DPIA-Canale di segnalazione interna

General Data Protection Regulation - Regolamento (UE) 2016/679

TITOLARE
DEL TRATTAMENTO DEI DATI

Comune di Fiesso d'Artico

Indirizzo	p.zza Marconi n. 16, 30032, Fiesso d'Artico (VE)
telefono	041/5137145
e-mail	protocollo@comune.fiessodartico.ve.it
PEC	comunefiessodartico.ve@legalmail.it

Comune di Fiesso d'Artico	ALTO	
PROBABILITA'	MEDIO	6
IMPATTO	MOLTO ALTO	9

IMPATTO SUI DIRITTI DEGLI INTERESSATI	**MOLTO ALTO**	**9**
Perdita di DISPONIBILITA' *Quale potrebbe essere il probabile impatto sugli interessati di una distruzione o perdita non autorizzate di dati personali?*	Impatto significativo	2
Descrizione	L'impatto sarebbe alto in relazione ad una perdita o distruzione dei dati dei segnalanti o di quelli conte	
Perdita di INTEGRITA' *Quale sarebbe il probabile impatto sugli interessati di un'alterazione non autorizzata di dati personali?*	Impatto severo	3
Descrizione	L'impatto sarebbe alto in relazione sia ai dati dei Responsabili delle segnalazioni, perché potrebbe non	
Perdita di RISERVATEZZA *Quale sarebbe il probabile impatto sugli interessati di una divulgazione non autorizzata di dati personali?*	Impatto critico, compreso il fermo operativo dell'organizzazione	4
Descrizione	L'impatto sarebbe molto alto in considerazione del fatto che la legge stessa in materia di whistleblowing dichiara di importanza fondamentale la tutela della riservatezza degli	

IMPATTO SISTEMI INFORMATIVI (RETE E RISORSE TECNOLOGICHE)	**MEDIO**	**2**
QUALCHE PARTE DEL TRATTAMENTO DEI 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 di aggressori esterni online (ad esempio Denial of Service, SQL injection, attacchi Man-in-the-Middle), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet.*	SI', tuttavia la connessione di rete è protetta a tutti i livelli per limitare il rischio di intercettazioni delle trasmissioni di dati.	

E' POSSIBILE FORNIRE L'ACCESSO A UN SISTEMA INTERNO DI TRATTAMENTO DEI DATI PERSONALI TRAMITE INTERNET? (ad esempio per determinati utenti o gruppi di utenti) *Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT.*	SI'. L'accesso alla Piattaforma richiede una connessione a internet.
IL SISTEMA DI TRATTAMENTO DEI DATI PERSONALI E' INTERCONNESSO CON UN ALTRO SISTEMA O SERVIZIO IT ESTERNO O INTERNO (all'organizzazione)? *La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente 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 a tale accesso).*	NO
IL SISTEMA DI TRATTAMENTO DEI DATI PERSONALI E' PROGETTATO, IMPLEMENTATO O MANTENUTO SENZA SEGUIRE LE MIGLIORI PRASSI? *Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi 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 (ai rischi) e raggiungere determinati livelli di resilienza.*	NO. Si veda il Foglio "Misure".

LE 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 (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico).*	NO. La Piattaforma è accessibile solo a chi disponga delle necessarie credenziali, quindi all'RPCT, che le conserva personalmente e con diligenza. Per quanto riguarda l'accesso agli ambienti in cui si trovano i server fisici, questo viene impedito alle persone non autorizzate in forza delle policy di sicurezza certificate dal fornitore dei server e da quello della Piattaforma.	
IMPATTO PROCESSI/PROCEDURE COLLEGATE ALL'ELABORAZIONE DEI DATI	**MEDIO**	**2**
I RUOLI E LE RESPONSABILITA' RELATIVI AL TRATTAMENTO DEI DATI PERSONALI SONO VAGHI O NON CHIARAMENTE DEFINITI?	NO. Il Comune ha tra l'altro adottato una procedura interna specifica relativa alla gestione dei canali di segnalazione per il c.d. whistleblowing. Il Comune ha adottato	
L'USO ACCETTABILE DELLA RETE, DEL SISTEMA E DELLE RISORSE FISICHE ALL'INTERNO DELL'ORGANIZZAZIONE E' AMBIGUO O NON CHIARAMENTE DEFINITO?	NO	
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 rete potenzialmente insicuri (es. Reti Wi-Fi aperte), sia uso non autorizzato di queste informazioni.*	SI'. Un tanto è vero in riferimento ai trattamenti di dati relativi alla gestione delle segnalazioni di whistleblowing.	
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.*	SI'. Un tanto è vero in riferimento ai trattamenti di dati relativi alla gestione delle segnalazioni di whistleblowing. Nei dispositivi personali e nei browser utilizzati non possono tuttavia essere salvate le credenziali personali per l'accesso alla Piattaforma.	
LE ATTIVITA' DI ELABORAZIONE DEI DATI PERSONALI POSSONO ESSERE ESEGUITE SENZA LA CREAZIONE DI UN FILE DI 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.*	NO. La Piattaforma raccoglie log delle azioni svolte. I log sono cifrati e l'accesso agli stessi è consentito esclusivamente al Responsabile delle segnalazioni.	
IMPATTO PARTI/PERSONE COINVOLTE NELL'ELABORAZIONE DEI DATI	**BASSO**	**1**

