Valutazione d'impatto sulla protezione dei dati

ex articolo 35 Regolamento UE n. 2016/679 (GDPR)

trattamento "Whistleblowing"

1. CONTESTO

1.1 PANORAMICA DEL TRATTAMENTO

Quale è il trattamento in considerazione?

Il trattamento oggetto di valutazione è denominato "**whistleblowing**" ed è conseguente all'esecuzione degli obblighi normativi previsti dal decreto legislativo 10 marzo 2023, n. 24 (il "*Decreto Whistleblowing*") di 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*". Il trattamento ha lo scopo di implementare e disciplinare un sistema di segnalazioni di irregolarità nell'ambito dell'attività svolta dalla Società.

La procedura per la presentazione e gestione delle segnalazioni prevede che la gestione del canale interno di segnalazione venga affidato a Forward Srl, società esterna di consulenza, indipendente e autonoma, in grado di offrire adeguate garanzie di riservatezza e protezione dei dati che opera in qualità di responsabile del trattamento ex art. 28 GDPR. Forward ha implementato, per conto della Società mediante la sottoscrizione di un contratto di servizi, il canale interno di segnalazione. Il gestore della segnalazione svolge la propria attività attenendosi a quanto previsto dalla Procedura per la presentazione e la gestione delle segnalazioni adottata formalmente dalla Società.

Tale canale interno di segnalazione viene reso mediante l'attivazione del canale online di whistleblowing (in seguito anche "canale" o "portale") fornita dalla società EQS Group Srl che opera in qualità di (sub)responsabile del trattamento ex art. 28 GDPR.

Per le misure tecniche e organizzative adottate dalla piattaforma si rimanda allo specifico allegato.

Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento: Dimensione Serramenti Srl.

Responsabile del trattamento: Forward Srl, in qualità di gestore della segnalazione (nel seguito anche "gestore").

(sub) Responsabile del trattamento: ISIgame Srls, in qualità di fornitore della piattaforma online di whistleblowing.

Incaricati/Autorizzati al trattamento: OdV.

Ci sono standard applicabili al trattamento?

Il trattamento segue i seguenti riferimenti normativi e di prassi:

- Direttiva (UE) n. 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (cd. direttiva Whistleblowing).
- Decreto Legislativo n. 24 del 2023 in attuazione della Direttiva (UE) n. 2019/1937.
- Linee guida relative alle procedure per la presentazione e gestione delle segnalazioni esterne, predisposte da A.N.AC. in attuazione del Decreto Legislativo n. 24 del 2023 (testo in consultazione 01.06.2023; testo approvato con Delibera n. 311 del 12 luglio 2023).

- Guida operativa per gli enti privati sulla nuova disciplina whistleblowing – Confindustria, Ottobre 2023.
- Documento di ricerca sulla Nuova disciplina del whistleblowing e impatto sul D.Lgs. n. 231/2001- Consiglio Nazionale dei Dottori Commercialisti e degli Esperti contabili e FNC, Ottobre 2023;
- Regolamento (UE) n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (General Data Protection Regulation, c.d. GDPR).
- Decreto Legislativo n. 196/2003, codice in materia di protezione dei dati personali (c.d. Codice privacy) e successive modifiche e integrazioni.
- Decreto Legislativo n. 231/2001 in ambito di responsabilità amministrativa degli enti, per alcune tipologie di reato, i c.d. reati 231.

1.2 DATI, PROCESSI E RISORSE DI SUPPORTO

Quali sono i dati trattati?

I dati personali che possono esser trattati, ove indicati dal segnalante nella segnalazione effettuata mediante il canale online, possono essere i seguenti:

Segnalazione anonima:

- dati del segnalato: (i) dati anagrafici; (ii) posizione lavorativa; (iii) relazione con il segnalante;
- dati di eventuali testimoni: (i) dati anagrafici; (ii) posizione lavorativa; (iii) relazione con il segnalante;

Segnalazione identificata: oltre ai dati di cui sopra relativi al segnalato e degli eventuali testimoni

- dati del segnalante: (i) dati anagrafici; (ii) dati di contatto; (iii) ruolo; (iv) ogni ulteriore dato che sia fornito volontariamente nell'ambito della segnalazione dal segnalante.

