INFORMATIVA SUL TRATTAMENTO DATI PERSONALI AI SENSI DELL'ART. 13, REG. UE n. 679/2016 (GDPR) per segnalanti

IN RELAZIONE ALLE SEGNALAZIONI DI WHISTLEBLOWING (D.lgs. n. 24/2023; Dir. UE 1937/2029)

Titolare del Trattamento

Titolare del trattamento è ARRR S.p.A., con sede in Via di Novoli n. 26, 50127 – Firenze, e-mail: arrr@arrr.it.

Responsabile della protezione dati personali

Il Responsabile della Protezione dei Dati (RPD) / Data Protection Officer (DPO) è raggiungibile al seguente indirizzo e-mail: dpo@arrr.it.

Indicazioni sul trattamento

ARRR S.p.A., nell'intento di conformarsi alla Direttiva (UE) 2019/1937 ed al D.lgs. 10 marzo 2023, n. 24, che ne ha recepito il contenuto in ambito nazionale, ha istituito un apposito canale, una piattaforma protetta da misure di crittografia, attraverso cui segnalare violazioni di normative nazionali e dell'unione europea, indicate in dettaglio all'art. 2, comma 1, del d.lgs. 24/2023, commesse nell'ambito dell'organizzazione di ARRR S.p.A.
Tale canale permette a determinati soggetti che siano venuti a conoscenza nel contesto lavorativo di uno o più comportamenti impropri, di segnalarli in modo riservato o anche anonimo al Responsabile della Prevenzione della Corruzione e Trasparenza (in seguito "RPCT").

Tipologia e categorie di dati trattati

I dati oggetto di trattamento possono essere dati comuni (quali nome, cognome, indirizzo e-mail, numero di telefono), nonché eventuali dati giudiziari (relativi a condanne penali e reati, art. 10 GDPR). Il segnalante è invitato a comunicare le sole informazioni utili all'individuazione dei fatti segnalati. Qualora siano indicati nel contenuto della segnalazione dati particolari (relativi, tra gli altri, a condizioni di salute, orientamento sessuale o appartenenza sindacale, di cui all'art. 9 del REG. UE n. 679/2016, di seguito GDPR), questi ultimi potranno essere trattati ai sensi dell'art. 9 par. 2, lett. b) o g) GDPR.
Per procedere all'invio della segnalazione il segnalante dovrà compilare un *form* con alcune domande per fornire le informazioni rilevanti sul fatto oggetto di segnalazione. Il conferimento di tali informazioni è obbligatorio per procedere all'invio della segnalazione e consente al RPCT di valutare l'attendibilità del fatto segnalato e la credibilità del segnalante.
Il conferimento dei dati identificativi del segnalante è facoltativo, è possibile scegliere di rimanere anonimi ponendo un *flag* nell'apposita casellina proposta nella piattaforma al momento dell'invio della segnalazione. Lo stesso segnalante potrà identificarsi successivamente.
Le misure di protezione del segnalante che subisce ritorsioni di cui al D.lgs. 24/2023 si applicano anche nei casi di segnalazioni anonime, se la persona segnalante è stata successivamente identificata.
La registrazione delle segnalazioni avviene in modo anonimo nella piattaforma. Non è presente alcuna registrazione relativa all'indirizzo IP o all'ID macchina del computer su cui è stata effettuata la segnalazione.

Finalità, base giuridica del trattamento

La finalità è gestire correttamente le segnalazioni di eventuali illeciti e reati di cui, tra gli altri, dipendenti, collaboratori, fornitori siano venuti a conoscenza nel contesto lavorativo, tutelando i segnalanti da ritorsioni e garantendo riservatezza a segnalati e segnalanti (Obbligo di Legge - D.lgs. 10 marzo 2023, n. 24 e Direttiva (UE) 2019/1937). I dati personali sono trattati esclusivamente per lo svolgimento delle necessarie attività istruttorie volte a verificare la

fondatezza dei fatti segnalati, dell'accertamento degli stessi e per la definizione di azioni da intraprendere, di adozione delle eventuali misure correttive da applicare e dei conseguenti provvedimenti.
Ciò nel rispetto del principio di minimizzazione dei dati personali, di cui all'art. 5 del Reg. UE n. 679/2016 (GDPR).

