VALUTAZIONE D'IMPATTO
(DATA PROTECTION IMPACT ASSESSMENT - "DPIA")
ai sensi dell'art. 35 Reg. UE PRIVACY 679/2016 (GDPR)
relativa ai trattamenti di dati personali connessi
alla PROCEDURA WHISTLEBLOWING di FOR.MA MANTOVA

REDATTO	ADACTA TAX & LEGAL Avv. De Muri Luca Governance e Compliance Advisor
CONTROLLATO	DIRETTORE E LEGALE RAPPRESENTANTE (ANDREA SCAPPI)
APPROVATO	CdA
VERSIONE	2.0
DATA	02/12/2025

Sommario

PREMESSA

Soggetto che redige la DPIA	
TITOLARE DEL TRATTAMENTO	AZIENDA FORMAZIONE MANTOVA - FOR.MA
DATI DI CONTATTO (SEDE)	Via Lorenzo Gandolfo 13 - 46100 - MANTOVA (MN)

Nel presente documento di DPIA vengono citati vari Allegati, che per comodità di lettura vengono identificati in carattere ***Grassetto corsivo***. Gli stessi si intendono costituire parte integrante e sostanziale del documento di DPIA.

1. ATTIVITÀ/TRATTAMENTO OGGETTO DI ANALISI

1.1 Generalità

AZIENDA FORMAZIONE MANTOVA - FOR.MA (di seguito "**FOR.MA**") nell'ambito delle proprie attività opera il trattamento di dati personali, come di seguito descritti, connessi alla propria ***Procedura di Whistleblowing***" sub **Allegato A** adottata in ossequio al D.Lgs. 24/2023 (**Decreto Whistleblowing**), la cui ultima versione viene allegata alla presente DPIA quale **ALLEGATO A** e che verrà approvata dall'organo amministrativo.

In ossequio alla ***Procedura Whistleblowing***, è stato implementato un portale SaaS (Software-as-a-Service) per l'acquisizione tramite web e la conseguente gestione delle segnalazioni di condotte illecite (il "**Portale SaaS**") con il supporto di funzionalità di dialogo criptato tra i vari stakeholders coinvolti.

Le segnalazioni sono disponibili ai team di investigazione (costituiti da uno o più Responsabili di gestione della Segnalazione (denominati anche "**Case Manager**" e nel loro insieme, se più di uno, "**Comitato Segnalazioni**") per ulteriori comunicazioni con i segnalanti e per cooperare con altri investigatori per il seguito e l'istruttoria della segnalazione.

La Piattaforma SaaS è disponibile sia durante che al di fuori dell'orario di lavoro, per 24h/giorno 7 giorni su 7.

Il Portale SaaS include misure tecniche ed organizzative di sicurezza tali da garantire l'osservanza del principio della privacy by design, quindi della "protezione dei dati fin dalla progettazione" (art. 25 GDPR) (tramite misure ragionevolmente adeguate tenuto conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto, delle finalità e dei rischi connessi al trattamento).

Il trattamento ha per oggetto dati personali connessi alla segnalazione di illeciti meglio identificati nella ***Procedura Whistleblowing*** (in particolare, Violazioni di Atti Settoriali della UE, Violazioni 231).

I dati contenuti nelle segnalazioni o successivamente scambiati tra segnalante e FOR.MA o comunque da questa raccolti e trattati in relazione alle stesse sono riferibili a varie categorie di soggetti interessati (segnalanti, segnalato, soggetti tutelati, persone che in veste di Responsabili della Segnalazione o ulteriori Titolari autonomi istruiscono la stessa, persone che partecipano all'istruttoria, membri degli organi apicali di FOR.MA verso i quali sono diretti determinati flussi informativi, referenti di Autorità competenti esterne, ecc., come meglio descritto nell'***Informativa Privacy sul Whistleblowing*** **(Allegato B)**.

1.2 Ciclo di vita dei dati

Il circolo di vita dei dati trattati è il seguente:

1. Il segnalante apre il Front End del sistema SaaS di raccolta e gestione delle segnalazioni "Integrity Line" adottato da FOR.MA ed erogato dal terzo fornitore EQS (raggiungibile tramite qualsiasi browser; la piattaforma include inoltre un back-end riservato ad utenti diversi dal segnalante) e inserisce i dati relativi alla (potenziale) violazione, ai colpevoli e ai recapiti (non obbligatori). Un disclaimer per ottenere il consenso al trattamento dei dati è obbligatorio per essere accettato per continuare il processo.

