D.LGS. 24/2023

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

Questo documento contiene le informazioni che il titolare del trattamento deve obbligatoriamente fornire agli interessati i cui dati personali sono coinvolti nella gestione delle segnalazioni ricevute in base alla normativa sul whistleblowing.

1 – Titolare del trattamento e informazioni di contatto

Il titolare del trattamento è Dahua Technology Italy S.R.L.U. in persona del legale rappresentante pro tempore.
La sede legale è in Via Cesare Cantu', 8/10 20092 Cinisello Balsamo (MI).
La PEC è **videotrend@twtcert.it.**
La mail per le comunicazioni relative al d.lgs. 24/2023 **ESCLUSE LE SEGNALAZIONI** è wb.italy@dahuatech.com.

2 - Base giuridica, finalità e modalità del trattamento

2.1 – Base giuridica

Il trattamento dei dati personali comunicati dal segnalante tramite la piattaforma di gestione delle segnalazioni interne è basato sull'adempimento a obblighi di legge e in particolare:
- D.lgs. 24/2023 per quanto riguarda gli accertamenti necessari a verificare la fondatezza della segnalazione;
- D.lgs. 231/01 per quanto riguarda gli accertamenti necessari a rispettare il modello organizzativo;
- L. 300/70 per quanto riguarda le contestazioni disciplinari.

2.2 – Finalità del trattamento

I trattamenti connessi alle segnalazioni interne sono finalizzati a:
- adempimento di obblighi di legge;
- tutela del diritto dell'azienda;

2.3 – Modalità di trattamento

I trattamenti sono eseguiti essenzialmente in modalità elettronica e dematerializzata, tramite una piattaforma di gestione delle segnalazioni gestita tecnicamente da un responsabile contrattualizzato ai sensi dell'articolo 28 del GDPR.

3 – Responsabile del trattamento

Limitatamente alla memorizzazione dei dati in forma cifrata e non accessibile e alla raggiungibilità della piattaforma per le segnalazioni interne il responsabile è ISWEB S.p.a. con sede legale in Via L. Cadorna 31 - 67051 Avezzano (AQ), PEC dpo@pec.isweb.it.
In base all'articolo 38 del GDPR al responsabile del trattamento è stato chiesto, fra l'altro, di:
- garantire il rispetto delle misure di sicurezza certificate ACN dichiarate in sede di acquisto del servizio;
- localizzare permanentemente i dati oggetto di trattamento in Italia o comunque all'interno della UE o in un Paese per il quale la Commissione europea ha adottato una decisione di adeguatezza;
- utilizzare esclusivamente personale adeguatamente formato dal punto di vista tecnico e organizzativo;
- cooperare con il titolare, per quanto di sua competenza, nel fornire riscontro alle richieste degli interessati

4 – Categorie di destinatari

Le categorie di dati personali dei destinatari sono quelle indicate dalle interfacce della piattaforma di gestione delle segnalazioni interne che corrispondono al tracciato record del database.

5 – Durata e finalità della conservazione

I dati personali sono conservati per una durata non inferiore al termine di prescrizione (statute of limitation) relativo ai reati oggetto della segnalazione e/o a quelli commessi dal segnalante.
La durata della conservazione è definita per consentire al titolare di agire o difendersi in giudizio, per cooperare con le autorità inquirenti nell'ambito di indagini penali, per controdedurre in procedimenti amministrativi e/o attivati da autorità indipendenti.

6 – Obbligatorietà del conferimento e non necessità del consenso
Il titolare non accetta segnalazioni anonime dunque il conferimento dei dati personali da parte del segnalante è una condizione necessaria per attivare il procedimento di segnalazione.
I trattamenti connessi alle basi giuridiche e alle finalità dichiarate non richiedono il consenso dell'interessato-segnalante.

7 - Diritti dell'interessato e procedura per il loro esercizio
7.1 – Diritti dell'interessato
L'interessato-segnalante ha il diritto di:
- chiedere l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento nel caso i trattamenti siano eccedenti rispetto alle basi giuridiche e alle finalità dichiarate
- ottenere copia dei dati personali comunicati al titolare;
- revocare in qualsiasi momento il consenso al trattamento dei propri dati personali, senza tuttavia che questo possa impedire l'utilizzo di quelli già conferiti e che devono essere comunicati a enti ed autorità pubbliche (ad esempio: magistratura inquirente, autorità indipendenti);
- proporre reclamo all'Autorità garante per la protezione dei dati personali secondo le procedure indicate sul sito www.garanteprivacy.it

7.2 – Procedura per l'esercizio dei diritti dell'interessato
L'interessato può esercitare i propri diritti inviando la richiesta via PEC della quale è diretto intestatario alla PEC indicata nell'articolo 1 di questa informativa.
La richiesta di esercizio dei diritti deve:
- essere firmata digitalmente con firma elettronica qualificata a norma di legge, per garantire l'identità del segnalante ed evitare di dover trattare anche i dati di un documento di identità:
- se avviene tramite un delegato, essere firmata digitalmente, con firma elettronica qualificata a norma di legge, sia dal delegante sia dal delegato;
- indicare espressamente se la risposta deve essere fornita al delegato oppure all'interessato.
Il titolare, salve necessità di accertamenti che possono richiedere più tempo e che saranno comunicate, risponderà entro trenta giorni dal ricevimento della richiesta.