In linea generale, non è richiesta la comunicazione di alcuna categoria particolare di dati personali (quali, a titolo esemplificativo, informazioni sull'origine razziale e/o etnica, convinzioni religiose e/o ideologiche, appartenenza sindacale o orientamento sessuale). Tuttavia, tali categorie particolari di dati possono essere volontariamente comunicate nei campi a testo libero nel modulo di registrazione.

Nel caso in cui vengano indicate categorie particolari di dati ai sensi dell'articolo 9 GDPR, come pure dati relativi a condanne penali e reati ai sensi dell'articolo 10 GDPR, tali dati saranno utilizzati solo ove strettamente necessari per la gestione della denuncia, nel pieno rispetto dei principi di proporzionalità e necessità e, se ritenuti irrilevanti ai fini della segnalazione, non saranno oggetto di ulteriore trattamento.

I dati personali, eventualmente comunicati, saranno conservati, a cura del gestore della segnalazione, per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni dalla chiusura della segnalazione, decorsi i quali saranno cancellati, fatta salva l'eventuale instaurazione di un procedimento disciplinare e/o giudiziario per il quale troveranno rispettivamente applicazione le normative applicabili in ambito giudiziario.

I dati personali degli interessati potranno essere resi accessibili, portati a conoscenza di o comunicati ai seguenti soggetti:

- gestore della segnalazione, in qualità di responsabile del trattamento;

- l'Organismo di Vigilanza, solo per quanto concerne le segnalazioni che abbiano una rilevanza rispetto al D.Lgs. n. 231/2001;

- il soggetto incolpato nell'ambito della segnalazione ai fini della propria difesa, qualora ricorrano i presupposti previsti dal D.Lgs. 24/2023;

- il fornitore del servizio ricezione e conservazione delle segnalazioni, in qualità di responsabile del trattamento.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

1. Il segnalante si collega alla portale mediante il link reso accessibile dal sito internet della Società o comunicato in occasione della diffusione dell'apposita circolare interna.
2. Il segnalante sul portale decide se effettuare una segnalazione scritta, vocale o chiedere un incontro di persona.
3. Il segnalante sul portale decide se effettuare una segnalazione anonima o identificata rilasciando i suoi dati anagrafici e di contatto.
4. Il segnalante compila i campi facoltativi. rilascia le informazioni che ritiene necessarie e, prima dell'invio, sceglie la sua password personale per controllare lo stato della segnalazione.
5. Il segnalante al termine della segnalazione riceve un identificavo della segnalazione
6. Il gestore della segnalazione riceve via email un avviso che sul portale è stata inserita una nuova segnalazione.
7. Il gestore della segnalazione **entro sette giorni** si collega al portale e rilascia al segnalante l'avviso di ricevimento dalla presentazione della segnalazione stessa.
8. Il gestore valuta la procedibilità (sussistenza dei presupposti soggettivi e oggettivi per effettuare una segnalazione whistleblowing).
9. valuta l'ammissibilità come segnalazione whistleblowing.
10. Nel caso in cui la segnalazione risulti improcedibile o inammissibile, il gestore della segnalazione può procedere all'archiviazione, garantendo comunque la tracciabilità delle motivazioni a supporto.
11. Procede all'istruttoria e all'accertamento della segnalazione. Verificata la procedibilità e l'ammissibilità della segnalazione, il gestore avvia l'istruttoria interna sui fatti e sulle condotte segnalate al fine di valutarne la fondatezza.
12. Completata l'attività di accertamento, il gestore della segnalazione può:
    - archiviare la segnalazione perché infondata, motivandone le ragioni;
    - dichiarare fondata la segnalazione e rivolgersi agli organi/funzioni interne competenti per i relativi seguiti (es. il management aziendale, Direttore Generale, ufficio legale o risorse umane). Al gestore della segnalazione non compete alcuna valutazione in ordine alle responsabilità individuali e agli eventuali successivi provvedimenti o procedimenti conseguenti.
13. Il gestore fornisce un riscontro al segnalante, **entro tre mesi** dalla data di avviso di ricevimento o - in mancanza di tale avviso - entro tre mesi dalla data di scadenza del termine di sette giorni per tale avviso.
14. Le segnalazioni e la relativa documentazione sono conservate sul portale.