2. Prima di inoltrare la segnalazione, il segnalante riceve un numero univoco di segnalazione (case ID) e definisce una propria password. Con questi dati di accesso il segnalante può accedere alla propria casella di posta personale protetta sul sistema, per ulteriori comunicazioni con il/i Gestore/i delle Segnalazioni, dopo aver inoltrato la segnalazione.

3. Quando il rapporto viene inviato, tutti i dati in transito e i dati inattivi vengono crittografati utilizzando un protocollo di cifratura avanzata. I dati sono archiviati in modo sicuro in un data center certificato ISO 27001.

Solo le persone preventivamente identificate e appositamente autorizzate presso FOR.MA ricevono una notifica automatica via e-mail quando viene inviata una nuova segnalazione e possono accedere ai dati accedendo al Portale/Software di Case Management (back end) tramite il proprio nome utente e password univoci.

4. Gli utenti autorizzati possono procedere e, se necessario, contattare l'informatore utilizzando una funzionalità di dialogo crittografato (casella di posta protetta) sul Portale SaaS per comunicare ulteriormente e scambiare le informazioni necessarie.

5. Nel termine massimo di 5 anni dalla data di decisione finale circa la segnalazione (archiviazione), fatte salve le esigenze di ulteriore conservazione in caso di Seguiti che danno luogo ad accertamenti, esercizi o difese di un diritto in sede giudiziaria, tutti i relativi dati personali vengono distrutti o resi anonimi da parte del Gestore delle Segnalazioni.

1.3 Ruoli privacy

FOR.MA attua il trattamento dei dati in esame nella veste di **titolare autonomo**, in relazione alle segnalazioni che riguardano la propria organizzazione.

ADACTA STUDIO ASSOCIATO ("ADACTA"), distributore autorizzato del software denominato "Integrity Line" (Portale SaaS) per la raccolta, gestione e archiviazione delle segnalazioni whistleblowing, sviluppato da EQS Group ed accessibile in cloud tramite web app, è stato nominato responsabile del trattamento in relazione al set-up e alla fornitura in licenza al Titolare del Portale e al servizio di help desk di 1° livello.

EQS GROUP SRL è stato nominato sub-responsabile del trattamento in relazione ai servizi di data center e di help desk di 2° livello.

2. OBBLIGATORIETÀ DELLA DPIA

L'articolo 35, comma 1, del GDPR prevede che la Valutazione d'Impatto (di seguito "DPIA") sia obbligatoria quando un trattamento di dati personali "*presenti un **rischio elevato** per i **diritti** e le **libertà** delle **persone fisiche***".

L'art. 13 comma 6 del Decreto Whistleblowing espressamente conferma l'obbligatorietà della redazione della presente DPIA. Tale adempimento è ribadito anche nelle Linee Guida dell'ANAC n. 311/2023 nelle quali si dà conto che è necessario "*Effettuare, nella fase di progettazione del canale di segnalazione e dunque prima dell'inizio del trattamento, una valutazione d'impatto sulla protezione dei dati*".

3. METODOLOGIA DI DPIA

La presente DPIA fa propri alcuni elementi elencati dal Considerando 90 GDPR che risultano sovrapponibili ad elementi ben noti di schemi esistenti per la gestione del rischio (es. ISO 31000).

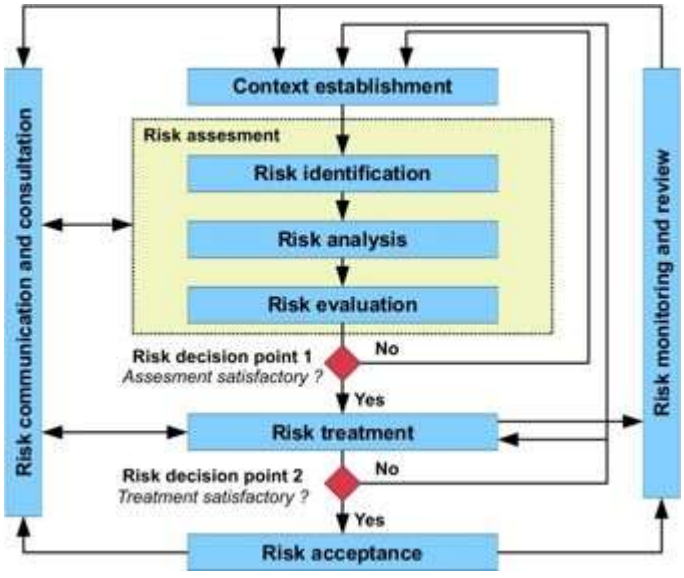


Figura 1: Metodologia DPIA

In termini di gestione del rischio, la DPIA mira a "gestire i rischi esistenti" per i diritti e le libertà delle persone fisiche attraverso i processi di seguito indicati:

