INFORMATIVA PRIVACY (artt. 13-14 GDPR)

Il presente documento contiene l'informativa prevista dagli articoli 13 e 14 del Regolamento UE 679/2016 (GDPR), in relazione al trattamento dei dati personali degli interessati che vengono coinvolti, a vario titolo, nelle segnalazioni di violazioni rilevanti ai sensi della Procedura Whistleblowing di PRO.STAND SRL.

Titolare

Titolare del trattamento dei dati personali è PRO.STAND SRL, con sede legale ed operativa in Via Santarcangiolese, 18-18A/B, Poggio Torriana, e-mail privacy@prostand.com

Dati personali e conferimento facoltativo

In linea di principio, il sistema di segnalazione illeciti può essere utilizzata **senza fornire dati personali** propri o di terzi. Tuttavia, nell'ambito della procedura di segnalazione, è possibile divulgare **volontariamente** dati personali, in particolare informazioni sulla propria identità, nome e cognome, paese di residenza, numero di telefono o indirizzo e-mail.
Di regola, inoltre, **non richiediamo o trattiamo alcuna categoria particolare di dati personali**, ad esempio sull'origine razziale e/o etnica, convinzioni religiose e/o filosofiche, appartenenza sindacale o orientamento o vita sessuale. Tuttavia, a causa di campi di testo libero nel modulo di registrazione, tali categorie particolari di dati personali possono essere da te volontariamente comunicati, se li ritieni necessari.
La segnalazione può contenere anche **dati personali di terzi**.

Le persone a cui si riferiscono i dati personali trattati sono i) persone a conoscenza dei fatti segnalati, o che comunque vengono richieste di fornire informazioni a fronte di una segnalazione ii) "soggetti coinvolti" (cioè incolpata della violazione oggetto della segnalazione), iii) "soggetti tutelati" (cioè che godono delle tutele inderogabili previste dalla normativa Whistleblowing a fronte di una segnalazione), iv) Case Manager persone fisiche, v) altre persone che a vario titolo possono essere messe a conoscenza dell'esistenza e del follow-up della segnalazione.

I dati trattati potranno includere dati e omissioni punibili da un tribunale o da un'autorità amministrativa, in particolare anche al sospetto di commissione di reati, e a condanne penali o misure di prevenzione ai sensi dell'art. 10 del GDPR. Tali dati di cui all'art. 10 del GDPR devono essere trattati solo in caso di assoluta necessità, sono documentati per iscritto e conservati solo nella misura strettamente necessaria dopo che la decisione sul reato è divenuta definitiva in un procedimento in cui sono stati trattati; la conservazione avviene, se possibile, senza rielaborazione.

Il **conferimento** dei tuoi dati personali **è facoltativo** e pertanto l'eventuale mancato conferimento dei dati non pregiudicherà il tuo diritto a ricevere un riscontro dopo l'invio della tua segnalazione, e, se hai rivelato la tua identità, a godere delle tutele previste dalla legge.

I segnalanti che trattano dati personali di loro conoscenza al di là di quanto necessario per dare seguito alla segnalazione, assumono la veste di Titolari del trattamento ai sensi dell'art. 4 n 7 del GDPR.

Comunicazione dei dati personali

Il Titolare nel rispetto della **tutela della riservatezza** dell'identità del segnalante, potrà **condividere** i dati, in conformità al principio di stretta necessità, proporzionalità e minimizzazione, con:

i. **Altre funzioni interne del Titolare**, che i Case Manager dello stesso reputino opportuno coinvolgere nelle azioni di sèguito di una segnalazione.
ii. **Case Manager** cioè agli organi, interni o esterni, designati dalla società ricevente ad ammettere e/o esaminare nel merito la segnalazione e/o ad adottare le azioni conseguenti, incluso il riscontro al segnalante.
iii. **Soggetti terzi espressamente designati come Responsabili esterni** del Trattamento per finalità di hosting, manutenzione o gestione tecnica del datacenter e della piattaforma on-line da te usata per eseguire la segnalazione e del relativo database.
iv. **Autorità esterne competenti** in base alle normative applicabili (es. autorità giudiziaria, organi di polizia, guardia di finanza, ANAC – Autorità Nazionale Anticorruzione, etc.).
v. **Studi e/o consulenti legali, consulenti di compliance aziendale e/o altri soggetti coinvolti nel processo di valutazione della segnalazione** (es. periti di parte, consulenti tecnici, altre società del nostro gruppo presso le quali vengano accentrate le attività di investigazione e decisione delle segnalazioni o che risultino a qualsiasi titolo coinvolte in una violazione segnalata).