Quali sono le risorse di supporto ai dati?

I dati sono gestiti dal gestore della segnalazione, Forward Srl, mediante l'utilizzo della piattaforma online Global Leaks ISIgame.

2. Principi Fondamentali

2.1 PROPORZIONALITÀ E NECESSITÀ

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento è finalizzato esclusivamente alla gestione della segnalazione e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing.

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica su cui si si fonda il trattamento è l'adempimento di un obbligo di legge a cui è tenuto il titolare – art. 6, par. 1, lett. c) ed e) – GDPR).

Alcune fasi del trattamento possono richiedere il consenso del segnalante.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

In applicazione dell'art. 5, par. 1, lettera c) GDPR vengono trattati solamente le informazioni pertinenti, adeguate e limitate rispetto allo scopo per la quale vengono raccolte.

Il segnalante è tenuto a fornire tutti gli elementi utili a consentire ai soggetti competenti di procedere alle dovute e appropriate verifiche a riscontro della fondatezza dei fatti oggetto di segnalazione.

I dati sono esatti e aggiornati?

Il segnalatore può in qualsiasi momento aggiornare o rettificare le informazioni che ha trasmesso integrando la comunicazione già inviata o, in caso di perdita delle credenziali di accesso alla inbox, inoltrando una nuova segnalazione.

Il gestore della segnalazione inoltre si occupa della verifica della procedibilità e l'ammissibilità della segnalazione ricevuta

Qual è il periodo di conservazione dei dati?

Ai sensi dell'art. 14 del D.Lgs. 24 del 10 marzo 2023 le segnalazioni e la relativa documentazione sono conservate, a cura del gestore delle segnalazioni, per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, o fino a conclusione del procedimento giudiziale o disciplinare eventualmente conseguito nei confronti del segnalato o del segnalante, nel rispetto degli obblighi di riservatezza.

Si precisa inoltre che per le Segnalazioni non rilevanti e non trattabili si prevede la conservazione per un massimo di 12 mesi dal completamento dell'istruttoria dei fatti esposti.

2.2 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Come sono informati del trattamento gli interessati?

L'informativa ex art. 13 GDPR resa ai soggetti interessati è disponibile, prima di procedere al trattamento dei dati, mediante link accessibile sul sito internet del Titolare del trattamento nell'apposita sezione riferita al whistleblowing, sulla pagina principale del canale online di segnalazione e all'interno della sezione dedicata alla raccolta delle informazioni.

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso da parte del segnalatore si ottiene mediante il canale online di segnalazione.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Come indicato nell'informativa messa a disposizione gli interessati possono esercitare i loro diritti scrivendo attraverso il canale di segnalazione messo a disposizione, nei limiti di quanto previsto dall'articolo 2-undecies del D.Lgs. n. 196/2003.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Come indicato nell'informativa messa a disposizione gli interessati possono esercitare i loro diritti scrivendo attraverso il canale di segnalazione messo a disposizione, nei limiti di quanto previsto dall'articolo 2-undecies del D.Lgs. n. 196/2003.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Come indicato nell'informativa messa a disposizione gli interessati possono esercitare i loro diritti scrivendo attraverso il canale di segnalazione messo a disposizione, nei limiti di quanto previsto dall'articolo 2-undecies del D.Lgs. n. 196/2003.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi del gestore della segnalazione sono definiti e disciplinati con un apposito contratto a cui è presente anche la nomina a responsabile del trattamento ex art. 28 GDPR.

