Intelligenza Organizzativa

Valutazione di impatto sulla protezione dei dati
Guida per i titolari del trattamento dei dati che utilizzano Whistleblowing Intelligente

Ai sensi del Regolamento generale sulla protezione dei dati (GDPR), i titolari del trattamento dei dati sono tenuti a preparare una valutazione d'impatto sulla protezione dei dati (DPIA) per il trattamento di operazioni che "potrebbero comportare un rischio elevato per i diritti e le libertà delle persone fisiche".

Il decreto legislativo del 10 marzo 2023, n.24 *Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, 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.* prevede espressamente all'art. 13 c.6 l'obbligo per il Titolare di definire "il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018."

Contenuto di una DPIA

L'articolo 35, paragrafo 7, del GDPR impone che una valutazione dell'impatto sulla protezione dei dati specifichi le finalità del trattamento e una descrizione sistematica del trattamento previsto. Una descrizione sistematica di una DPIA completa può includere fattori quali i tipi di dati elaborati, la durata della conservazione dei dati, gli scopi e la base legale del trattamento, la posizione e il trasferimento dei dati e le terze parti che possono avere accesso ai dati

La DPIA deve inoltre includere:

- Una valutazione della necessità e della proporzionalità delle operazioni di trattamento in relazione alle finalità;
- Una valutazione dei rischi per i diritti e le libertà delle persone fisiche;
- Le misure previste per affrontare i rischi, tra cui misure di sicurezza, e meccanismi

per garantire la protezione dei dati personali e dimostrare il rispetto del regolamento sul trattamento dei dati, tenendo conto dei diritti e degli interessi legittimi degli interessati e di altre persone interessate.

La tabella seguente contiene informazioni su Whistleblowing Intelligente rilevanti per ognuno di questi elementi.
I titolari del trattamento dei dati devono prendere in considerazione i dettagli forniti nella tabella, insieme a tutti gli altri fattori rilevanti, nel contesto dell'utilizzo specifico del sistema Whistleblowing Intelligente, al fine di elaborare la loro valutazione di impatto.

Finalità del trattamento	**Gli scopi dell'elaborazione dei dati utilizzati dalla piattaforma Whistleblowing Intelligente sono determinati dal titolare del trattamento dei dati che la configura e utilizza.** **Come specificato dall'atto di nomina nei confronti di Tecnolink quale Responsabile del trattamento, Tecnolink elabora i dati inseriti nella piattaforma al solo e unico scopo di fornire al cliente i servizi online richiesti.** **Tecnolink non utilizzerà i dati dei clienti o le informazioni da essi derivanti a scopi di profilazione, pubblicitari o simili.** **Tecnolink elabora i dati personali solo per fornire ai clienti i servizi online inclusi gli scopi compatibili con la fornitura di tali servizi, ad esempio: personalizzazione, sicurezza, prevenzione di frodi e malware, risoluzione dei problemi e miglioramento.**
Categorie di dati personali trattati	**Sono raccolti i seguenti dati personali dei Segnalanti (dipendenti dell'ente o equiparati):** • **Nome e Cognome** • **Luogo e data di nascita** • **Datore di lavoro** • **Posizione/Ruolo lavorativo** • **indirizzo di posta elettronica** • **Codice Fiscale** **Nel modulo di segnalazione, il segnalante potrebbe riportare dati personali non predeterminabili riferiti a persone segnalate.** **In riferimento al Responsabile della Prevenzione della corruzione ed eventuali collaboratori autorizzati, oltre ai**

	dati già indicati, sono raccolti i seguenti dati: • indirizzo ip • dati di log I sistemi informatici e le procedure software preposte al funzionamento di Whistleblowing Intelligente acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Si tratta di informazioni che non sono raccolte per essere associate a persone identificate, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche e per controllare il corretto funzionamento della piattaforma e vengono cancellati immediatamente dopo l'elaborazione.
Conservazione dei dati	I dati personali sono conservati per un periodo di 5 anni, la durata massima consentita dalle disposizioni di legge in merito alla conservazione delle segnalazioni di condotte illecite
Ubicazione e trasferimento dei dati personali	i dati sono ubicati in West Europe (Netherlands). Eventuali trasferimenti saranno regolamentati come da atto di nomina Responsabile trattamento dati
Condivisione dei dati con terze parti	Tecnolink condivide i dati con terze parti che agiscono come sub processori (come definito nel GDPR) per supportare funzioni come il supporto tecnico, la manutenzione dei servizi e altre operazioni utili al corretto funzionamento della piattaforma. Tutti i sub processori a cui Tecnolink trasferisce i dati dei clienti, avranno stipulato contratti scritti che non sono meno protettivi rispetto a quanto stabilito nell'atto di nomina di Tecnolink come responsabile del trattamento adottato dal cliente. Tutti i sub processori di terze parti con cui vengono condivisi i dati dei clienti sono inclusi nell'elenco Sotto Processore dell'atto di nomina Responsabile del trattamento
Diritti dei soggetti interessati	Tecnolink mette a disposizione del cliente/titolare del trattamento, i dati personali dei suoi interessati e la capacità di soddisfare le richieste degli interessati quando questi esercitano i propri diritti ai sensi del