IL TRATTAMENTO DEI DATI PERSONALI E' ESEGUITO DA UN NUMERO NON DEFINITO DI DIPENDENTI?	NO	
QUALCHE PARTE DELL'OPERAZIONE DI TRATTAMENTO DEI DATI E' ESEGUITA DA UN APPALTATORE/TERZA PARTE (RESPONSABILE DEL TRATTAMENTO)?	SI'	
GLI OBBLIGHI DELLE PARTI/PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI SONO AMBIGUI O NON CHIARAMENTE DEFINITI? *Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo.*	NO	
IL PERSONALE COINVOLTO NEL TRATTAMENTO DEI DATI PERSONALI NON HA FAMILIARITA' 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.*	NO. I dati personali raccolti mediante le segnalazioni o per la gestione delle stesse sono trattati, per conto del Titolare del trattamento, dall'RPCT.	
LE PERSONE/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 file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati.*	NO. L'archiviazione e la distruzione dei dati sono gestite quasi esclusivamente dal fornitore della Piattaforma, secondo le istruzioni impartite dal Titolare del trattamento. I dati personali raccolti mediante le segnalazioni o per la gestione delle stesse potrebbero essere archiviati e poi distrutti, sotto la responsabilità del Titolare del trattamento, solo da parte dell'RPCT, che è vincolato al rispetto delle procedure interne relative al c.d. whistleblowing adottate dal Comune.	
IMPATTO SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	**BASSO**	**1**
RITIENI CHE IL TUO SETTORE DI ATTIVITA' SIA ESPOSTO AGLI ATTACCHI INFORMATICI? *Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore*	SI'	
LA TUA ORGANIZZAZIONE HA SUBITO ATTACCHI INFORMATICI O ALTRI TIPI DI VIOLAZIONI DELLA SICUREZZA NEGLI ULTIMI DUE ANNI?	NO	

HAI RICEVUTO NOTIFICHE E/O RECLAMI RIGUARDO ALLA SICUREZZA DEL SISTEMA INFORMATICO (UTILIZZATO PER IL TRATTAMENTO DEI DATI PERSONALI) NELL'ULTIMO ANNO? *Bug di sicurezza / vulnerabilità possono essere sfruttati per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra.*	NO
IL TRATTAMENTO RIGUARDA UN GRANDE VOLUME DI INDIVIDUI E/O DATI PERSONALI? *Il tipo e 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
ESISTONO BEST PRACTICE DI SICUREZZA SPECIFICHE PER IL TUO SETTORE DI OPERATIVITA' 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 migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza.*	NO

