AZIENDA TERRITORIALE PER L'EDILIZIA RESIDENZIALE DELLA PROVINCIA DI BELLUNO

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

A norma di quanto stabilito dall'art. 25 del Regolamento UE 679/2016 (GDPR)

Tipologie di trattamento: Whistleblowing

Scopo ambito di applicazione

La valutazione d'impatto sulla protezione dei dati consiste in un'auto-valutazione aziendale, come prevista dall'art. 35 del Regolamento (UE) 2016/679 (GDPR).

La DPIA è uno strumento rilevante per il principio di *accountability, in quanto serve al Titolare per adottare misure appropriate per assicurare la conformità del trattamento di dati personali ai principi stabiliti dal GDPR.*

Il Titolare è obbligato ad eseguire la DPIA ogni qual volta sia in presenza di trattamenti di dati personali che possano presentare rischi elevati per i diritti e le libertà delle persone fisiche (interessati) così da determinare le misure organizzative e tecniche adeguate ad indirizzare i rischi, con riferimento ad una specifica attività aziendale.

L'attività di valutazione è strumentale all'implementazione di idonee misure di mitigazione dei rischi con riferimento a quelli che a norma dell'art. 35 del GDPR riguardano dati che presentano un rischio elevato per le libertà e i diritti dei soggetti a cui tali dati si riferiscono.

Il Ruolo del Whistleblowing è:

- Strumento di prevenzione degli illeciti
- Manifestazione di un diritto umano (libertà di espressione)

Tipologie di trattamento oggetto della valutazione

Considerati i principi del GDPR, che impongono al Titolare del trattamento una valutazione di impatto qualora il trattamento possa presentare un rischio elevato, per ATER Belluno la valutazione di impatto si incentra sul trattamento correlato alle eventuali segnalazioni di illeciti (c.d. Whistleblowing).

Il whistleblower è la persona che segnala, divulga ovvero denuncia all'Autorità giudiziaria o contabile, violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'ente, di cui è venuta a conoscenza nel contesto lavorativo.

L'ATER di Belluno si è dotata di un sistema interno per le segnalazioni, accessibile dal sito istituzional.e La piattaforma è gestita Whistleblowing Solutions Impresa Sociale S.r.l. (WBS) con sede a Milano in Viale Aretusa 34. Ai sensi dell'Art. 28 del GDPR, Ater ha nominato detto soggetto quale Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679 (GDPR).

La natura del processo sensibile

L'ATER tratta i dati personali dei soggetti "informatori", quali:

dati forniti dal segnalante al momento della registrazione nella piattaforma Whisteblowing.it

altri dati personali che siano strettamente pertinenti allo svolgimento delle descritte attività (dati contenuti nelle segnalazioni).

La normativa di riferimento:

- L. 190/2012, per la prima volte introduce la regolamentazione del whistleblowing nell'ambito della PA; prevista la tutela per il lavoratore che segnali un illecito, proteggendolo contro le eventuali ritorsioni;
- D.Lgs. 231/2001, introduce l'obbligo per gli Enti, le Società pubbliche e private con modello organizzativo 231 di istituire almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- L. 179/2017, inserisce la disciplina del whistleblowing nell'ordinamento italiano, rafforzando il contrasto alla corruzione attraverso il divieto di provvedimenti negativi nei confronti di chi segnala e la tutela della riservatezza dell'identità;
- Direttiva UE 2019/1937 sul Whistleblowing, pubblicata il 16 dicembre 2019. Tutti gli stati dell'UE sono chiamati a recepire le disposizioni, nel loro ordinamento, entro due anni.
- D Lgs. 10 marzo 2023 n. 24, pubblicato in GURI S.G. n. 63 del 15 marzo 2023. Il provvedimento è entrato in vigore il 30 marzo 2023.