- **definizione del contesto**: "*tenendo conto della natura, dell'ambito, del contesto e delle finalità del trattamento e delle fonti di rischio*";

- **valutazione dei rischi**: "*valutare la particolare probabilità e gravità del rischio elevato*";
- **gestione dei rischi**: "*attenuare tale rischio*" "*assicurando la protezione dei dati personali*" e "*dimostrando la conformità al presente Regolamento*" (GDPR, n.d.r.).

La metodologia scelta da FOR.MA per l'attuazione della DPIA rispetta i requisiti minimi obbligatori previsti dall'allegato 2 delle Linee Guida WP248[1], l'attuazione dei quali viene operata nel prosieguo del presente documento.

La presente DPIA utilizza:

- la **metodologia ENISA 2017** di cui al documento **"***Guidelines for SMEs on the security of personal data processing***"** del 27.01.2017, per la valutazione delle **misure di protezione** da applicare ai dati personali;
- la metodologia prevista dalla **norma tecnica ISO/IEC 27001:2022**, come interpretata dalla ISO/IEC 27002;
- la metodologia prevista dalla **norma ISO/IEC 27134:2017** in materia di Valutazione di Impatto in materia di protezione dei dati personali;
- spunti tratti dalla **norma tecnica ISDP©10003:2020** limitatamente alla valutazione e gestione dei **rischi di conformità** diversi quindi da quelli di mera protezione dei dati (la Società ritiene però ridondante e non necessario, nella presente sede, un ricorso sistematico ai requisiti e controlli previsti da tale metodologia, rispetto agli scopi della DPIA); e
- la classificazione delle misure di protezione dei dati personali prevista dal tool per la DPIA del **CNIL**, Autorità Garante francese per la protezione dati personali (per quanto riguarda le misure di competenza del terzo sub-fornitore EQS GROUP AG).

La figura che segue illustra il processo iterativo per lo svolgimento di una DPIA:

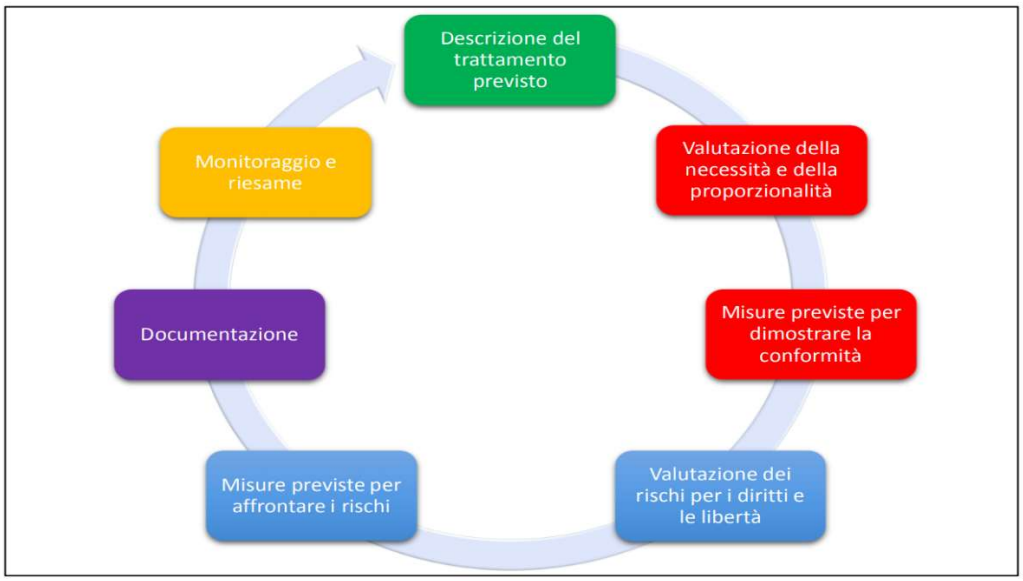


Figura 2: Iter svolgimento DPIA

4. DEFINIZIONE DEL CONTESTO: descrizione sistematica dei trattamenti previsti e delle attività di trattamento

4.1. Intensità del trattamento

Il bilanciamento di interessi tiene conto inoltre dell'intensità del trattamento, valutata ricorrendo a tre criteri: i) tipo di informazioni raccolte; ii) portata (densità delle informazioni e estensione spaziale e geografica), iii) numero di interessati in questione (come quantità specifica).