	GDPR. Tecnolink lo fa in modo coerente con la funzionalità del prodotto e con il suo ruolo di responsabile del trattamento dei dati. Se riceviamo una richiesta da parte dell'interessato di un cliente per l'esercizio di uno o più dei suoi diritti ai sensi del GDPR, reindirizziamo tale interessato a presentare la richiesta direttamente al titolare del trattamento dei dati.
Valutazione della necessità e proporzionalità delle operazioni di trattamento in relazione agli scopi	**Il trattamento di dati personali è necessario al fine di adempiere ad un obbligo di legge a cui è tenuto il Titolare del Trattamento.** **Per quanto riguarda il trattamento effettuato da Tecnolink, tale trattamento è necessario ed è limitato al solo fine di fornire i servizi al titolare del trattamento dei dati.**
Valutazione dei rischi per i diritti e le libertà del soggetto dei dati	**I rischi principali per i diritti e le libertà degli interessati derivanti dall'uso Whistleblowing Intelligente dipenderanno da come e in quale contesto il titolare del trattamento dei dati configura e usa la piattaforma.** **Tecnolink adotta e fa adottare ai suoi sub processori tutte le misure necessarie a ridurre al minimo il rischio del trattamento per gli interessati.** **Tuttavia, come sempre in questi casi, i dati personali trattenuti in Whistleblowing Intelligente potrebbero essere a rischio di accesso non autorizzato o divulgazione involontaria.** **Tecnolink non partecipa con il suo personale e non è coinvolta direttamente nelle operazioni di trattamento di dati ma si assicura periodicamente che le misure adottate dai suoi sub processori per affrontare tali rischi siano adeguate.** **Il sub processore Interzen è certificato ISO 27001, lo standard internazionale della sicurezza delle informazioni** **https://www.zenshare.it/2023/03/24/interzen-ottiene-la-certificazione-iso-27001/** **Le misure adottate da Microsoft per affrontare tali rischi sono illustrate nelle Condizioni del prodotto**
Le misure previste per affrontare i rischi, comprese le misure di sicurezza e i meccanismi	**Tecnolink adotta (e ne verifica l'adozione da parte dei sub processori) misure tecniche e organizzative adeguate e ragionevoli per tutelare i dati personali che elabora.**

per garantire la protezione dei dati personali e per dimostrare la conformità al GDPR, tenendo conto dei diritti e degli interessi legittimi dell'interessato e di altre persone	**Tecnolink e i suoi sub processori adottano complessivamente le seguenti misure:** • **si accerta che chiunque agisca sotto la propria autorità ed abbia accesso a dati personali, non tratti tali dati se non è stato istruito in tal senso dal responsabile stesso e vincolato contrattualmente (o ex lege) alla riservatezza/segreto** • **applica le misure minime di sicurezza ict per le pubbliche amministrazioni individuate dall AGID** • **applica misure tecniche di crittografia dei dati personali, dei documenti e del DB** • **garantisce la riservatezza e l'integrità adottando strumenti e tecnologie di accesso mediante sistemi di autenticazione forte** • **adotta mezzi che permettono di garantire la continuità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento** • **adotta mezzi che permettono di garantire la capacità di ripristinare la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico]** • **adotta delle misure tecniche per la gestione dei log a norma di legge** • **archivia i dati in un paese dell'Unione Europea** • **modalità' di conservazione dei dati, conservazione digitale** **L'insieme degli aspetti tecnici delle misure di sicurezza adottate, sono descritte in dettaglio nell'allegato 1 del presente documento**
Ulteriori informazioni utili	**Ulteriori informazioni utili alla predisposizione della DPIA sono acquisibili consultando i seguenti documenti:** **Modello Nomina Responsabile trattamento dati personali** **Modello Informativa Privacy Whistleblowing Intelligente** **Modello Atto Organizzativo WHistleblowing** **Descrizione tecnica e funzionale WHistleblowing Intelligente**

Allegato 1

CARATTERISTICHE DELL'INFRASTRUTTURA E SICUREZZA APPLICATIVA

1° LIVELLO – SISTEMI ESTERNI DI PREVENZIONE	
Scansione online delle vulnerabilità	Nessus® Essentials: soluzione per la rilevazione delle vulnerabilità di Tenable®, Inc. Nel 2021 Tenable è stato un Software Vendor di Gartner rappresentativo della Vulnerability Assessment.