Autorizzati al trattamento e Responsabile del trattamento
La responsabilità della gestione del canale interno di segnalazione è attribuita al RPCT, come previsto dall'art. 4, comma 5, D.lgs. 10 marzo 2023, n. 24. I dati relativi alle segnalazioni trasmesse sono conosciuti dal RPCT, dagli eventuali "autorizzati al trattamento" (art. 2 *quaterdecies*, D.lgs. n. 196/2003 e s.m.i., Codice Privacy) delle segnalazioni whistleblowing e da uno Studio Legale, che supporta il RPCT nella ricezione, gestione ed esame delle segnalazioni, tramite apposita piattaforma informatica crittografata ed è nominato nel ruolo di Responsabile del trattamento, ai sensi dell'art. 28 GDPR.

Destinatari
I dati personali trasmessi potranno essere comunicati, qualora necessario, all'Autorità Giudiziaria, alla Corte dei Conti e all'Autorità Nazionale Anticorruzione, che operano quali Titolari autonomi del trattamento. Si applicano le disposizioni di cui all'art. 12 del D.lgs. 24/2023.
Nel caso in cui il RPCT valuti di attribuire accertamenti, verifiche e/o analisi sulle segnalazioni, ovvero un supporto tecnico od approfondimenti in discipline specifiche su cui la segnalazione ha impatto, ad eventuali soggetti interni o esterni all'ente, questi conosceranno soltanto dati anonimi, salvi i casi in cui la conoscenza di dati personali risulti indispensabile per lo svolgimento dell'attività richiesta. In quest'ultimo caso saranno formalizzati ai sensi del GDPR i relativi obblighi.

Profilazione e diffusione dei dati
I dati personali relativi al segnalante e quelli dei soggetti indicati come possibili responsabili di condotte illecite, nonché di altri eventuali soggetti coinvolti nel contenuto della segnalazione, non sono soggetti a diffusione, né ad alcun processo decisionale interamente automatizzato, ivi compresa la profilazione.

Trasferimento all'estero
I dati relativi alle segnalazioni sono trattati all'interno dell'Unione Europea, sono conservati in server europei certificati ISO 27001 e le Società che li gestiscono sono europee.

Conservazione dei dati
Se le segnalazioni sono totalmente non pertinenti rispetto all'oggetto di segnalazione whistleblowing o non attendibili, sono cancellate al momento in cui si accerta la non pertinenza/non veridicità. In generale i dati relativi alle segnalazioni sono conservati il tempo necessario al trattamento delle stesse e, comunque, non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, come previsto dall'art. 14, comma 1, D.lgs. n. 24/2023. Potranno essere conservati dati anonimi sulle segnalazioni per valutare nel tempo, tra gli altri, la quantità di segnalazioni ricevute e gli ambiti che hanno riguardato.

Diritti dell'Interessato
Gli artt. da 15 a 22 GDPR conferiscono agli Interessati la possibilità di esercitare specifici diritti, quali, per esempio, il diritto di accesso, di rettifica, di cancellazione, di limitazione del trattamento, di opposizione al trattamento.
Il segnalante che ha svolto una segnalazione potrà in ogni momento accedere ai suoi dati tramite la piattaforma, cliccando sulla casella "Inbox sicura" e inserendo le credenziali relative alla