4.1.1. Tipo di informazioni raccolte

[1] 17/EN - WP 248 rev.01 - *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. Si tratta delle linee guida emesse dal Gruppo ex Art 29 della Dir. Europea 95/46/EC, fatte successivamente proprie dal European Data Protection Board

Le finalità del trattamento non richiedono che gli interessati **Segnalanti** siano sempre identificati o identificabili.

I segnalanti da un lato sono incoraggiati a identificarsi, dall'altro lato per legge sono liberi di optare per l'anonimato.

Il Portale SaaS permette al Segnalante di essere ricontattato dai Case Manager tramite lo stesso anche senza necessità di fornire propri dati di contatto (ed. residenza, domicilio, indirizzo e-mail, P.E.C., numerazioni telefoniche). Il Segnalante viene avvisato di tale circostanza per iscritto dal Titolare, tramite l'***Informativa Privacy Whistleblowing***, prima dell'invio della segnalazione.

Il Segnalante, in particolare, può fornire discrezionalmente il proprio nome e cognome, eventuali codici identificativi personali, informazioni sul proprio ruolo, dati di contatto come ad esempio numeri di telefono, indirizzi e-mail o indirizzi fisici, dati su attività proprie o di altre persone fisiche (es. condotte, circostanze di tempo e di luogo).

I dati concernenti la segnalazione connessa al Segnalante sono automaticamente associati dal Portale SaaS ai relativi dati di orario di raccolta (giorno, ora, minuto, secondo) e all'identificativo univoco della segnalazione stressa. Il Portale SaaS non raccoglie cookie né l'indirizzo IP del dispositivo con cui il Segnalante contatta il Portale SaaS. Tutte le azioni compiute dal Segnalante, nonché degli utenti amministratori, nel Portale SaaS sono inoltre registrate tramite specifici logs.

I dati del Segnalante possono includere la voce degli interessati, captata e registrata in un file audio tramite una funzionalità di casella vocale del Portale SaaS o di un servizio di numerazione telefonica ad esso collegato da parte del Titolare. L'anonimato del segnalante è garantito in tal caso dal c.d. morphing automatizzato della voce registrata, prima della registrazione su server, che impedisce ai Case Manager di riconoscere la voce originale.

I dati di segnalazione sono inoltre classificati per materia, o in base allo stato di avanzamento della segnalazione (es. ricevuta, in fase istruttoria, decisa, ecc.) e al tipo di decisione finale (rigettata, accolta, ecc.).

Il Segnalante è incoraggiato dal titolare a fornire informazioni in suo eventuale possesso relative ad altre persone fisiche o a referenti di persone giuridiche e/o terze altre organizzazioni, che potrebbero essere, in particolare, i) responsabili delle violazioni segnalate (c.d. **soggetti coinvolti**), o ii) a loro volta, **persone a conoscenza dei fatti segnalati** (es. testimoni, o persone fisiche danneggiate dalla violazione di volta in volta segnalata al Titolare) e/o che possono fornire informazioni o documenti utili all'istruttoria della segnalazione.

Il Titolare, inoltre, può venire a conoscenza di dati personali di persone fisiche **accusate di atti o tentativi di atti ritorsivi**, sospettati o posti in essere ai danni del segnalante e/o degli altri soggetti tutelati dalla legge, o, in generale, di eventuale violazione delle norme applicabili al processo di gestione della segnalazione.

Le suddette persone possono essere nominativamente comunicate dal Segnalante stesso o individuate dal Case Manager in occasione dell'istruttoria della segnalazione, es. mediante l'analisi complessiva o più puntuale di elementi indicati nella segnalazione o mediante raffronto con set di informazioni già in possesso del Case Manager.