Il gestore della segnalazione si avvale di una software house per la fornitura della piattaforma online del canale di segnalazione. Tale software house, che presenta adeguati standard di sicurezza, è nominata responsabile del trattamento ex art. 28 GDPR.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati non vengono trasferiti in paesi extra-Ue.

3. RISCHI

3.1 MISURE ESISTENTI O PIANIFICATE

Crittografia

La piattaforma di whistleblowing attivata utilizza un protocollo di crittografia che garantisce la protezione dei dati inseriti.

Controllo degli accessi fisici

Per quanto riguarda il Data center:

- sistema di controllo elettronico degli ingressi fisici con registro
- recinzione perimetrale ad alta sicurezza attorno all'intero parco del data center
- distribuzione documentata delle chiavi ai dipendenti e ai clienti di colocation per i rack di colocation
- politiche per l'accompagnamento e la designazione degli ospiti nell'edificio
- personale del data center presente 24 ore su 24, 7 giorni su 7
- videosorveglianza agli ingressi e alle uscite;
- sistemi di interblocco delle porte di sicurezza e sale server
- per le persone esterne al personale (visitatori del data center), l'ingresso all'edificio è consentito solo in compagnia di un dipendente.

Controllo degli accessi logici

- Software antivirus per la posta in ingresso e in uscita
- Separazione degli account amministrativi e degli account cliente
- Firewall
- Regole e politica delle password (complessità, lunghezza, scadenza, lockout on failure)
- VPN per l'accesso remoto
- Assegnazione delle autorizzazioni secondo il principio della "necessità di sapere, necessità di operare”
- Linee guida documentate sulla protezione dei dati e sulla sicurezza informatica

Controllo di accesso ai dati

Le seguenti misure sono state implementate per garantire che i dati personali possano essere accessibili solo in conformità con le autorizzazioni assegnate. Inoltre, è garantito che i dati personali non possono essere elaborati senza autorizzazione, cioè non possono essere registrati, letti, copiati, modificati o cancellati senza autorizzazione.

- Unico utente amministrativo limitato al CISO
- Gestione dei diritti degli utenti da parte del CISO
- Registrazione degli accessi ai dati
- Identificazione e autenticazione degli utenti
- Regole di autorizzazione e di accesso centralizzate
- Crittografia dati laddove necessario

Controllo della separazione

Le seguenti misure sono state implementate per garantire che i dati raccolti per scopi diversi siano trattati separatamente.

- Autorizzazione per l'accesso ai dati
- Configurazioni software sicure
- Separazione logica e di sistema
- Crittografia
- Reti e sistemi isolati e separati

Backup

- Infrastruttura ridondante
- Backup regolari e criptati
- Archiviazione di backup off-site
- Controllo regolare dei backup per disponibilità, completezza e integrità

Anonimizzazione / pseudonimizzazione dei dati personali

Se necessario, le seguenti misure sono attuate per evitare che i dati personali siano attribuiti a una specifica persona interessata senza l'uso di informazioni aggiuntive.

- I dati personali devono essere cancellati o resi anonimi/pseudonimizzati dopo la scadenza del periodo di conservazione legale, se la cancellazione non è possibile.
- Funzioni per l'anonimizzazione / pseudonimizzazione dei dati.
- Nessuna registrazione dei dati degli indirizzi IP o di altri metadati dei segnalatori.
- Comunicazione sicura e, se desiderato, anonima con gli informatori.

.