2° LIVELLO – INFRASTRUTTURA I.T. DEL CLOUD SERVICE PROVIDER	
Service Provider	Microsoft Azure.
Tipologia di servizio cloud	Public Cloud
Certificazioni del cloud service provider	Consulta la documentazione di conformità di Microsoft Azure.
Localizzazione dei data center utilizzati	West Europe (Netherlands)

Livelli di sicurezza adottati dal service provider	**Operazioni eseguite da Microsoft per proteggere l'infrastruttura di Azure.**
Ridondanza dei dati del service provider	**Archiviazione con ridondanza di zona (Zone Redundancy Storage, ZRS): replica i dati archiviati in Azure in modalità sincrona su tre aree disponibili interne all'area primaria (primary region).**

3° LIVELLO – INFRASTRUTTURA I.T.	
Firewall	**PfSense®, firewall riconosciuto come uno dei più potenti, sicuri ed affidabili.**
Back-up	**Procedura di back-up delle Virtual Machine:** ● **1. Frequenza: ogni 4 ore.** ● **2. Modalità di archiviazione: ridondanza geografica GRS (GEO-REDUNDANT-STORAGE). Copia dei dati in modo sincrono tre volte all'interno di un'unica posizione fisica nell'area primaria usando l'archiviazione con ridondanza locale. Copia quindi i dati in modo asincrono in un'unica posizione fisica nell'area secondaria. All'interno dell'area secondaria i dati vengono copiati in modo sincrono tre volte usando l'archiviazione con ridondanza locale.** ● **3. Area Primaria: West Europe (Netherlands).** ● **4. Area Secondaria : North Europe (Ireland).** ● **5. Retention Backup: 15 giorni.**
disaster recovery	**Procedura di Disaster Recovery delle Virtual Machine:** **1. Modalità: Cross Region Restore.** **2. Ridondanza: geografica (Geo-Redundancy Storage, GRS). Replica dei dati archiviati in Azure in modalità sincrona su una località fisica differente (regione secondaria).** **3. Localizzazione del data center utilizzato per il Disaster recovery: North Europe (Ireland).**

	RTO (Recovery Time Objective, il tempo necessario per il ripristino del sistema): 2 giorni lavorativi (tempo minimo)
	RPO (Recovery Point Objective, quantità massima di dati - espressa in ore - che l'azienda perde a seguito del verificarsi di un evento disastroso, poiché non rientrati nella normale procedura ciclica di back-up): 4 ore (tempo massimo)

4° LIVELLO – COMPONENTI SOFTWARE	
Sistema operativo	**Antivirus Microsoft Forefront**
Server virtuale	**L’accesso ai server virtuali avviene mediante una VPN ed utilizzando un profilo utente dimensionato strettamente in base alle necessità di monitoraggio e manutenzione.**

5° LIVELLO – CODICE APPLICATIVO	
Sicurezza informatica del produttore	Nell'ambito del processo di qualificazione del Cloud Marketplace ACN, il produttore ha validato i propri livelli di gestione della riservatezza e della sicurezza dei dati della soluzione Whistleblowing Intelligente presso lo STAR Registry (Security, Trust, Assurance, and Risk) della Cloud Security Alliance. Visualizza la scheda di qualificazione del Marketplace ACN Cloud Visualizza la scheda di Whistleblowing intelligente su Cloud Security Alliance Visualizza la scheda del produttore su Cloud Security Alliance
Sistema di autenticazione	Sistema proprietario. È il sistema che vincola la password di accesso del singolo utente Interfacciamento con sistemi esterni. Possibilità di demandare la gestione dell'accesso utenti mediante procedura di Single Sign On con altri sistemi: SPID (Sistema Pubblico di Identità Digitale)
IP filtering	Utenti collegati. Possibilità di visualizzare tutti gli utenti autenticati (non i Segnalanti) sulla piattaforma Whistleblowing Intelligente con i seguenti dati: cognome, nome, ruolo, indirizzo IP, ultimo accesso effettuato.

6° LIVELLO – DATI E DOCUMENTI DELLA PIATTAFORMA WHISTLEBLOWING INTELLIGENTE	
Criptaggio database e documenti	**1. Database. Chiave di criptazione dati a sua volta criptata mediante un algoritmo per un ulteriore livello di sicurezza. Il dato resta criptato nel database e la sua decrittazione avviene solo quando viene visualizzato.** **2. Documenti. Criptazione e decriptazione mediante chiave privata.**
Protocollo HTTPS	**L'HyperText Transfer Protocol Secure (over Secure Socket Layer) è un protocollo per la comunicazione su Internet che protegge integrità e riservatezza dei dati scambiati tra la piattaforma e l'hardware (PC, tablet, smartphone) dell'utente che vi accede. Certificato SSL erogato da Network Solutions LLC.**