In base alla vigente normativa, tutte le Amministrazioni/Enti/Società alle quali si applicano le disposizioni, devono:

- istituire un canale informatico di segnalazione interno che garantisca la riservatezza dell'identità del whistleblower tramite crittografia dei dati, progettato secondo i principi della privacy by design e by default in conformità al GDPR;
- informare i whistleblower di aver ricevuto della segnalazione entro 7 giorni dall'invio, e fornire riscontro entro 3 mesi dalla data di ricevimento, o 3 mesi e 7 giorni in caso di mancato avviso di ricezione.
- mettere a disposizione informazioni chiare sulle procedure da seguire per effettuare una segnalazione, inserendole sia nel canale informatico che sul proprio sito internet.
- garantire la riservatezza dell'identità del segnalante, del contenuto della segnalazione e della relativa documentazione.

I whistleblower sono protetti dalle azioni ritorsive specificate nell'art. 19, tra cui il licenziamento, la mancata promozione, le note di merito e la riduzione dello stipendio. La normativa prevede un sistema di sanzioni in caso di violazioni.

Ai sensi dell'Art. 12 del D.Lgs n. 24 del 10 marzo 2023:

Obbligo di riservatezza

1. Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

2. L'identita' della persona segnalante e qualsiasi altra informazione da cui può' evincersi, direttamente o indirettamente, tale identità' non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

3. Nell'ambito del procedimento penale, l'identità' della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale.

4. Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità della persona segnalante non può' essere rivelata fino alla chiusura della fase istruttoria.

5. Nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa.

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.

6. E' dato avviso alla persona segnalante mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati, nella ipotesi di cui al comma 5, secondo periodo, nonché nelle procedure di segnalazione interna ed esterna di cui al presente capo quando la rivelazione della identità della persona segnalante e delle informazioni di cui al comma 2 è indispensabile anche ai fini della difesa della persona coinvolta.

7. I soggetti del settore pubblico e del settore privato, l'ANAC, nonché le autorità amministrative cui l'ANAC trasmette le segnalazioni esterne di loro competenza, tutelano l'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione nel rispetto delle medesime garanzie previste in favore della persona segnalante.

8. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, nonché dagli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33.

9. Ferma la previsione dei commi da 1 a 8, nelle procedure di segnalazione interna ed esterna di cui al presente capo, la persona coinvolta può essere sentita, ovvero, su sua richiesta, è sentita, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

Il contesto di trattamento

Il contesto del trattamento consiste nell'acquisizione dei dati del segnalante e gestire le informazioni contenute nella segnalazione.

La natura del contesto si inserisce nell'ambito di Diritti Costituzionalmente tutelati:

- Art. 21 Costituzione Italiana – libertà di espressione (tutelata anche da Articolo 11 - Libertà di espressione e d'informazione – Carta dei Diritti fondamentali dell'Unione Europea - Gazzetta ufficiale dell'Unione europea C 303/17 - 14.12.2007;

- Art. 3 Costituzione Italiana - Principio di eguaglianza

- Art. 4 Costituzione Italiana - Diritto al Lavoro (La Repubblica riconosce a tutti i cittadini il diritto al lavoro e promuove le condizioni che rendano effettivo questo diritto. Ogni cittadino ha il dovere di svolgere, secondo le proprie possibilità e la propria scelta, un'attività o una funzione che concorra al progresso materiale o spirituale della società)

- Art. 97, comma 1, della Costituzione, sotto la rubrica: "La Pubblica Amministrazione", recita: "I pubblici uffici sono organizzati secondo disposizioni di legge in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione". La norma (ri)afferma, dunque, un principio fondamentale – sorto con la nascita degli stati democratici e presente in tutti gli ordinamenti moderni - che concepisce l'amministrazione pubblica come soggetto che deve perseguire, esclusivamente e nel modo migliore, gli interessi dei cittadini; donde la facoltà loro riconosciuta di agire contro di essa qualora i suoi atti risultino contrari a loro situazioni soggettive.

Le finalità del trattamento sono correlate agli obblighi di legge previsti dalla L. 179/2017 e D.Lgs. 24 del 10 marzo 2023.

I dati trattati da ATER derivano da quanto presente, e caricato dall'interessato, nella piattaforma Segnalazioni.net.