Sistema di gestione della sicurezza delle informazioni

Il canale online di segnalazione implementa:

- Responsabile interno della sicurezza delle informazioni (CISO)
- Revisione regolare dell'efficacia delle misure tecniche di sicurezza

3.2 ACCESSO ILLEGITTIMO AI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

- Ritorsioni sul segnalante e altre persone coinvolte (es. colleghi di lavoro);
- impatti psicologici per diffusione del nominativo del segnalante;
- impatti sui diritti alla libertà del segnalante (es. telefonate, e- mail o altro di comunicazioni indesiderate);
- impatti psicologici sui soggetti interessati derivanti da una diffusione non autorizzata del contenuto della segnalazione che può essere non veritiera.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Attacco informatico al canale online di segnalazione;
- perdita di riservatezza da parte del gestore della segnalazione;
- perdita di riservatezza da parte dei soggetti interni che devono dare seguito alla segnalazione;
- erronea configurazione degli accessi logici al canale online di segnalazione.

Quali sono le fonti di rischio?

- Soggetti estranei all’organizzazione;

- gestore della segnalazione;
- soggetti interni all'organizzazione.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Controllo di accesso ai dati;
- sistema di gestione della sicurezza delle informazioni;
- crittografia;
- controllo degli accessi fisici;
- controllo degli accessi logici.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitato in quanto le misure di sicurezza informatica sono adeguate, come gestore della segnalazione è stata scelta una società esterna di consulenza, indipendente e autonoma ed in grado di offrire adeguate garanzie di riservatezza e protezione dei dati. I soggetti interni ricevono adeguate istruzioni su come trattare i dati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Sulla base delle misure in essere.

3.3 MODIFICHE INDESIDERATE DEI DATI

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

- Ritorsioni sul segnalante e altre persone coinvolte (es. colleghi di lavoro);
- impatti sui diritti alla libertà del segnalante (es. telefonate, e- mail o altro di comunicazioni indesiderate);
- impatti psicologici sui soggetti interessati derivanti da una diffusione non autorizzata del contenuto della segnalazione che può essere non veritiera.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Attacco informatico al canale online di segnalazione.

Quali sono le fonti di rischio?

Soggetti estranei all'organizzazione.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

- Crittografia;
- controllo degli accessi fisici;
- controllo degli accessi logici;

- controllo di accesso ai dati;
- sicurezza dell'hardware;
- backup;
- Responsabile interno della sicurezza delle informazioni (CISO)
- sistema di gestione della sicurezza delle informazioni.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitato in quanto le misure di sicurezza informatica sono adeguate, come gestore della segnalazione è stata scelta una società esterna di consulenza, indipendente e autonoma ed in grado di offrire adeguate garanzie di riservatezza e protezione dei dati. I soggetti interni ricevono adeguate istruzioni su come trattare i dati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Sulla base delle misure in essere.

3.4 PERDITA DI DATI

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Disagio/Frustrazione nel non vedere esercitato un proprio diritto e dovere.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

- Attacco informatico al canale online di segnalazione;
- cancellazione accidentale.

Quali sono le fonti di rischio?

- Soggetti estranei all'organizzazione;
- gestore della segnalazione.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

- Controllo degli accessi fisici;
- controllo di accesso ai dati;
- controllo degli accessi logici;
- sicurezza dell'hardware;
- backup.