Comune di Fiesso d'Artico

RISCHIO CALCOLATO		**ALTO**			
RISCHIO APPLICATO	**3**	**ALTO**	**STATUS**	**NOTE**	**IN CARICO A**

MISURE ORGANIZZATIVE

A. Politica di sicurezza e procedure per la protezione dei dati personali (A.5 Politica di sicurezza)

A1 L'organizzazione ha incluso la propria politica in merito al trattamento dei dati personali inerenti alle segnalazioni whistleblowing nella sua politica di sicurezza delle informazioni	1	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento. Il Comune ha adottato una procedura per il whistleblowing in cui viene trattata anche la sicurezza delle informazioni. Questa sarà tenuta in considerazione in sede di adozione della policy di sicurezza delle informazioni generale.
A2 La politica di sicurezza viene revisionata e rivista, se necessario, su base annuale	1	SI	ATTIVO	
A3M L'organizzazione possiede e rispetta una policy di sicurezza dedicata alla piattaforma informatica utilizzata come canale di segnalazione, separata per quanto riguarda il trattamento dei dati personali. La policy è approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate	2	SI	ATTIVO	
A4M La policy di sicurezza si riferisce almeno a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.	2	SI	ATTIVO	
A5M Esiste ed è mantenuto un inventario di policy / procedure specifiche relative alla sicurezza dei dati personali, basato sulla policy generale di sicurezza	2	SI	ATTIVO	
A6H Le policy di sicurezza vengono riviste e corrette, se necessario, su base semestrale.	3	SI	ATTIVO	

B. Ruoli e responsabilità (A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni)

B1 I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità con le politiche di sicurezza	1	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.

B2 In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'organizzazione ha una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento	1	SI	ATTIVO	
I soggetti autorizzati ad accedere ai dati contenuti nella Piattaforma in qualità di Responsabili delle segnalazioni sono autonomi, cioè soggetti imparziali ed indipendenti.	1	SI	ATTIVO	Si vedano le procedure relative al c.d. whistleblowing adottate dal Comune.
B3M E' stata effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.	2	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
B4 Il responsabile della sicurezza dovrebbe essere nominato formalmente (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.	3	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
B5H Compiti e responsabilità in conflitto (ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO) sono considerati separatamente per ridurre le ipotesi di modifiche non autorizzate o non intenzionali o un uso improprio di dati personali	3	SI	ATTIVO	
C. Politica di controllo degli accessi (A.9.1.1 Politica di controllo degli accessi)				
C1 I diritti specifici di controllo degli accessi sono assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati	1	SI	ATTIVO	
L'accesso ai dati contenuti nella Piattaforma è consentito solamente ai soggetti autorizzati alla gestione del canale di segnalazione e delle segnalazioni stesse.	1	SI	ATTIVO	Si vedano le procedure relative al c.d. whistleblowing adottate dal Comune.
C2M E' stata dettagliata e documentata una politica di controllo degli accessi. L'organizzazione ha determinato in questo documento le regole di controllo appropriate degli accessi, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nell'ambito dei processi e delle procedure	2	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
C3M E' stata chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi)	2	SI	ATTIVO	
C4 I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff	3	SI	ATTIVO	
D. Gestione risorse/asset (A.8 Asset management)				
D1 L'organizzazione dispone di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro include almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica).	1	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
D2 Definire la periodicità con cui il censimento delle risorse e degli apparati IT e il relativo registro vengono rivisti e aggiornati (almeno annuale)	1	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.

D3M I ruoli che hanno accesso a determinate risorse sono stati definiti e documentati nell'apposito registro	2	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
D4H Le risorse IT vengono riviste e aggiornate su base annuale	3	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
E. Gestione delle modifiche apportate alle risorse, agli apparati ed ai sistemi IT (A. 12.1 Procedure operative e responsabilità)				
E1 L'organizzazione si è assicurata che tutte le modifiche alle risorse, agli apparati ed al sistema IT sono registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Descrivere tempi e modalità di monitoraggio delle eventuali modifiche	1	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento (si veda il documento "Policy sulle misure di sicurezza-My Whistleblowing", adottato da
E2 Lo sviluppo software è eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, vengono utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, sono state previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	1	SI	ATTIVO	Il Titolare del trattamento non effettua attività di sviluppo software. La misura è garantita dal Responsabile del trattamento.
E3M E' prevista e applicata una policy interna che disciplina la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.	2	SI	ATTIVO	
F. Responsabili del trattamento (A.15 Rapporti con i fornitori)				
F1 Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.	1	SI	ATTIVO	Si veda nomina a Responsabile sottoscritta con il Fornitore della Piattaforma.
F2 Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.	1	SI	ATTIVO	Si veda nomina a Responsabile sottoscritta con il Fornitore della Piattaforma.
F3 Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.	1	SI	ATTIVO	Si veda nomina a Responsabile sottoscritta con il Fornitore della Piattaforma e documenti tecnici dallo stesso condivisi.
F4 L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.	2	SI	ATTIVO	Si veda nomina a Responsabile sottoscritta con il Fornitore della Piattaforma.