I dati possono riguardare nome, indirizzo email, documento di riconoscimento, contenuti delle segnalazioni. I dati personali del segnalante non sono direttamente visualizzabili nella segnalazione.

Proposta di interventi finalizzati a ridurre il rischio

I dati personali oggetto di trattamento sono pertinenti e limitati a quanto indicato nella finalità del trattamento (c.d. principio di minimizzazione dei dati).

Gli stessi dati possono essere detenuti oltre che dal personale interno, anche da soggetti pubblici a cui la comunicazione avviene in forza di obblighi di legge, da soggetti terzi (persone fisiche o giuridiche) che svolgono servizi di verifica della conformità normativa di ATER (primo fra tutti Organismo di vigilanza, istituito ai sensi del D. Lgs. n.231/2001), da soggetti che svolgono attività di verifica relativamente ai sistemi di gestione certificati applicati da ATER (es. l'Organismo che certifica il sistema di gestione o degli standard di qualificazione), da soggetti a cui la comunicazione è necessaria per la gestione del rapporto contrattuale, a personale informatico (interno od esterno) in modo limitato a quanto strettamente necessario.

I dati sono trasmessi solo per necessità correlate alla vigente normativa in materia di Whistleblowing (ovvero alle norme da essa richiamate).

Valutazione dell'impatto

Al fine di valutare l'impatto sui diritti e sulle libertà fondamentali delle persone fisiche, derivanti dalla possibile perdita di sicurezza dei dati personali, ATER Belluno ha ritenuto necessario valutare separatamente l'impatto considerando l'ambito della *RISERVATEZZA* poi l'ambito dell'*INTEGRITA'* dei dati e infine della *DISPONIBILITA' DEI DATI*.

ATER Belluno, ha considerato quattro livelli di impatto, conformemente a quanto indicato nel Manuale sulla sicurezza nel trattamento dei dati personali redatto a cura dell'Agenzia Europea per la sicurezza cibernetica (ENISA). Nella tabella sotto riportata, sono riportate le risultanze dell'analisi.

Ambito	*Domanda*	*Valutazione*
1) Riservatezza	Quale impatto in termini di conseguenze negative, può avere sui diritti dell'interessato la divulgazione non autorizzata dei suoi dati personali conferiti ad ATER?	o Basso o Medio o **Alto** ☑ o Molto Alto
2) Integrità	Quale impatto, in termini di conseguenze negative, può avere sull'interessatol'alterazione non autorizzata dei suoi dati personali conferiti ad ATER?	o Basso o Medio o **Alto** ☑ o Molto Alto
3) Disponibilità dei dati	Quale impatto sui diritti dell'interessato, in termini di conseguenze negative, può avere la distruzione, la perdita, la criptazione non autorizzata, dei suoi dati personali conferiti ad ATER?	o Basso o Medio o **Alto** ☑ o Molto Alto

Il più alto di questi livelli è considerato come il risultato finale della valutazione dell'impatto.

Livello di impatto	*Descrizione*
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (ad esempio: necessità per gli interessati di dedicare altro tempo per inoltrare nuovamente i dati eventualmente smarritida ATER).
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, impossibilità temporanea di accedere ai servizi aziendali).
Alto ☑	**Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà.**
Molto Alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (danni fisici o psicologici a lungo termine, incapacità lavorative).

Attese le valutazioni di cui sopra, si ritiene di attribuire alle attività di assegnazione, sottoscrizione del contratto relativo a un alloggio di ERP, il livello **alto** di valutazione di impatto.

Definizione delle minacce possibili e valutazione delle probabilità che si verifichino.

Per individuare le minacce correlate al contesto complessivo del trattamento dei dati personali e valutare la probabilità del loro accadimento, l'ATER di Belluno ha considerato quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati, vale a dire:

a) Risorse di rete e tecniche (hardware e software);

b) Processi/procedure relativi all'operazione di trattamento dei dati;

c) Diverse parti e persone coinvolte nel trattamento;

d) Settore di operatività e scala del trattamento.

