INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI PER LA GESTIONE DELLE SEGNAZIONI DI ILLECITO – WHISTLEBLOWING

Informativa resa ai sensi degli artt. 13 e 14 del Regolamento UE 679/2016 (GDPR) sul trattamento dei dati personali relativi alle persone fisiche

Con la presente informativa, Terminal Darsena Toscana S.r.l. a socio unico (di seguito anche "la Società") fornisce informazioni relative al trattamento dei dati personali del soggetto interessato che effettua una segnalazione (di seguito, "il Segnalante") e degli altri soggetti interessati, menzionati o coinvolti nella segnalazione stessa, o dei potenziali responsabili degli illeciti oggetto di segnalazione (di seguito, "il Segnalato"). Tutti questi soggetti vengono anche definiti "Soggetti Interessati". Il trattamento sarà improntato a principi di correttezza, liceità, trasparenza e tutela della riservatezza.

TITOLARE DEL TRATTAMENTO

Titolare del trattamento è la società Terminal Darsena Toscana s.r.l. a socio unico, con sede legale in Loc. Darsena Toscana – Porto Industriale – 57123 Livorno, P. Iva: 01178350490, indirizzo mail privacy@tdt.it.

RESPONSABILE DELLA PROTEZIONE DATI (RPD o DPO)

Il Titolare ha provveduto a nominare quale DPO la società Digital Strategy S.r.l.s.u. – servizio MY DPO, con sede legale e operativa in Via dei Lanzi 33, 57123, Livorno (LI), contattabile all'indirizzo e-mail dpo@tdt.it.

FONTE DEI DATI TRATTATI

Le informazioni possono essere fornite:

- nella segnalazione, dal Segnalante;
- nel corso delle necessarie attività istruttorie (a titolo esemplificativo, da fonti pubbliche, terzi intervistati, etc.);
- durante il processo di gestione della segnalazione
- attraverso i log di traffico[1] sulle connessioni alla piattaforma di segnalazione registrati sui sistemi aziendali della Società.

La Società ha implementato, al proprio interno, sistemi di sicurezza informatica che rilevano i log di traffico delle connessioni via web (filtro web, sistemi antivirus, sistemi anti-malware). Pertanto, in caso di utilizzo di PC e/o smartphone aziendali collegati alla rete aziendale, suddetti sistemi di protezione e sicurezza informatica registrano i log di traffico riguardanti le connessioni alla piattaforma di whistleblowing; ciò comporta la registrazione su alcuni sistemi, all'interno del log, dell'indicazione di utente ed indirizzo IP che ha fatto il collegamento alla piattaforma.
Tuttavia, la Società ha adottato misure di sicurezza idonee ad escludere e/o ridurre al minimo la tracciabilità delle attività di Log. In ogni caso, la Società garantisce che queste informazioni siano accessibili esclusivamente al personale tecnico debitamente autorizzato e istruito.

[1] *In generale, i log sono file che registrano – e quindi permettono di ricostruire – l'intera "storia" delle operazioni effettuate da un utente o da una macchina. Tramite i log, infatti, vengono registrate tutte le operazioni, in ordine cronologico, svolte nel normale utilizzo di un software, di un applicativo o più semplicemente di un computer. Il log registra anche tutte le operazioni che un computer svolge in autonomia, senza necessità di intervento umano. La gestione dei log a livello aziendale permette di monitorare una serie di attività, tra cui gli accessi al sistema effettuati in un dato lasso temporale (anche quelli fuori dall'orario di lavoro, quelli non andati a buon fine o quelli tramite VPN), le transazioni fallite, eventuali anomalie (sia software che hardware) e possibili minacce malware. Tali informazioni sono necessarie per comprendere lo stato della sicurezza informatica aziendale: sia in caso di normale funzionamento della macchina ma, soprattutto, in caso di errori e problemi, come eventuali attacchi hacker, permettendo così alla funzione IT di indagarne le cause e trovare una risoluzione, evitando o bloccando tempestivamente situazioni pregiudizievoli.*

Resta inteso che non viene rilevata in alcun modo l'attività che viene effettuata dal segnalante dopo l'accesso alla piattaforma (che peraltro può riguardare distinte tipologie di segnalazione) ma viene rilevata solo la "chiamata" alla piattaforma, ovvero la connessione alla stessa.

Per garantire un anonimato totale al Segnalante, si raccomanda di effettuare la segnalazione da un dispositivo personale tramite rete privata non aziendale.