Realizzazione tecnica e sicurezza dei vostri dati

Il canale di segnalazione on-line include un'opzione per la comunicazione anonima tramite una connessione criptata. Quando si utilizza il sistema di segnalazione illeciti, l'indirizzo IP e la geolocalizzazione del dispositivo da te utilizzato (PC, tablet, smartphone) non vengono memorizzati in nessun momento. Ti raccomandiamo, se possibile, di **non collegarti al sistema di segnalazione da un dispositivo aziendale**. Durante l'invio della segnalazione, dovrai creare la password di accesso ad una Inbox Sicura, per poter poi comunicare con noi in modo protetto. **È tuo dovere proteggere adeguatamente la riservatezza sia del codice identificativo della segnalazione da te effettuata (che ti sarà comunicato dal nostro sistema), sia della password di accesso all'Inbox Sicura**. Manteniamo misure tecniche e organizzative adeguate per garantire la protezione dei dati e la riservatezza. Il canale di comunicazione internet usato è cifrato tramite protocolli avanzati. I dati saranno memorizzati in un formato cifrato presso un datacenter certificato a norma ISO 27001, ubicato in Germania o in Svizzera.

I dati personali non necessari per la gestione di una Segnalazione non verranno raccolti o verranno immediatamente cancellati se raccolti involontariamente.

Trasferimento dati extra-SEE. Diffusione

I dati potranno essere trasferiti extra-SEE in Svizzera, dove è ubicato un datacenter del fornitore del servizio saas Integrity Line. la garanzia applicabile a tale trasferimento ai sensi e per gli effetti del GDPR è la decisione di adeguatezza della Commissione UE circa la normativa svizzera sulla privacy.

I dati **non** saranno **diffusi**, se non nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Finalità e base giuridica

I dati saranno trattati per i) valutare l'ammissibilità e fondatezza della segnalazione di illeciti da te comunicata, ii) applicare le misure di tutela e supporto dei soggetti protetti dalla normativa in materia di Whistleblowing, iii) dare seguito alla segnalazione e, se possibile, misure di risposta ai risultati di una segnalazione, iv) applicare eventuali misure disciplinari contro chi segnala con dolo o colpa grave, o contro eventuali soggetti coinvolti ai quali sia addebitabile la violazione segnalata, v) usare gli esiti delle segnalazioni come prova in procedimenti giudiziari, vi) adempiere a qualsiasi obbligo previsto da una legge, da un regolamento o da un'altra normativa applicabile.

Base giuridica del trattamento per le finalità sub i), ii) e iii) (in relazione alle finalità di attuare misure di risposta ai risultati di una segnalazione, strettamente necessarie per rimuovere le conseguenze della Violazione segnalata) è l'esigenza di adempiere agli obblighi previsti a carico del Titolare dalla legge, da un regolamento o da un'altra normativa.
In relazione alle finalità di attuare misure di risposta ai risultati di una segnalazione, eventualmente diverse da quelle strettamente necessarie per rimuovere le conseguenze della Violazione segnalata, la base giuridica è l'interesse legittimo del Titolare di migliorare l'assetto dell'organizzazione.
In relazione alle finalità disciplinari, la base giuridica è l'interesse legittimo del Titolare di perseguire in sede disciplinare eventuali inosservanze della Procedura Whistleblowing del Titolare e/o, più in generale, della normativa relativa al Whistleblowing.
In relazione alle finalità di uso dei dati come prova in procedimenti giudiziari, la base giuridica è l'interesse legittimo del Titolare di esercitare la difesa dei propri diritti.