segnalazione svolta (codice univoco attribuito alla segnalazione e password da lui creata per quella segnalazione), così da rivedere i dati personali e le informazioni comunicate e conoscere lo stato in cui si trova la sua segnalazione.
Non sarà possibile ad alcuno conoscere se è in corso una segnalazione che lo riguarda e qual è l'oggetto della stessa, salvi i casi in cui questa sia pubblica perché è stata oggetto di divulgazione pubblica o di denuncia quando sia stata notificata al segnalato dalle competenti Autorità.
Il segnalante che si accorge di aver fornito informazioni incomplete o errate, può inviare una nuova segnalazione tramite la piattaforma in cui fa riferimento alla segnalazione precedente e descrive cosa dovrebbe essere corretto.
Gli altri diritti previsti dal GDPR, possono essere esercitati inviando una e-mail agli indirizzi di posta elettronica di Titolare o DPO indicati nella presente informativa. L'esercizio di tali diritti è limitato qualora possa causare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante o di altri soggetti coinvolti nella segnalazione.

Reclamo
Se l'Interessato ritiene che il trattamento dei dati che lo riguardano avvenga in violazione di quanto previsto dal GDPR ha diritto di proporre reclamo al Garante per la protezione dei dati personali, come previsto dall'art. 77 del GDPR, o di adire le opportune sedi giudiziarie, come disciplinato nell'art. 79 del GDPR.

English Version

PRIVACY POLICY
in accordance with art. 13, General Data Protection Regulation 2016/679 (Gdpr), relating to whistleblowing reports (Legislative Decree no. 24/2023; Dir. (EU) 1937/2029)

Data Controller
The Data Controller is ARRR S.p.A., with headquarters in Via di Novoli n. 26, 50127 – Firenze, e-mail: arrr@arrr.it.

Data Protection Officer (DPO)
Data Protection Officer (DPO) can be reached at the following e-mail address: dpo@arrr.it .

Indications on Data Processing
ARRR, in order to comply with Directive (EU) 2019/1937 and Legislative Decree No. 24 of 10 March 2023, which transposed its contents into national law, has set up a special channel, a platform protected by encryption measures, through which to report possible unlawful acts of employees and other persons, including, collaborators, suppliers, managers and directors of the Agency.
This channel allows anyone who has become aware, in the context of their work, of improper behaviour constituting violations of Union law and/or violations of national regulations, to report it confidentially or even anonymously to the Head of Prevention of Corruption and Transparency (hereinafter 'RPCT').

Type and categories of data processed
The data processed may be common data (such as name, surname, e-mail address, telephone number), as well as any judicial data (relating to criminal convictions and offences, Art. 10 GDPR). The person making the report is requested to communicate only information that is useful for identifying the facts reported. Should special data (relating to, among others, health conditions, sexual orientation or trade union membership, as referred to in Art. 9 of EU REG. no. 679/2016,

hereinafter GDPR) be indicated in the content of the report, the latter may be processed pursuant to Art. 9 par. 2 (b) or (g) GDPR.
In order to proceed with the submission of the report, the reporter will have to fill in a form with some questions to provide relevant information about the fact being reported. Providing this information is mandatory in order to proceed with sending the report and allows the RPCT to assess the reliability of the reported fact and the credibility of the reporter.
Providing the identification data of the reporter is optional; it is possible to choose to remain anonymous by placing a flag in the box provided in the platform when sending the report. The reporter himself/herself may identify him/herself at a later stage.
The protection measures for whistleblowers who suffer retaliation set out in Legislative Decree 24/2023 also apply in cases of anonymous reports, if the whistleblower is subsequently identified.
Reports are recorded anonymously in the platform. There is no recording of the IP address or machine ID of the computer on which the report was made.

Purpose, legal basis of Data Processing
The purpose of the processing is to properly handle reports of any unlawful acts and offences of which, among others, employees, collaborators, suppliers may have become aware in their work context, protecting the reporters from retaliation and guaranteeing confidentiality to the reporters and the persons involved in the content of the report (Legal Obligation - Legislative Decree no. 24 of 10 March 2023 and Directive (EU) 2019/1937). Personal data are processed exclusively for the purpose of carrying out the necessary investigative activities aimed at verifying the justification of the reported facts, the ascertainment of the same and the definition of actions to be taken, the adoption of any corrective measures to be applied and the consequent measures.
This is in compliance with the principle of personal data minimisation, as set out in Article 5 of EU Reg. no. 679/2016 (GDPR).