F5 I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.	3	SI	ATTIVO	Misura garantita dal Fornitore della Piattaforma.
G. Gestione degli incidenti / Violazione dei dati personali (Personal data breaches) (A.16 Gestione degli incidenti sulla sicurezza delle informazioni)				
G1 Nel Piano di Business Continuity è stato incluso un piano di risposta agli incidenti (Piano di Risposta agli Incidenti) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma. Nello specifico, il fornitore specifica che entrambi i server fisici su cui poggia la Piattaforma eseguono una macchina virtuale di Key Management System (KMS) per consentire continuità di servizio con immediato automatico riavvio dei sistemi senza intervento amministrativo anche in caso di totale fallimento di uno dei due server fisici componenti il cluster.
G2 Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) vengono segnalate immediatamente al Management competente secondo l'organizzazione interna. Sono in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.	1	SI	ATTIVO	La segnalazione delle violazioni è garantita dal Titolare del trattamento mediante l'adozione della procedura per la gestione delle violazioni di dati personali. Il Fornitore della Piattaforma garantisce l'adempimento di questa misura mediante sue procedure interne.
G3M Il piano di risposta degli incidenti (Piano di Risposta agli Incidenti) è documentato e comprende un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	2	SI	ATTIVO	
G4H Gli incidenti e le violazioni dei dati personali vengono registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione intraprese.	3	SI	ATTIVO	Il Titolare del trattamento tiene costantemente aggiornato il "Registro delle violazioni".
H. Business continuity (A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa)				
H1 L'organizzazione ha definito le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali)	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
H2M E' stato predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza) che include azioni chiare e assegnazione di ruoli.	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
H3M Il Piano di Business continuity definisce il livello di qualità del servizio garantito per i processi fondamentali dell'Ente che attengono alla sicurezza dei dati personali	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
H4M E' stato nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali (documentare)	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
H5H Indicare la struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT	3	SI	ATTIVO	Misura garantita dal Fornitore dei server mediante lo SLA.
I. Obblighi di confidenzialità imposti al personale (A.7 Sicurezza delle risorse umane)				

I1 L'organizzazione garantisce che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati e comunicati durante il processo di pre-assunzione e / o assunzione .	1	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
L'identità 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	1	SI	ATTIVO	Questa misura è garantita dal Fornitore della Piattaforma e dalle procedure interne adottate dal Titolare del trattamento.
Si tutela la riservatezza del segnalante anche quando la segnalazione perviene a personale diverso da quello autorizzato e competente a gestire le segnalazioni, al quale, comunque, le stesse vanno trasmesse senza ritardo	1	SI	ATTIVO	Questa misura è garantita dalle procedure interne adottate dal Titolare del trattamento.
E' tutelata la riservatezza del facilitatore che assiste il segnalante	1	SI	ATTIVO	Questa misura è garantita dal Fornitore della Piattaforma e dalle procedure interne adottate dal Titolare del trattamento.
E' tutelata la riservatezza anche delle persone differenti dal segnalato ma menzionate nella segnalazione, tramite il ricorso a strumenti di crittografia ove si utilizzino strumenti informatici.	1	SI	ATTIVO	Questa misura è garantita dal Fornitore della Piattaforma.
I2M Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento vengono invitati a visionare e concordare le policy di sicurezza dell'organizzazione e firmare reciproci accordi di riservatezza e di non divulgazione	2	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
I3H I dipendenti ad alto rischio sono vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale)	3	SI	ATTIVO	
J. Formazione (A.7.2.2 Consapevolezza della sicurezza delle informazioni, educazione e formazione)				
J1 L'organizzazione garantisce che tutti i dipendenti, lavoratori e persone autorizzate al trattamento sono adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali sono inoltre adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.	1	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
L'organizzazione garantisce che i Responsabili delle segnalazioni abbiano ricevuto regolare formazione sia in ambito protezione dei dati personali sia in relazione alla disciplina sulle segnalazioni ("cd. whistleblowing").	1	SI	ATTIVO	Si vedano le procedure relative al c.d. whistleblowing adottate dal Comune.
I dipendenti dell'Ente sono stati informati del fatto che, qualora ricevano erroneamente segnalazioni, le stesse dovranno essere trasmesse al soggetto interno competente, dandone contestuale notizia della trasmissione alla persona segnalante. Tutti i dipendenti sono in ogni caso vincolati, anche per legge, da specifici obblighi di riservatezza a tutela del segnalante.	1	SI	ATTIVO	Si vedano le procedure relative al c.d. whistleblowing adottate dal Comune.
J2M L'organizzazione dispone di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati	2	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.