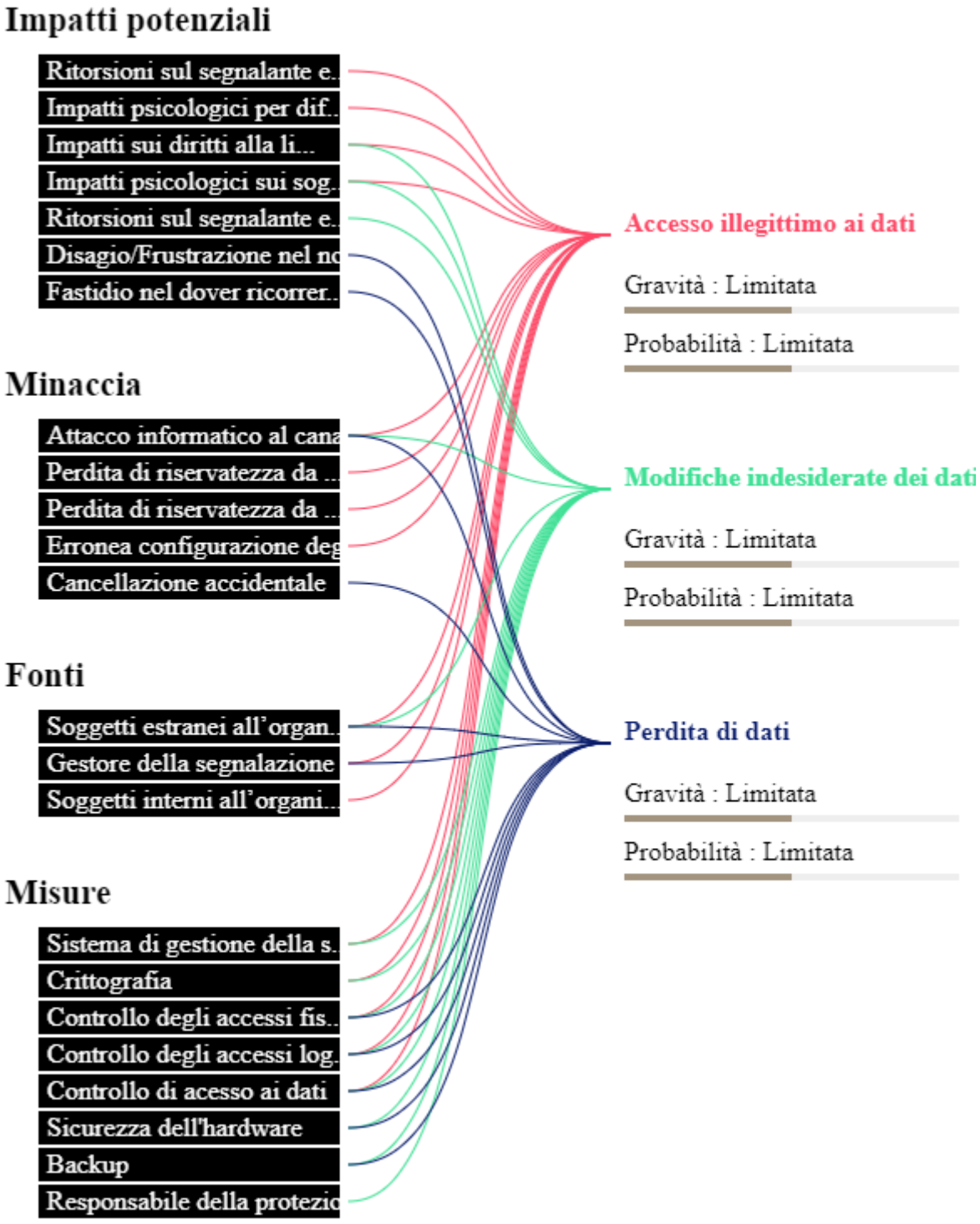
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitato in quanto le misure di sicurezza informatica sono adeguate.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