A) RISORSE TECNICHE DI RETE

Domande	*Spiegazione*	*Risposte*
Quale parte del trattamentodei dati personali viene eseguita tramite Internet?	Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte degli aggressori esterni online, soprattutto quando il servizio è disponibile a tutti gli utenti di Internet.	I dati del segnalante sono acquisiti tramite piattaforma Whistleblowing PA che ha recepito le indicazioni rese dal Garante per la protezione dei dati personali in merito alle caratteristiche tecniche che deve avere l'applicativo, al fine di assicurare la non identificabilità dei segnalanti a partire dall'indirizzo IP **[1]. Le segnalazioni sono gestite anche tramite un canale di segnalazione analogico, che prevede l'inoltro di una lettera al Responsabile della prevenzione della corruzione e della trasparenza. La missiva, recante il modulo per la segnalazione, deve indicare all'esterno la dicitura "Riservata al Responsabile della prevenzione della corruzione e della trasparenza".**
E' possibile fornire l'accesso ad un sistema interno di trattamento di dati personali tramite Internet?	Quando l'accesso ad un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterna aumenta. Allo stesso modo aumenta anche la probabilità di abuso dei dati da parte degli utenti. Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione/amministrazione remota del sistema IT.	I dati del segnalante sono acquisiti tramite piattaforma Segnalazioni.net di DigitalPA Srl, collegato al sistema di posta elettronica Microsoft365. L'accesso al sistema di posta elettronica è consentito da remoto all'RPCT e al personale incaricato per il supporto alle attività in capo all'RPCT (2 INCARICATI). **[1]. Per quanto riguarda le segnalazioni in modalità analogica, queste sono indirizzate direttamente dal mandante al Responsabile della prevenzione della corruzione e della trasparenza.**
Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (ed ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunatamente configurati, tali connessioni possono consentire l'accesso ai dati personali a più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate all'accesso).	I dati del segnalante sono acquisiti tramite piattaforma Segnalazioni.net di DigitalPA Srl, collegato al sistema di posta elettronica Microsoft365. L'accesso al sistema di posta elettronica è consentito da remoto a personale autorizzato. Sono configurati differenti livelli di autorizzazione alla consultazione dei dati a seconda del ruolo rivestito in azienda e le specifiche mansioni svolte. **[1]**

Persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza.	Le Segnalazioni non permettono di identificare il segnalante e sono conservate solo con modalità digitale. La sala Ced è chiusa a chiave e accessibile solo agli addetti [1]. La documentazione relativa ad ogni singola segnalazione, sia in formato cartaceo che elettronico, va archiviata e conservata in maniera adeguata a cura del RPTC . La documentazione cartacea viene conservata per un periodo di 5 anni in un armadio chiuso a chiave nella stanza del RPTC.
Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	Componenti hardware e software mal progettate, implementate e/o mantenute possono comportaregravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione e raggiungere determinati livelli di resilienza.	Il sistema di trattamento è implementato e mantenuto dalla Ditta DigitalPA Srl a regola d'arte, con la supervisione, per gli opportuni adeguamenti alla normativa, del DPO. **[1]**