Data Processors and persons in charge of the processing
The responsibility for managing the internal whistleblowing channel is assigned to the RPCT, as provided for in Article 4(5) of Legislative Decree No. 24 of 10 March 2023. The data related to the reports transmitted are known by the RPCT, by any "processors" (art. 2 quaterdecies, Decree No. 196 of 30 June 2003 as amended or added) of whistleblowing reports, identified by the latter, in accordance with the Data Protection Policy of the Region of Tuscany and by a Law Firm, which supports the RPCT in receiving, managing and examining the reports, through a special encrypted IT platform and is appointed in the role of Data Processor, pursuant to art. 28 GDPR.

Recipients
The personal data transmitted may be communicated, if necessary, to the Judicial Authority, the Court of Auditors (i.e. Corte dei Conti) and the National Anti-Corruption Authority (i.e. ANAC), which act as autonomous Data Controllers. The provisions of Article 12 of Legislative Decree 24/2023 shall apply.
In the event that the RPCT decides to assign assessment, monitoring and/or analysis on the reports, or technical support or in-depth studies in specific disciplines on which the report has an impact, to persons internal or external to the entity, they will only know anonymous data, except in cases where knowledge of personal data is indispensable for the performance of the requested activity. In the latter case, the relevant obligations will be formalised in accordance with the GDPR.

Data Profiling and Dissemination
Personal data relating to the whistleblower and those of the persons indicated as possibly responsible for unlawful conduct, as well as any other persons involved in the content of the report, are not subject to dissemination, nor to any fully automated decision-making process, including profiling.

Transfer abroad
Data relating to reports are processed within the European Union, are stored in ISO 27001-certified European servers and the companies handling them are European.

Data Retention
If the reports are totally irrelevant with respect to the subject of the whistleblowing report or unreliable, they are deleted when the irrelevance/unreliability is established. In general, data relating to whistleblowing reports are retained for the time necessary to process them and, in any case, for no longer than five years from the date of communication of the final outcome of the whistleblowing procedure, as provided for in Article 14(1) of Legislative Decree no. 24/2023. Anonymous data on the reports may be stored in order to assess over time, among other things, the number of reports received and the areas they concerned.

Rights of the Data Subject
Articles 15 to 22 GDPR give Data Subjects the possibility to exercise specific rights, such as, for example, the right of access, rectification, cancellation, restriction of processing, opposition to processing.
A reporting person who has made a report may at any time access his or her data via the platform by clicking on the 'Secure Inbox' box and entering the credentials relating to the report made (the unique code assigned to the report and the password created by him or her for that report), in order to review the personal data and information communicated and to know the status of his or her report.
It will not be possible for anyone to know whether a report concerning him or her is in progress and what the subject of that report is, except in cases where the report is public because it has been publicly disclosed or has been the subject of a complaint when it has been notified to the reported person by the competent authorities.
A whistleblower who realises that he or she has provided incomplete or incorrect information may send a new report via the platform in which he or she refers to the previous report and describes what should be corrected.
The other rights provided for by the GDPR may be exercised by sending an e-mail to the Controller's or DPO's e-mail addresses indicated in this notice. The exercise of these rights shall be limited if it may cause actual and concrete prejudice to the protection of the confidentiality of the identity of the person making the report or of other persons involved in the report.

Complaint
If the Data Subject considers that the processing of data relating to him/her takes place in violation of the provisions of the GDPR, he/she has the right to lodge a complaint with the supervisory authority (in Italy, Garante per la protezione dei dati personali), as provided for in Article 77 of the GDPR, or to take legal action, as regulated in Article 79 of the GDPR.