IMPORTANTE:

La piattaforma informatica adottata dalla Società – Whistleblower Software Aps prevede sistemi di sicurezza informatica che garantiscono un'elevata sicurezza dell'ambiente tramite il controllo degli accessi logici. La tracciabilità delle attività poste in essere all'interno di Whistleblower Software è garantita dalla predisposizione di sei livelli di registrazione che consentono di verificare eventi concernenti rispettivamente la visualizzazione di un evento, il registro completo di chi ha avuto accesso ad un caso e per quanto tempo, eventuali modifiche apportate, tentativi di utilizzo di valori o campi non validi, errori generati dal codice, tentativi di attacco a forza bruta.

Il metodo predefinito per l'autenticazione avviene tramite e-mail e password, queste ultime vengono archiviate in forma crittografata.

Queste informazioni sono accessibili esclusivamente al personale tecnico debitamente autorizzato e istruito.

La piattaforma Whistleblower Software Aps – al fine di garantire la miglior tutela delle informazioni ivi inserite - ha sviluppato un modello di crittografia end-to-end personalizzato; questo consente, prima che i server della Piattaforma ricevano i dati, che questi vengano crittografati lato client (sul dispositivo del segnalante o su quello del gestore del caso). Ciò significa che i dati vengono crittografati prima che l'HTTPS e la normale crittografia del disco entrino in gioco.

TIPOLOGIA DEI DATI TRATTATI

Qualora il Segnalante decida di non effettuare una segnalazione anonima optando per la segnalazione "in forma confidenziale" e/o utilizzando gli altri canali alternativi (posta elettronica, modalità cartacea con consegna a mano, incontro di persona con interlocuzione orale diretta), il Titolare tratterà i seguenti dati personali riferibili allo stesso:

- dati identificativi e di contatto forniti dal Segnalante in fase di registrazione e/o nel form di segnalazione, quali: nome, cognome, indirizzo e-mail o altri dati di contatto e qualsiasi altro dato personale contenuto nell'oggetto della segnalazione.
- eventuali dati di natura particolare ai sensi dell'art. 9 del GDPR, in quanto idonei a rivelare uno stato generale di salute (assenze per malattia, maternità, infortunio, etc.), l'idoneità allo svolgimento di specifiche mansioni, l'adesione ad un sindacato e/o ad un partito politico, la titolarità di cariche pubbliche elettive o infine le convinzioni religiose;
- eventuali dati giudiziari ai sensi dell'art. 10 del GDPR in quanto relativi a condanne penali e ai reati o a connesse misure di sicurezza.
- qualsiasi altro dato personale contenuto nella segnalazione;
- dati personali che dovessero emergere dalle successive attività istruttorie.

Nel caso in cui, invece, il Segnalante effettui una segnalazione anonima, il Titolare tratterà esclusivamente le informazioni fornite dal Segnalante nell'oggetto della segnalazione. A tal proposito, ove il segnalante voglia preservare l'anonimato si invita a rimuovere qualsiasi riferimento all'identità del Segnalante dalla segnalazione e dagli eventuali allegati.

A seguito della segnalazione potranno essere trattati anche dati personali, ivi compresi dati di natura particolare ai sensi dell'art. 9 del GDPR e/o dati cd. giudiziari ai sensi dell'art. 10 del GDPR, riferiti a terzi soggetti (definiti nel complesso "Soggetti Interessati"), tra cui:

- il soggetto Segnalato;
- i soggetti informati sui fatti;
- eventuali altri soggetti menzionati nella segnalazione e/o coinvolti nel processo di segnalazione.

Potranno, altresì, essere oggetto di trattamento i Log di traffico riguardanti le connessioni alla piattaforma di segnalazione registrati sui sistemi aziendali, come sopra meglio specificato.

Saranno acquisiti i soli dati personali strettamente necessari e pertinenti al raggiungimento delle finalità di seguito indicate, nel rispetto del principio di minimizzazione di cui all'art. 5, comma 1, lett. c) GDPR.
I dati acquisiti saranno trattati secondo i principi di correttezza, liceità e trasparenza di cui all'art. 5, comma 1, lett. a) GDPR.