B) PROCESSI RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

Domande	***Spiegazione***	***Risposte***
I ruoli e le responsabilità relative al trattamento dei dati personali sono vaghi o non chiaramente definiti?	Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza comprensiva del sistema.	Sono state predisposte e consegnate, a tutti i dipendenti, le istruzioni agli addetti al trattamento ai sensi del Regolamento UE 679/2016 sul trattamento dei dati personali. Nelle istruzioni sono state specificati gli ambiti di trattamento dell'addetto e le finalità del trattamento. **[1]**
L'uso accettabile della rete, del sistema e delle risorse fisiche all'internodell'organizzazione èambiguo o non chiaramente definito?	Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgereminacce alla sicurezza a causa di incomprensioni o di un uso improrio, intenzionaledel sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali.	L'Azienda si è dotata degli Allegati 2-3 al Registro dei Trattamenti (art. 30 del Regolamento UE), aggiornati di recente, disciplinando anche le modalità di accesso alle risorse informatiche aziendali ed alla rete internet. **[1]**
I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi.	I dipendenti non sono autorizzati a collegare dispositivi informatici personali ai PC aziendali, come rinnovato anche nelle istruzioni agli addetti al trattamento recentemente consegnate **[1]**
I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di retepotenzialmente insicuri (es. Reti Wi - Fi aperte), sia uso non autorizzato di queste informazioni.	No. Per il trattamento dei dati oggetto della presente l'accesso è limitato all'RPCT e al personale incaricato per il supporto alle attività in capo all'RPCT (2 INCARICATI. **[1]**
Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file del registro?	La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/procedure e risorse, con conseguente abuso di dati personali.	Sul piano tecnico la piattaforma Segnalazioni.net non tiene traccia dei log di collegamento da parte dei segnalanti; e ciò per evitare che il segnalante diventi identificabile. **[1]**

C) PERSONE COINVOLTE NEL TRATTAMENTO DE DATI PERSONALI

Domande	*Spiegazione*	*Risposte*
Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	Quando l'accesso dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso acausa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.	Relativamente alle attività in esame, i dati personali degli utenti sono trattati dall'RPCT e dal personale incaricato per il supporto alle attività in capo all'RPCT (2 INCARICATI) e nei casi previsti, dall'OdV. **[2]**
Quale parte dell'operazione di trattamento dei dati è eseguita da unappaltatore/terza parte (responsabile del trattamento)?	Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. E' importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un altolivello di controllo.	Il sistema di trattamento è implementato e mantenuto dalla Ditta Digitalpa Srl a regola d'arte, con la supervisione, per gli opportuni adeguamenti alla normativa, del DPO. La Ditta è stata nominata, con apposito atto, Responsabile del Trattamento ex art. 28 GDPR **[1]**
Gli obblighi delleparti/persone coinvolte nel trattamento dei dati personali sono ambigui o chiaramente definiti?	Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo.	Sono state predisposte e consegnate, a tutti i dipendenti, le istruzioni agli addetti al trattamento ai sensi del Regolamento UE 679/2016 sul trattamento dei dati personali. Nelle istruzioni sono state specificati gli ambiti di trattamento dell'addetto e le finalità del trattamento.**[1]**
Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.	E' stata effettuata formazione a tutti i dipendenti nel corso del 2021; sono in programma, a breve, corsi di formazione in materia di Privacy, Anticorruzione e Modello 231/2001. **[1]**
Le persone/le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e/o distruggere in modo sicuro i dati personali?	Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I documenti cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazioni e riutilizzo non autorizzati.	Gli armadi utilizzati per la conservazione delle pratiche sono muniti di chiave. L'Azienda utilizza dispositivi per la distruzione dei documenti e ha impartito al personale apposite istruzioni per la distruzione dei documenti **[2]**

D) SETTORE DI OPERATIVITÀ E SCALA DEL TRATTAMENTO

Domande	*Spiegazione*	*Risposte*
ATER ritiene che il suo settore di attività sia esposto ad attacchi informatici?	Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell'organizzazione del Titolare del trattamento, questa è un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile.	Ater non rientra tra I settori a rischio sicurezza. **[1]**
ATER ha subito attacchi informatici o a altri tipi di violazioni della sicurezza negli ultimi due anni?	Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caos, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.	Ad oggi l'Azienda non è mai stata oggetto di attacchi informatici. **[1]**
ATER ha ricevuto notifiche e/o reclami riguardo alla sicurezza del sistema informatico (utilizzando per il trattamento dei dati personali) nell'ultimo anno?	Bug di sicurezza/vulnerabilità possono essere sfruttai per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alla vulnerabilità della sicurezza che potrebbero influire sui sistemi e servizi menzionati sopra.	L'Azienda non ha ricevuto notifiche e/o reclami riguardo alla sicurezzadel sistema informatico. **[1]**
Un'operazione di elaborazione riguarda un grande volume di individui e/o dati personali?	Il tipo ed il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati).	No. **[1]**
Esistono *best practice* di sicurezza specifica per il tuo settore di operatività che non sono state adeguatamente seguite?	Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni e ai rischi del particolare settore. La mancanza di conformità con le *best practice* pertinenti potrebbe essere un indicatore si scarsa gestione della sicurezza.	No **[1]**

Una volta calcolate le probabilità delle 4 aree, si determina il punteggio con la tabella sottostante.