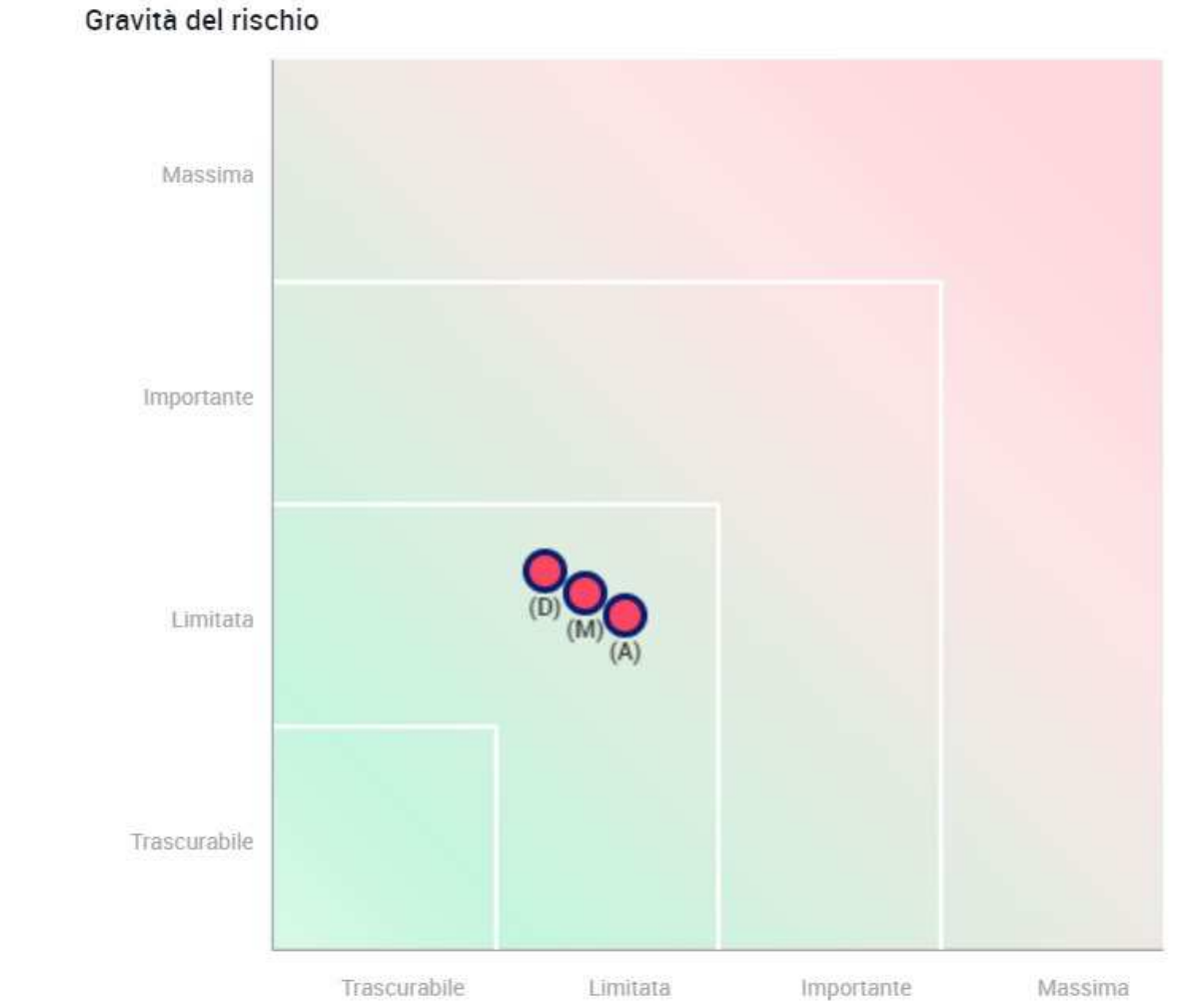
Limitata, sulla base delle misure in essere.