J3H E' stato predisposto e viene eseguito su base annuale un piano di formazione con scopi e obiettivi definiti	3	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.

MISURE TECNICHE

K. Controllo degli accessi e autenticazione (A.9 Controllo degli accessi)

K1 E' stato implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema consente la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	1	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
K2 L'uso di account utente comuni (con credenziali di accesso condivise tra più utenti) è evitato. Nei casi in cui questo sia necessario, viene garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	1	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
K3 E' attivo un meccanismo di autenticazione che consente l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). E' utilizzata almeno una combinazione di nome utente / password. Le password rispettano un determinato (e configurabile) livello di complessità	1	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
K4 Il sistema di controllo degli accessi è in grado di rilevare e non consentire l'utilizzo di password che non rispettano un determinato (e configurabile) livello di complessità	1	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento. La Piattaforma viet altresì il riutilizzo di precedenti password.
K5 Dovrebbe essere definita e documentata una policy specifica per la password. La policy deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.	2	SI	ATTIVO	Misura implementata con riferimento sia all'organizzazione del Titolare del trattamento, sia all'organizzazione del Responsabile del trattamento.
K6M Le password degli utenti sono memorizzate in una forma "hash"	2	SI	ATTIVO	Misura garantita dal Fornitore della Piattaforma.
K7H L'autenticazione a due fattori (autenticazione forte) è implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.	3	SI	ATTIVO	Il sistema della Piattaforma implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238. Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.
K8H Ogni dispositivo è soggetto ad autenticazione endpoint per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete dell'Ente	3	SI	NON APPLICABILE	

L. Generazione di file di log e monitoraggio (A.12.4 Registrazione e monitoraggio)

L1 I file di log devono essere attivati in riferimento a ciascun sistema/applicazione utilizzati per il trattamento di dati personali. I file di log includono tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	1	SI	ATTIVO	Misura garantita dal Fornitore per quanto riguarda la Piattaforma e dal Titolare del trattamento nel caso in cui vengano utilizzati dispositivi del Comune. L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing.

Garantire il divieto di tracciamento dei canali di segnalazione. Nel caso in cui l'accesso alla Piattaforma avvenga dalla rete dati interna del Titolare del trattamento e sia mediato da dispositivi firewall o proxy, deve essere garantita la non tracciabilità del segnalante – sia sulla Piattaforma che negli apparati di rete eventualmente coinvolti nella trasmissione o monitoraggio delle comunicazioni - nel momento in cui viene stabilita la connessione a tali canali	1	SI	NON IMPLEMENTABILE	Se il segnalante accede alla Piattaforma tramite la rete internet del Comune, la sua attività può essere tracciata mediante log e questa misura di sicurezza non può essere garantita.
Garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione. Deve essere evitato il tracciamento di qualunque informazione che possa ricondurre	1	SI	ATTIVO	Misura garantita dal Fornitore per quanto riguarda la Piattaforma e dal Titolare del trattamento nel caso in cui vengano utilizzati dispositivi del Comune. Si rileva, in particolare, che tutte le operazioni effettuate sulle
L2 I file di log devono avere una marca temporale e devono essere adeguatamente protetti contro manomissioni e accessi non autorizzati. Gli orologi dei file di log devono essere sincronizzati ad un'unica fonte di misurazione del tempo	1	SI	ATTIVO	Misura garantita dal Fornitore per quanto riguarda la Piattaforma e dal Titolare del trattamento nel caso in cui vengano utilizzati dispositivi del Comune.
L3M Le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente, sono registrate dalla Piattaforma con file di log	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.
L4M Non deve esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di log della Piattaforma. L'accesso ai file di log deve a sua volta essere registrato in aggiunta al monitoraggio necessario per rilevare attività inusuali	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
L5M Un sistema di monitoraggio analizza i file log della Piattaforma, produce report sullo stato del sistema e notifica potenziali allarmi. Descrivere le modalità, la periodicità e la posizione fisica dei report.	2	SI	NON IMPLEMENTABILE	
M. Sicurezza di Server e Database (A. 12 Operations security)				
M1 I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
M2 I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR) .	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
La riservatezza della persona segnalante, del facilitatore, della persona coinvolta o comunque menzionata, del contenuto della segnalazione e della relativa documentazione è garantita da strumenti di crittografia.	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento. Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.