A) Valutazione della probabilità di occorrenza delle minacce per area

Area di valutazione	Probabilità	
	Livello	Punteggio
Rete e risorse tecniche	Basso	1☑
	Medio	2
	Alto	3
Processi/Procedure relativi al trattamento dei dati personali	Basso	1☑
	Medio	2
	Alto	3
Parti/Persone Coinvolte nel trattamento dei dati personali	Basso	1☑
	Medio	2
	Alto	3
Parti/Persone Coinvolte nel trattamento dei dati personali	Basso	1☑
	Medio	2
	Alto	3
Settore di operatività dei dati personali	Basso	1☑
	Medio	2
	Alto	3

Infine, con la tabella sotto riportata si può ottenere il livello della probabilità della minaccia.

B) Valutazione della probabilità di occorrenza di una minaccia

Somma globale della probabilità di occorrenza diuna minaccia	Livello di probabilità delle minacce
5-6	Basso ☑
7-8	Medio
9-12	Alto

La probabilità di occorrenza finale della minaccia viene calcolata dopo aver sommato i 4 punteggiottenuti nella Tabella (A) e associato il risultato complessivo alle somme globali della Tabella (B).

Attese le valutazioni suesposte, si ritiene di considerare le attività in esame a bassa probabilità dioccorrenza di una minaccia.

Calcolo del rischio

Dopo aver valutato l'impatto (alto) dell'operazione di trattamento dei dati personali e la probabilità (bassa) di accadimento della minaccia, è possibile effettuare la valutazione finale del rischio.

L'incrocio dei due valori di *impatto* e *probabilità* ci fornisce l'indicazione del valore del rischiorisultante.

		IMPATTO		
		BASSO	MEDIO	ALTO / MOLTO ALTO ☑
PROBABILITA'	BASSA ☑	Rischio basso	Rischio medio	Rischio alto ☑
	MEDIA	Rischio basso	Rischio medio	Rischio alto
	ALTA	Rischio medio	Rischio alto	Rischio alto

Come desumibile dalla tabella sopra riportata, pur avendo valutato come **bassa la probabilità** dioccorrenza, la valutazione **alta dell'impatto** attribuito determina una valutazione complessiva di Rischio alto connessa alle attività oggetto della presente indagine.

Misure di sicurezza

In allegato alla presente relazione, il documento redatto da WhistleblowingPa a supporto del Titolare dell'Azienda da usare per la valutazione di impatto sulla protezione dei dati relativi alle segnalazioni di illeciti, aggiornato all'11.01.2023, in cui indica dettagliatamente:

- descrizione della piattaforma di whistleblowing;
- descrizione e analisi del contesto;
- valutazione in merito ai trattamenti;
- indicazioni delle misure aggiuntive di sicurezza informatica.

Conclusioni

L'attività di gestione delle segnalazioni di illecito è definita nel "*Regolamento del Whisteblowing*"; conformemente alle precisazioni contenute nel D.lgs 24/2023.

L'Azienda si è dotata per il processo di segnalazione, di una piattaforma ad hoc disponibile all'indirizzo web: https://aterbl.whistleblowing.it/.Tale servizio informatizzato garantisce la riservatezza dei dati del segnalante, che sono conservati solo ai fini della segnalazione e con le cautele descritte nel regolamento summenzionato.

Pure considerato come alto il rischio potenzialmente connesso al trattamento di dati degli istanti in relazione alle attività di trattamento, si ritengono adeguate le misure di mitigazione del rischio adottate in Azienda, la cui scrupolosa osservanza determina un rischio residuo accettabile.