FINALITÀ E BASI GIURIDICHE DEL TRATTAMENTO
Il Titolare tratterà i dati personali suindicati al fine di:

1. gestire e di dare diligente seguito alle segnalazioni ricevute, ivi incluse le attività di accertamento ed indagini interne legate alla verifica delle condotte oggetto di segnalazione e l'instaurazione di procedimenti, anche disciplinari, nei limiti di quanto richiesto dalle norme applicabili. Inoltre, i dati personali potranno essere trattati per dare seguito a richieste da parte dell'autorità amministrativa o giudiziaria competente e, più in generale, dei soggetti pubblici nel rispetto delle formalità di legge. I dati saranno trattati, altresì, per prevenire e contrastare efficacemente comportamenti fraudolenti e condotte illecite o irregolari e di supportare l'effettiva applicazione e l'operatività del Modello di Organizzazione e Gestione ex d.lgs. 231/2001.

Pertanto, la base giuridica che giustifica la liceità del trattamento è rappresentata dalla necessità di adempiere ad obblighi di legge e di eseguire compiti di interesse pubblico cui è sottoposto il Titolare del trattamento e disposizioni di Autorità legittimate dalla legge (art. 6, par. 1, lett. c) ed e); art. 9, par. 2, lett. g); art. 10 del GDPR).

2. Soddisfare esigenze di controllo interno del Titolare e di monitoraggio dei rischi aziendali, nonché assicurare l'ottimizzazione e l'efficientamento dei processi gestionali aziendali e amministrativi interni; accertare, esercitare o difendere un diritto o un interesse legittimo del Titolare in ogni sede competente a garanzia dell'esercizio del diritto di difesa ex art. 24 della Costituzione; gestire la sicurezza informatica e tutelare il patrimonio e la sicurezza dei dati, l'assistenza degli utenti e la manutenzione dei sistemi di sicurezza e protezione perimetrale dei log di traffico riguardanti le connessioni alla piattaforma di *whistleblowing* registrati sui sistemi aziendali.

Pertanto, la base giuridica che giustifica la liceità del trattamento è rappresentata dalla necessità di perseguire un legittimo interesse del Titolare o di terzi (art. 6, par. 1, lett. f) del GDPR).

Qualora il Segnalante decida di effettuare una segnalazione "in forma confidenziale", ossia nominativa, e/o decida di utilizzare i canali alternativi alla piattaforma Whistleblower Software Aps scegliendo come mezzo di comunicazione l'invio di una e-mail, la consegna a mano di una segnalazione scritta in modalità cartaceo oppure l'interlocuzione orale con il soggetto preposto alla ricezione delle segnalazioni, il trattamento dei dati identificativi el Segnalante è legittimato dalla volontà dello stesso che li ha resi noti ai destinatari della comunicazione per fini di tutela d'interesse pubblico.

Nel caso in cui sia necessario rivelare l'identità della persona segnalante e/o qualsiasi altra informazione dalla quale possa evincersi, anche indirettamente, l'identità dell'interessato a persone diverse da quelle deputate alla ricezione e gestione delle segnalazioni, per garantire la difesa dell'incolpato la base giuridica è rappresentata dal consenso espresso della stessa persona segnalante.

MODALITA' DI TRATTAMENTO

In relazione alle indicate finalità, il trattamento dei dati personali avverrà da parte risorse debitamente autorizzate ed istruite, prevalentemente con modalità informatiche, mediante l'apposita Piattaforma di segnalazione, secondo quanto descritto nella Procedura Whistleblowing, con logiche strettamente correlate alle finalità stesse e, comunque, adottando misure tecniche e organizzative tali da garantire un livello di sicurezza adeguato a garantire la riservatezza dei Segnalanti e di eventuali altri soggetti coinvolti e la confidenzialità delle informazioni presenti all'interno delle segnalazioni, prevenendo il rischio di divulgazione non autorizzata dei dati o l'accesso, in modo accidentale o illegale, agli stessi.

DESTINATARI E AMBITO DI COMUNICAZIONE DEI DATI

I dati personali suindicati saranno trattati per conto del Titolare, al fine di consentire la gestione delle segnalazioni, da parte del soggetto nominato quale Destinatario delle segnalazioni, autorizzato a: i) gestire le segnalazioni, ii) effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto della segnalazione, iii) adottare gli eventuali provvedimenti. In particolare, sulla base dei ruoli e delle mansioni lavorative espletate, il trattamento dei dati personali avverrà ad opera di soggetti specificamente istruiti e autorizzati a compiere operazioni di trattamento e preposti alla gestione della segnalazione.