Durata della conservazione

I dati personali pervenuti al Titolare ma non strettamente necessari alla valutazione della segnalazione verranno immediatamente cancellati.
I dati di segnalazione e la relativa documentazione saranno conservati per il tempo necessario al trattamento della segnalazione e comunque al più tardi non oltre 5 (cinque) anni (in Italia) dalla data della comunicazione dell'esito finale della procedura di segnalazione (nel rispetto degli obblighi di riservatezza delle informazioni nonchè di limitazione della conservazione, previsti dalle normative applicabili in materia), e oltre tale periodo per tutto il tempo necessario all'espletamento di un procedimento amministrativo o giudiziario già avviato o per procedimenti investigativi ai sensi del Codice di Procedura Penale.

Diritti

Il Segnalante può rivolgersi in ogni momento al Titolare, senza formalità, per esercitare i seguenti diritti: a) accedere ai dati, b) rettificare i dati se inesatti, c) aggiornare i dati se obsoleti, d) richiedere la cancellazione dei dati, e) richiedere la limitazione del trattamento dei dati, f) opporsi in qualsiasi momento al trattamento dei dati per motivi derivanti dalla propria situazione particolare, g) ricevere la notifica di una violazione dei dati nel caso in cui la stessa comporti un elevato rischio per i diritti o le libertà fondamentali degli interessati, h) (se il Segnalante ha rivelato la propria identità, o, in caso di Segnalazione anonima, ciò è possibile anche senza rivelare l'identità), controllare, correggere e approvare il testo di una segnalazione che sia stata trascritta dal Titolare dopo essere pervenuta in una forma che non prevede l'utilizzo di una forma scritta (es. tramite incontro personale, telefonata o altra forma orale non registrata, posta ordinaria). La revoca del consenso non pregiudica la liceità del trattamento e della comunicazione effettuata su base volontaria fino alla revoca.
Previa richiesta di prova della tua identità (salvo nel caso tu abbia deciso di restare anonimo) riscontreremo la richiesta di esercizio dei diritti entro 30 giorni dalla ricezione della segnalazione, salvo in caso si renda necessario un particolare approfondimento del quale, in tal caso, ti invieremo un avviso.

Finchè e nella misura in cui sia necessario per proteggere l'identità di un segnalante, di un altro soggetto tutelato così come definito dalla normativa vigente, o delle persone interessate a una azione di sèguito (esempio case manager, persone informate sui fatti segnalati), e per conseguire gli scopi di prevenzione e punizione delle Violazioni, in particolare per prevenire i tentativi di impedire, compromettere o ritardare le Informazioni o le azioni di sèguito basate sulle Informazioni, in particolare per la durata di un procedimento amministrativo o giudiziario o di un procedimento preliminare ai sensi del codice di procedura penale, i seguenti diritti di una persona fisica interessata non si applicano:

- Diritto all'informazione, Diritto di rettifica, Diritto di cancellazione, Diritto alla limitazione del trattamento, Diritto di opposizione, Diritto alla notifica di una violazione dei dati personali.

Al ricorrere delle condizioni sopra previste, pertanto, il Titolare si asterrà dal fornire informazioni ad una persona interessata da una Segnalazione.

Il Segnalante se ritiene che i diritti suddetti siano stati violati può sempre proporre reclamo all'Autorità di controllo competente.

In Italia l'Autorità di controllo è il Garante per la protezione dei dati personali, con sede in Piazza Venezia, 11 - 00187 Roma, PEC: protocollo@pec.gpdp.it.

PRIVACY INFORMATION (articles 13-14 GDPR)

This document contains the information required by articles 13 and 14 of EU Regulation 679/2016 (GDPR), in relation to the processing of personal data of interested parties who are involved, for various reasons, in reporting significant violations pursuant to the Whistleblowing Procedure of PRO.STAND SRL.