Il trattamento potrebbe incidentalmente riguardare dati degli interessati, che rivelano un peculiare status tale da farli ritenere **soggetti "deboli"** che (es. dipendenti, soggetti portatori di handicap, familiari a carico dei dipendenti aventi diritto a particolari regimi giuridici legati allo stato di invalidità fisica come ad esempio L. 104, ecc.).

Inoltre, il processo di valutazione della segnalazione richiede il necessario trattamento di dati personali (es. nominativi, ruolo, account e-mail, logs delle attività svolte nel Portale SaaS) riferibili ai **Case Manager** e agli **Admin** designati dal Titolare, e/o di possibili referenti terzi (es. Organi di Polizia, Autorità Giudiziaria, ANAC) coinvolti nel seguito della segnalazione.

Il trattamento in esame di regola **non ha ad oggetto** categorie di **dati particolari** ai sensi dell'art. 9 del GDPR, poiché le attività di business del Titolare connesse alle tipologie di normative presupposto cui si riferisce la possibile segnalazione non implicano, di regola, la necessità di includere anche tale tipologia di dati personali.

L'unica eccezione, allo stato, sono eventuali segnalazioni di violazioni di regole privacy riferite a trattamenti di dati particolari (es. dati di salute) con riferimento ad eventuali violazioni di norme a tutela dei dati personali, richiamate nel Decreto Whistleblowing.

4.1.2 Portata

Estensione spaziale e geografica

Il Sistema di Whistleblowing presidia il rischio di commissione di violazioni, e quindi di azioni di remediation, che possono riguardare tutte le unità locali del Titolare.
I dati sulle segnalazioni risiedono nel database del Portale SaaS ospitato su datacenter con sede in Germania, consultato da utenti Case Manager del Portale SaaS appartenenti all'organizzazione del Titolare o di altre unità locali di FOR.MA.

Densità delle informazioni

Tale criterio riguarda la frequenza del coinvolgimento degli interessati nel sistema di Whistleblowing aziendale.
Tale frequenza è difficilmente stimabile ex ante, in quanto direttamente dipendente dalla volontà dei potenziali segnalanti di fare o meno segnalazioni.

Non sono disponibili informazioni statistiche basate dell'andamento storico delle segnalazioni Whistleblowing pervenute alla data della presente DPIA.

FOR.MA ritiene che una quantità attesa di segnalazione possa orientativamente essere stimata in un numero annuo da 0 a 4. Tale stima si basa, tra l'altro, sulla constatazione circa l'esistenza concreta di numerosi presidi tecnici e organizzativi

delle attività di business o di compliance oggetto delle normative presupposto previste dal Decreto Whistleblowing. Esistenza che di per sé dovrebbe costituire un elemento di tendenziale limitazione delle segnalazioni.

Il Titolare si riserva di aggiornare tale stima sulla base del reporting che diventerà disponibile dopo un primo periodo di uso del Portale SaaS.

4.1.3 Numero di interessati

Valgono, in merito, le stesse osservazioni di cui al punto ii). La quantità di interessati inclusi in una futura singola segnalazione può presumersi, di regola, non elevato, alla luce delle dimensioni e dell'organigramma funzionale del Titolare, del ridotto numero di Case Manager (variabile tendenzialmente da 3 a 5) e del fatto che eventuali Soggetti Coinvolti coincidono verosimilmente soprattutto con i Responsabili di area funzionale. Il numero di eventuali persone interrogate per valutare la segnalazione potrebbe risultare più elevato, ma anche in questo caso di regola non superiore a qualche unità.

4.2. Operazioni di trattamento

Il trattamento sopra descritto svolto da FOR.MA prevede, a seconda dei casi, una o più delle seguenti operazioni, applicate a dati personali o insiemi di dati personali:

- raccolta
- registrazione
- organizzazione
- strutturazione
- conservazione
- modifica
- estrazione
- consultazione
- uso
- raffronto
- interconnessione
- comunicazione (esclusa qualsiasi forma di diffusione)
- limitazione
- cancellazione
- distruzione.

Le specifiche attività di trattamento dei dati di Whistleblowing, la loro natura, l'ambito di applicazione, il contesto, e le aree funzionali aziendali coinvolte nel trattamento, sono descritte nel ***Registro Attività di Trattamento*** del Titolare (art. 30 GDPR) e nell'***Informativa Whistleblowing***.

4.3. