 19 agosto 2016, n. 175, anche se quotate.

3. Cosa si può segnalare

Comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del decreto legislativo 231/2001, o violazioni dei modelli di organizzazione e gestione ivi previsti;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- atti od omissioni che ledono gli interessi finanziari dell'Unione;
- atti od omissioni riguardanti il mercato interno;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.

4. Scelta dei canali di segnalazione

- interno (nell'ambito del contesto lavorativo);
- esterno (ANAC);
- divulgazione pubblica (tramite la stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone);
- denuncia all'Autorità giudiziaria o contabile.

Canale di segnalazione interno

La segnalazione interna destinata al Gestore delle segnalazioni della Società può essere presentata con le

seguenti modalità:

a) **Trasmissione cartacea della segnalazione** (posta ordinaria o con raccomandata con ricevuta di ritorno indirizzate al soggetto gestore della segnalazione), che rechi all'esterno la dicitura "All'attenzione del Gestore delle segnalazioni whistleblowing – riservata personale" a mezzo del **servizio postale all'indirizzo della sede legale.**

b) **Consegna *brevi manu*** (ovvero in busta chiusa indirizzata al Gestore delle segnalazioni, con la dicitura riservata personale) presso la sede legale.

c) **Invio mediante le Piattaforma informatica** per l'inoltro/acquisizione e la gestione delle segnalazioni di whistleblowing.

Per la trasmissione e la gestione delle segnalazioni interne effettuate in forma scritta, Sipcam Oxon S.p.A. ha optato per l'utilizzo piattaforma informatica Whistlelink disponibile all'indirizzo web https://sipcamoxon.whistlelink.com/ , compilando il modulo all'uopo predisposto.

La piattaforma consente di compilare, inviare e ricevere in modo informatizzato il "Modulo di segnalazione".

A seguito dell'inoltro della segnalazione, il whistleblower visualizza un codice identificativo univoco e una password necessari per i successivi accessi.

La notifica di avvenuta segnalazione viene inviata automaticamente alla mailbox del gestore della segnalazione.

Il whistleblower può monitorare lo stato di avanzamento dell'istruttoria unicamente accedendo alla Piattaforma informatica ed utilizzando il codice identificativo e la password ricevuti.

In alternativa alle segnalazioni interne effettuate in forma scritta mediante Piattaforma informatica, le segnalazioni possono essere effettuate su richiesta motivata della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole, secondo le modalità pubblicate nel sito https://www.sipcam-oxon.com/en/whistleblowing

Gli strumenti di trasmissione e gestione delle segnalazioni, garantiscono la riservatezza:

- ✓ della persona segnalante;
- ✓ del facilitatore;
- ✓ della persona coinvolta o comunque dei soggetti menzionati nella segnalazione;
- ✓ del contenuto della segnalazione e della relativa documentazione.

La gestione dei canali di segnalazione è affidata:

- a una persona specificamente formata per la gestione del canale di segnalazione, individuata in Lara Giuffrida appartenente alla funzione di Funzionario Affari Societari;
- a una persona specificamente formata per la gestione del canale di segnalazione, individuata in Giovanni Affaba appartenente alla funzione di Responsabile Affari Legali e Societari;
- a una persona specificamente formata per la gestione del canale di segnalazione, individuata in Gian Franco Soffiotto appartenente alla funzione di Membro dell'Organismo di Vigilanza.

Canale di segnalazione esterno

I segnalanti possono utilizzare il canale esterno (ANAC) quando:

- non è prevista, nell'ambito del contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto richiesto dalla legge;
- la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione potrebbe determinare un rischio di ritorsione;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;

Divulgazione pubblica

I segnalanti possono effettuare direttamente una divulgazione pubblica quando:

- la persona segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna e non è stato dato riscontro entro i termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- la persona segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

5. Condizioni per la segnalazione

Ragionevolezza

Al momento della segnalazione o della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica, la persona segnalante o denunciante deve avere un ragionevole e fondato motivo di ritenere che le informazioni sulle violazioni segnalate, divulgate pubblicamente o denunciate siano vere e rientrino nell'ambito della normativa

Modalità

La segnalazione o divulgazione pubblica deve essere effettuata utilizzando i canali previsti (interno, esterno e divulgazione pubblica) secondo i criteri indicati sopra alla voce “Scelta dei canali di segnalazione”.

6. Valutazione dell'interesse pubblico e dell'interesse personale del segnalante

Le segnalazioni devono essere effettuate

- nell’interesse pubblico o
- nell’interesse alla integrità dell’amministrazione pubblica o dell’ente privato.

I motivi che hanno indotto la persona a segnalare, denunciare o divulgare pubblicamente sono irrilevanti ai fini della sua protezione.

7. Cosa accade dopo la segnalazione?

Modalità di gestione delle segnalazioni

Sipcam Oxon S.p.A. provvede a:

- dare avviso alla persona segnalante del ricevimento della segnalazione entro 7 giorni dalla data del suo ricevimento, salvo esplicita richiesta contraria della persona segnalante ovvero salvo il caso in cui Sipcam Oxon S.p.A. ritenga che l'avviso pregiudicherebbe la protezione della riservatezza dell’identità della persona segnalante;
- mantenere le interlocuzioni con la persona segnalante e richiedere a quest'ultima, se necessario, integrazioni;
- dare diligente seguito alle segnalazioni ricevute;
- svolgere l'istruttoria necessaria a dare seguito alla segnalazione, anche mediante audizioni e acquisizione di documenti;
- dare riscontro alla persona segnalante entro tre mesi dalla data dell’avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione;
- comunicare alla persona segnalante l'esito finale della segnalazione.

8. Protezione della riservatezza delle persone segnalanti

- L'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni;
- La protezione riguarda non solo il nominativo del segnalante ma anche tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante;
- La segnalazione è sottratta all'accesso agli atti amministrativi e al diritto di accesso civico generalizzato;
- La protezione della riservatezza è estesa all'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore della persona segnalante.

9. Rispetto della normativa in materia di protezione dei dati personali

- Il trattamento di dati personali relativi al ricevimento e alla gestione delle segnalazioni è effettuato da Sipcam Oxon S.p.A., in qualità di titolare del trattamento, nel rispetto dei princìpi europei e nazionali in materia di protezione di dati personali, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte nelle segnalazioni, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.
- Inoltre, i diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.
- Le segnalazioni interne ed esterne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui alla normativa europea e nazionale in materia di protezione di dati personali.

L'informativa completa relativa al trattamento dei dati personali è accessibile come segue:

- Informativa al Segnalante (2) (art. 13 Regolamento UE 2016/679)
- Informativa alle Persone coinvolte (2) (art. 14 Regolamento UE 2016/679)

10. Ritorsioni

Pe “ritorsione” si intende qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all’autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.

Esempi di comportamenti ritorsivi:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l’impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

10.1 Competenza ad accertare la ritorsione

- La gestione delle comunicazioni di ritorsioni nel settore pubblico e nel settore privato compete ad ANAC che può avvalersi, per quanto di rispettiva competenza, della collaborazione dell'Ispettorato della funzione pubblica e dell'Ispettorato nazionale del lavoro.
- La dichiarazione di nullità degli atti ritorsivi spetta all'Autorità giudiziaria.

10.2 Prova della ritorsione

- ANAC deve accertare che il comportamento (atto o omissione) ritenuto ritorsivo sia conseguente alla segnalazione, denuncia o divulgazione.
- Una volta che il segnalante provi di aver effettuato una segnalazione in conformità alla normativa e di aver subito un comportamento ritenuto ritorsivo, spetta al datore di lavoro l'onere di provare che tale comportamento non è in alcun modo collegato alla segnalazione.
- Trattandosi di una presunzione di responsabilità, è necessario che le prove in senso contrario emergano nel contraddittorio davanti ad ANAC. A tal fine è fondamentale che il presunto responsabile fornisca tutti gli elementi da cui dedurre l'assenza della natura ritorsiva della misura adottata nei confronti del segnalante.

10.3 Protezione da ritorsioni estesa ad altri soggetti

La protezione da ritorsioni è estesa ad altri soggetti, oltre al segnalante:

- al facilitatore (persona fisica che assiste il segnalante nel processo di segnalazione e operante all'interno del medesimo contesto lavorativo);
- alle persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;

- agli enti di proprietà della persona segnalante o per i quali le stesse persone lavorano nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

11 Protezione dei Segnalanti

11.1 Non punibilità dei Segnalanti

Non è punibile chi riveli o diffonda informazioni sulle violazioni:

- coperte dall'obbligo di segreto, diverso da quello professionale forense e medico, o
- relative alla tutela del diritto d'autore o
- alla protezione dei dati personali ovvero

se, al momento della segnalazione, denuncia o divulgazione, aveva ragionevoli motivi di ritenere che la rivelazione o diffusione delle informazioni fosse necessaria per effettuare la segnalazione e la stessa è stata effettuata nelle modalità richieste dalla legge.

11.2 Perdita delle tutele

Le tutele non sono garantite quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave; in tali casi alla persona segnalante o denunciante può essere irrogata una sanzione disciplinare.

11.3 Misure di sostegno ai segnalanti

- Sono previste misure di sostegno che consistono in informazioni, assistenza e consulenze a titolo gratuito sulle modalità di segnalazione e sulla protezione dalle ritorsioni offerta dalle disposizioni normative nazionali e da quelle dell'Unione europea, sui diritti della persona coinvolta, nonché sulle modalità e condizioni di accesso al patrocinio a spese dello Stato.
- È istituto presso l'ANAC l'elenco degli enti del Terzo settore che forniscono alle persone segnalanti misure di sostegno. L'elenco, pubblicato dall'ANAC sul proprio sito, contiene gli enti del Terzo settore

che esercitano, secondo le previsioni dei rispettivi statuti, le attività di cui al decreto legislativo 3 luglio 2017, n. 117, e che hanno stipulato convenzioni con ANAC.