Holder

The personal data controller is PRO.STAND SRL, with registered and operating office in Via Santarcangiolese, 18-18A/B, Poggio Torriana, e-mail privacy@prostand.com

Personal data and optional provision

In principle, the whistleblowing system can be used without providing your own or third-party personal data. However, as part of the reporting process, you may voluntarily disclose personal data, in particular information about your identity, first and last name, country of residence, telephone number or email address.

Furthermore, as a rule, we do not request or process any particular category of personal data, for example about racial and/or ethnic origin, religious and/or philosophical beliefs, trade union membership or sex life or orientation. However, due to free text fields in the registration form, such special categories of personal data may be voluntarily disclosed by you, if you deem it necessary.

The report may also contain personal data of third parties.

The persons to whom the processed personal data refer are i) persons aware of the facts reported, or who are in any case requested to provide information following a report ii) "subjects involved" (i.e. blamed for the violation object of the report), iii) "protected subjects" (i.e. who enjoy the mandatory protections provided for by the Whistleblowing legislation in relation to a report), iv) Case Manager natural persons, v) other persons who for various reasons can be made aware of the existence and follow-up up of the report.

The data processed may include data and omissions punishable by a court or administrative authority, in particular also on suspicion of commission of crimes, and on criminal convictions or preventive measures pursuant to art. 10 of the GDPR. Such data pursuant to art. 10 of the GDPR must be processed only in case of absolute necessity, are documented in writing and kept only to the extent strictly necessary after the decision on the offense has become final in a proceeding in which they were processed; storage takes place, if possible, without reprocessing.

The provision of your personal data is optional and therefore any failure to provide data will not affect your right to receive feedback after sending your report, and, if you have revealed your identity, to enjoy the protections provided by law.

Reporters who process personal data of their knowledge beyond what is necessary to follow up on the report, assume the role of Data Controllers pursuant to art. 4 n 7 of the GDPR.

Communication of personal data

In compliance with the protection of the confidentiality of the identity of the whistleblower, the Data Controller may share the data, in accordance with the principle of strict necessity, proportionality and minimization, with:

the. Other internal functions of the Data Controller, which the Case Managers of the same deem appropriate to involve in the follow-up actions of a report.

ii. Case Manager, i.e. to the bodies, internal or external, designated by the receiving company to admit and/or examine the merits of the report and/or to adopt the consequent actions, including feedback to the whistleblower.

iii. Third parties expressly designated as External Data Processors for hosting, maintenance or technical management purposes of the data center and of the online platform used by you to make the report and of the related database.

iv. Competent external authorities based on the applicable regulations (e.g. judicial authorities, police bodies, financial police, ANAC - National Anti-Corruption Authority, etc.).

v. Law firms and/or consultants, corporate compliance consultants and/or other subjects involved in the process of evaluating the report (e.g. party experts, technical consultants, other companies of our group in which the investigation and decision-making activities of the reports or who are involved in any capacity in a reported violation).

Technical implementation and security of your data

The online reporting channel includes an option for anonymous communication over an encrypted connection. When using the offense reporting system, the IP address and geolocation of the device you are using (PC, tablet, smartphone) are not stored at any time. We recommend that, if possible, you do not connect to the reporting system from a company device. When sending the report, you will need to create the password to access a Secure Inbox, in order to then be able to communicate with us in a secure way. It is your duty to adequately protect the confidentiality of both the identification code of the report you made (which will be communicated to you by our system), and the password to access the Secure Inbox. We maintain appropriate technical and organizational measures to ensure data protection and confidentiality. The internet communication channel used is encrypted using advanced protocols. The data will be stored in an encrypted format in an ISO 27001 certified data center located in Germany or Switzerland.

Personal data not necessary for the management of a Report will not be collected or will be immediately deleted if collected unintentionally.

Non-EEA data transfer. Spread

The data may be transferred outside the EEA to Switzerland, where a data center of the Integrity Line saas service provider is located. the guarantee applicable to this transfer pursuant to and for the purposes of the GDPR is the adequacy decision of the EU Commission regarding the Swiss privacy legislation.

The data will not be disclosed, except in the cases specifically provided for by national or European Union law.

Purpose and legal basis

The data will be processed to i) evaluate the admissibility and validity of the report of offenses communicated by you, ii) apply the protection and support measures of the subjects protected by the legislation on Whistleblowing, iii) follow up on the report and, if possible, response measures to the results of a report, iv) apply any disciplinary measures against those who report with willful misconduct or gross negligence, or against any persons involved who are responsible for the reported violation, v) use the results of reports as evidence in legal proceedings , vi) fulfill any obligation established by a law, regulation or other applicable legislation.

Legal basis of the processing for the purposes under i), ii) and iii) (in relation to the purposes of implementing response measures to the results of a report, strictly necessary to remove the consequences of the reported Violation) is the need to fulfill the obligations provided for by the Data Controller by law, by a regulation or by other legislation.

In relation to the purposes of implementing response measures to the results of a report, possibly different from those strictly necessary to remove the consequences of the reported Violation, the legal basis is the legitimate interest of the Data Controller to improve the organization structure.
In relation to the disciplinary purposes, the legal basis is the legitimate interest of the Data Controller to prosecute any non-compliance with the Data Controller's Whistleblowing Procedure and/or, more generally, with the legislation relating to Whistleblowing.
In relation to the purposes of using data as evidence in legal proceedings, the legal basis is the legitimate interest of the Data Controller to exercise the defense of their rights.

Duration of storage
Personal data received by the Data Controller but not strictly necessary for the evaluation of the report will be immediately cancelled.
The reporting data and related documentation will be kept for the time necessary to process the report and in any case no later than 5 (five) years (in Italy) from the date of communication of the final outcome of the reporting procedure (in compliance with obligations of confidentiality of information as well as limitation of conservation, provided for by the applicable regulations on the subject), and beyond this period for all the time necessary for the completion of an administrative or judicial proceeding already started or for investigative proceedings pursuant to the Criminal Procedure Code .

Rights
The Whistleblower can contact the Data Controller at any time, without formalities, to exercise the following rights: a) access the data, b) rectify the data if inaccurate, c) update the data if obsolete, d) request the deletion of the data, and) request the restriction of data processing, f) object at any time to data processing for reasons arising from your particular situation, g) receive notification of a data breach in the event that it involves a high risk to your rights o the fundamental freedoms of the interested parties, h) (if the Whistleblower has revealed his identity, or, in the case of an anonymous Report, this is possible even without revealing his identity), check, correct and approve the text of a report that is been transcribed by the Data Controller after being received in a form that does not require the use of a written form (e.g. through a personal meeting, telephone call or other unregistered oral form, ordinary mail). The withdrawal of consent does not affect the lawfulness of the processing and communication carried out on a voluntary basis until the withdrawal.
Upon request for proof of your identity (unless you have decided to remain anonymous) we will respond to the request to exercise the rights within 30 days of receiving the report, unless particular in-depth analysis is necessary which, in this case, will we will send a notice.
As long as and to the extent that it is necessary to protect the identity of a whistleblower, of another protected subject as defined by current legislation, or of persons interested in a follow-up action (e.g. case managers, persons informed of the reported facts), and to achieve the purposes of preventing and punishing Infringements, in particular to prevent attempts to prevent, impair or delay the Information or subsequent actions based on the Information, in particular for the duration of an administrative or judicial proceeding or a proceeding preliminary under the Criminal Procedure Code, the following rights of a natural person concerned do not apply:
- Right to information, Right to rectification, Right to erasure, Right to restriction of processing, Right to object, Right to notification of a personal data breach.
Therefore, upon occurrence of the above conditions, the Data Controller will refrain from providing information to a person affected by a Report.
If the Reporter believes that the aforementioned rights have been violated, he can always lodge a complaint with the competent Supervisory Authority.

In Italy, the Supervisory Authority is the Italian Protection Authority, with headquarters in Piazza Venezia, 11 - 00187 Rome, PEC: protocol@pec.gpdp.it.