4.4 PANORAMICA DEI RISCHI



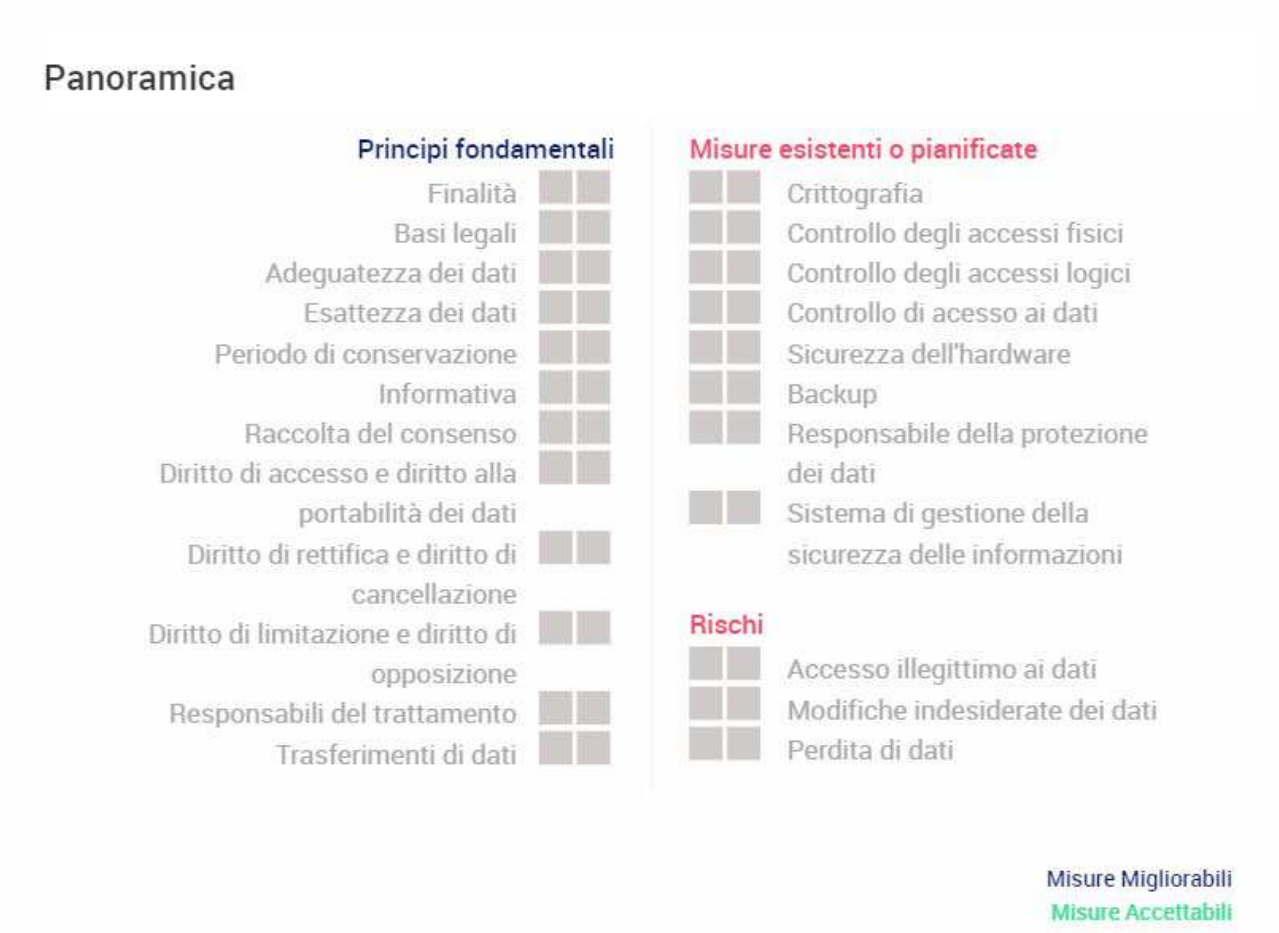
5. CONVALIDA

5.1 MAPPATURA DEL RISCHIO



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

5.2 PIANO D'AZIONE



5.3 PARERI DI DPO/RPD E INTERESSATI

Parere DPO/RPD: NA.

Parere degli interessati: non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento rappresentano l'adempimento di obblighi di legge. Ai fini dell'attivazione del canale di segnalazione interna, il titolare ha inviato via pec, all'associazione sindacale di riferimento, la Procedura per la presentazione e la gestione delle segnalazioni non ricevendo osservazioni in merito.

ALLEGATI

Si allegano alla presente:

- Procedura per la presentazione e la gestione delle segnalazioni;
- Misure tecniche e organizzative per i Servizi Cloud di Global Leaks ISIgame.