M3 Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.	2	SI	ATTIVO	Si veda misura precedente.
M4 Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma. Si veda misura precedente.
M5 Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
M6 Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.	3	SI	NON IMPLEMENTABILE	
N. Sicurezza delle Postazioni di lavoro (A. 14.1 Requisiti di sicurezza dei sistemi di informazione)				
N1 Gli utenti non sono in grado di disattivare o bypassare le impostazioni di sicurezza	1	SI	ATTIVO	
N2 Le applicazioni anti-virus e le firme di rilevamento sono configurate su base settimanale	1	SI	ATTIVO	Misura garantita sia dal fornitore della Piattaforma sia all'interno dell'organizzazione del Titolare del trattamento.
N3 Gli utenti non hanno i privilegi per installare o disattivare applicazioni software non autorizzate	1	SI	ATTIVO	Misura garantita dal Fornitore della Piattaforma.
N4 Il sistema attiva il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo (screensaver con password)	1	SI	ATTIVO	Misura garantita dal Fornitore della Piattaforma.
N5 Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo vengono installati regolarmente	1	SI	ATTIVO	Misura garantita dal Fornitore della Piattaforma.
N6 Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.	2	SI	ATTIVO	Misura garantita sia dal fornitore della Piattaforma, sia dal fornitore dei server, sia all'interno dell'organizzazione del Titolare del trattamento.
N7 Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).	3	SI	NON IMPLEMENTABILE	
N8 Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.	3	SI	NON IMPLEMENTABILE	
N9 La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.	3	SI	ATTIVO	Misura garantita dal Fornitore della Piattaforma.
O. Sicurezza della Rete e delle Infrastrutture di comunicazione Elettronica (A.13 Communications Security)				
O1 Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione è crittografata tramite protocolli crittografici (TLS / SSL).	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma. Nello specifico, ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+.

O2M L'accesso wireless al sistema IT è consentito solo a utenti e per processi specifici. Indicare i meccanismi di crittografia utilizzati per la protezione.	2	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
O3M In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Se è considerato necessario, specificare le motivazioni e documentare che viene eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.	2	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
O4M Il traffico da e verso il sistema IT è monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma. I flussi di dati vengono mediati da sistemi di firewall che permettono il transito solo dei dati necessari al funzionamento della Piattaforma.
O5M La connessione a Internet non è consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali	2	SI	NON IMPLEMENTABILE	
O6M La rete del sistema informatico è segregata dalle altre reti del Titolare/del Responsabile del trattamento dei dati	2	SI	NON IMPLEMENTABILE	
O7H L'accesso al sistema IT è eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC)	3	SI	NON IMPLEMENTABILE	
P. Back-up (A.12.3 Back-Up)		**SI**		
P1 Le procedure di backup e ripristino dei dati sono state definite, documentate e chiaramente collegate a ruoli e responsabilità	1	SI	ATTIVO	Backup gestiti dal Fornitore della Piattaforma e dal Subresponsabile Seeweb.
P2 Il livello di protezione fisica e ambientale dei backup è adeguato e coerente con gli standard applicati sui dati di origine (descrivere)	1	SI	ATTIVO	Backup gestiti dal Fornitore della Piattaforma e dal Subresponsabile Seeweb.
P3 L'esecuzione dei backup deve essere monitorata per garantirne la completezza.	1	SI	ATTIVO	Backup gestiti dal Fornitore della Piattaforma e dal Subresponsabile Seeweb.
P4 I backup completi devono essere eseguiti regolarmente.	1	SI	ATTIVO	Backup gestiti dal Fornitore della Piattaforma e dal Subresponsabile Seeweb. I sistemi della Piattaforma sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.
P5 I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.	2	SI	ATTIVO	Backup gestiti dal Fornitore della Piattaforma e dal Subresponsabile Seeweb.
P6M I backup incrementali sono eseguiti su base giornaliera	2	SI	ATTIVO	Backup gestiti dal Fornitore della Piattaforma e dal Subresponsabile Seeweb.
P7M Le copie del backup sono conservate in modo sicuro in luoghi diversi dalla sede dei dati originali	2	SI	ATTIVO	Backup gestiti dal Fornitore della Piattaforma e dal Subresponsabile Seeweb.
P8M In caso di utilizzo di un servizio di terze parti per l'archiviazione di backup, la copia è crittografata prima di essere trasmessa	2	SI	ATTIVO	Backup gestiti dal Fornitore della Piattaforma e dal Subresponsabile Seeweb.
P9H Le copie dei backup sono crittografate e archiviate in modo sicuro, anche offline	3	SI	NON IMPLEMENTABILE	
Q. Dispositivi mobili / portatili (A. 6.2 Dispositivi mobili e teleworking)				