8 – Ambito di comunicazione e diffusione
I dati personali comunicati tramite la piattaforma di gestione delle segnalazioni interne non sono diffusi e potranno essere comunicati esclusivamente ad enti ed autorità pubbliche in forza di un provvedimento, ove ricorrano gli estremi giuridici ad organismi di controllo (organismo di vigilanza 231, collegio sindacale), a periti, consulenti e avvocati per la gestione di contenziosi attivi e passivi anche stragiudiziali e nei limiti stabiliti dalla legge.

9 – Misure di sicurezza
Il titolare ha adottato misure di sicurezza tecniche e organizzative a protezione dei dati personali del segnalante che includono, fra le altre, l'utilizzo di responsabili esterni che forniscono adeguate garanzie di sicurezza, ricorso a personale interno adeguatamente competente e vincolato da obblighi di riservatezza, supporto indipendente per quanto attiene alla sussistenza dei requisiti legali per la comunicazione dell'identità del segnalante.
Nello specifico, sono state adottate anche le seguenti misure di sicurezza:

9.1 - Confidenzialità

La piattaforma di gestione delle segnalazioni memorizza i dati in forma cifrata.
La chiave di decifrazione è nella sola disponibilità del gestore delle segnalazioni interne.
Il responsabile esterno non ha alcuna possibilità di decifrare le informazioni memorizzate nella piattaforma.
La connessione con la piattaforma di gestione delle segnalazioni interne avviene tramite protocolli sicuri.
Il gestore delle segnalazioni tratta i dati personali delle segnalazioni esclusivamente tramite la piattaforma, evitando di memorizzarli localmente e/o di inserirli o di farvi riferimento nel corso delle attività di accertamento.

9.2 – Disponibilità

I dati personali memorizzati nella piattaforma di gestione delle segnalazioni esterne sono permanentemente accessibili ai soli aventi diritto (segnalante e gestore della segnalazione) tramite accesso a reti di comunicazione elettronica.
Il ripristino della disponibilità della piattaforma e dei dati personali è regolato dai livelli di servizio negoziati con il responsabile esterno.

9.3 – Integrità

L'integrità dei dati personali è realizzata grazie all'implementazione delle misure di sicurezza di cui alla certificazione ACN e in particolare alla possibilità di ripristinarli in caso di perdita o corruzione.

10 – Valutazione di impatto ai sensi dell'articolo 35 GDPR

10.1 - Rischi per i diritti e le libertà fondamentali del segnalante

Il rischio principale cui è esposto il segnalante è la rivelazione non autorizzata o in violazione degli obblighi legali della propria identità.
Astrattamente, questo lo espone al rischio di atti ritorsivi, intimidazioni, minacce, violenze, azioni giudiziarie strumentalmente proposte.

10.2 – Livello di rischio per i diritti e le libertà fondamentali del segnalante

In caso di rivelazione non autorizzata o in violazione di obblighi legali dell'identità del segnalante, il livello di rischio per i diritti e le libertà fondamentali del segnalante è molto alto.

10.3 – Valutazione dell'efficacia delle misure di sicurezza adottate

In relazione alla perdita di confidenzialità dell'identità del segnalante, le misure di sicurezza adottate dal titolare impediscono:

- che soggetti diversi dal segnalante e dal gestore della segnalazione possano accedere all'identità del segnalante nel corso delle attività di accertamento;
- che soggetti terzi (es.: gestore tecnico della piattaforma di segnalazione interna) possano accedere a qualsiasi titolo in chiaro ai dati memorizzati nella piattaforma per la segnalazion interna;
- in caso di esfiltrazione dei dati (es.: a seguito di attacco tramite ransomware) che terzi possano scoprire l'identità del segnalante;
- che la comunicazione con la piattaforma di gestione della segnalazione interna avvenga tramite protocolli insicuri e/o terminali non adeguatamente protetti.

Le misure in questione sono oggetto di revisione periodica circa la loro effettiva operatività ed efficienza e, ove necessario, sono adeguate e/o integrate.

10.4 – Valutazione di adeguatezza

Alla luce di quanto precede, i trattamenti necessari all'adempimento degli obblighi di cui al D.lgs. 24/2023 sono eseguiti con modalità tecniche e organizzative che gestiscono adeguatamente il livello di rischio di perdita di confidenzialità dell'identità del segnalante.