Il fornitore della Piattaforma informatica opera quale Responsabile del trattamento debitamente nominato *ex* art. 28 del GDPR.

Nell'ambito di un procedimento disciplinare l'identità della persona segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni o, comunque, autorizzate, ove la contestazione sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Tuttavia, qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona Segnalante alla rivelazione della propria identità.

Nei casi in cui sia tecnicamente impossibile escludere la registrazione o l'anonimizzazione dei log, la loro eventuale consultazione potrà avvenire solo ed esclusivamente da parte dei soggetti tecnici autorizzati solo ed esclusivamente per finalità di risoluzione di incidenti informatici; l'iter prevede che il DPO sia informato rispetto a tale circostanza.

NATURA OBBLIGATORIA DEL CONFERIMENTO E CONSEGUENZA DI EVENTUALI RIFIUTI

Al fine di effettuare una segnalazione, il conferimento di dati personali è facoltativo e dipende dalla modalità di segnalazione scelta dal soggetto segnalante fra quelle indicate dalla Società; tuttavia, se conferiti, in taluni casi può rendersi necessario un loro utilizzo da parte del personale autorizzato per il perseguimento delle finalità già espresse. Il mancato conferimento dei dati necessari a dare seguito alla segnalazione impedirà l'esecuzione delle attività.

TRASFERIMENTO DATI ALL'ESTERO

Il Titolare del trattamento non trasferisce i dati personali in Paesi terzi e tutti i dati sono localizzati su server in Europa. Nel caso in cui si rendesse necessario un trasferimento di dati extra UE, la Società verificherà che i fornitori prestino garanzie adeguate, così come previsto dall'art. 46 GDPR, e provvederà ad aggiornare la presente informativa.

TEMPI DI CONSERVAZIONE DEI DATI

I dati personali raccolti saranno conservati per il tempo strettamente necessario ad espletare le finalità già indicate nei precedenti paragrafi e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della segnalazione, salvo il caso in cui si renda necessario in virtù di obblighi previsti dalla legge (ad esempio, il caso in cui sia in corso un procedimento giudiziario o disciplinare, fino alla conclusione dello stesso).

Il Titolare, giunto tale termine, provvederà alla cancellazione dei dati personali.

DIRITTI DELL'INTERESSATO

Il Titolare informa gli Interessati che, in via generale e previa prova della propria identità, possono esercitare – ove ne ricorrano i presupposti – i diritti di cui agli artt. 15 e ss. del GDPR, in particolare: i) diritto di accesso; ii) diritto di rettifica; iii) diritto alla cancellazione; iv) diritto di limitazione di trattamento; v) diritto alla portabilità dei dati; vi) diritto di

opposizione; vii) diritto di non essere sottoposto a processo decisionale automatizzato. L'esercizio dei diritti può avvenire contattando il Titolare attraverso l'invio di una richiesta all'indirizzo e-mail privacy@tdt.it.
Per ogni informazione in relazione alla presente informativa e nel caso in cui si riscontrino violazioni della normativa sulla protezione dei dati personali è possibile contattare il DPO all'indirizzo dpo@tdt.it.
Gli interessati hanno, inoltre, diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali, Piazza Venezia, 11 – 00187 – Roma tramite modulistica disponibile al seguente link www.garanteprivacy.it/diritti/come-agire-per-tutelare-i-tuoi-dati-personali/reclamo.

Nel caso di specie, tuttavia, in base a quanto previsto dall'art. 2-undecies e 2-duodecies del d.lgs. 196/2003 "Codice Privacy", il Titolare si riserva la facoltà di limitare o ritardare l'esercizio di tali diritti, nei limiti di quanto stabilito dalle disposizioni di legge applicabili, in particolare laddove sussista il rischio che possa derivare un pregiudizio effettivo, concreto e non altrimenti giustificato alla riservatezza dell'identità del Segnalante e che si possa compromettere la capacità di verificare efficacemente la fondatezza della segnalazione o di raccogliere prove necessarie.
In particolare, l'esercizio di tali diritti:

- Sarà possibile conformemente alle disposizioni di legge o di regolamento che regolano il settore (tra cui il d.lgs. 231/2001 e ss.mm.ii.);
- Potrà essere ritardato, limitato o escluso previa comunicazione motivata all'interessato, a meno che la comunicazione possa compromettere le finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare la riservatezza dell'identità del Segnalante.

Ultimo aggiornamento: Marzo 2024