Q1 Le procedure di gestione dei dispositivi mobili e portatili sono state definite. Sono state stabilite regole chiare per il loro corretto utilizzo.	1	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
Q2 I dispositivi mobili ai quali è consentito accedere al sistema informativo sono pre-registrati e pre-autorizzati	1	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
Q3 I dispositivi mobili sono soggetti agli stessi livelli delle procedure di controllo degli accessi delle altre apparecchiature terminali	1	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
Q4M I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili sono stati chiaramente definiti	2	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
Q5M L'organizzazione è in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso	2	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
Q6M I dispositivi mobili supportano la separazione dell'uso privato e lavorativo del dispositivo attraverso contenitori software sicuri	2	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
Q7M I dispositivi mobili vengono fisicamente protetti contro il furto quando non sono in uso	2	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
Q8H Per l'accesso ai dispositivi mobili è utilizzata l'autenticazione a due fattori (autenticazione forte)	3	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
Q9H I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati) sono crittografati	3	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.

R. Sicurezza del ciclo di vita delle applicazioni (A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto)

R1 Durante lo sviluppo del ciclo di vita vengono seguite le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti (documentare)	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
R2 Specifici requisiti di sicurezza sono stati definiti durante le prime fasi del ciclo di vita dello sviluppo	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.

R3 Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) sono adottate in analogia con i requisiti di sicurezza	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
R4 Dovrebbero essere seguiti standard e pratiche di codifica sicure.	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
R5 Durante lo sviluppo, test e convalida viene eseguita l'implementazione dei requisiti di sicurezza iniziali	1	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
R6M Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture vengono eseguiti da una terza parte certificata prima dell'adozione operativa (dettagliare). L'applicazione considerata non è adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto (documentare la verifica del raggiungimento del livello e il ruolo incaricato).	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma. L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review. A questi controlli si aggiunge la peer review indipendente.
R7M Devono essere eseguiti test periodici di penetrazione.	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
R8M Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.
R9M I patch software vengono testati e valutati prima di essere installati in un ambiente operativo (descrivere le modalità)	2	SI	ATTIVO	Misura garantita dal fornitore della Piattaforma.

S. Cancellazione/eliminazione dei dati (A. 8.3.2 Smaltimento di supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura)

S1 La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), è necessario eseguire la distruzione fisica.	1	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
S2 È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.	1	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.

S3 Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti.	2	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
S4 Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.	2	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
S5 Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.	3	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.
S6 Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file cartacei, il processo si dovrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento all'esterno dei dati personali.	3	SI	NON APPLICABILE	Questa misura non rileva per il trattamento concernente la gestione del canale di segnalazione.

T. Sicurezza fisica (A. 11 - Sicurezza fisica e ambientale)

T1 Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato	1	SI	ATTIVO	Misura garantita dal Responsabile e dai Subresponsabili del trattamento.
T2 Identificazione chiara, tramite mezzi appropriati, ad es. I badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbero essere stabiliti, a seconda dei casi.	2	SI	ATTIVO	Misura garantita dal Responsabile e dai Subresponsabili del trattamento.
T3 Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro	2	SI	ATTIVO	Misura garantita dal Responsabile e dai Subresponsabili del trattamento.
T4 I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.	2	SI	ATTIVO	Misura garantita dal Responsabile e dai Subresponsabili del trattamento. I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi,
T5 Se del caso, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato.	2	SI	ATTIVO	Misura garantita dal Responsabile e dai Subresponsabili del trattamento.
T6 Aree sicure non occupate devono essere chiuse fisicamente e periodicamente riviste.	2	SI	ATTIVO	Misura garantita dal Responsabile e dai Subresponsabili del trattamento.
T7 Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) dovrebbero essere attivati nella sala server.	2	SI	ATTIVO	Misura garantita dal Responsabile e dai Subresponsabili del trattamento.
T8 Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette.	2	SI	ATTIVO	Misura garantita dal Responsabile e dai Subresponsabili del trattamento.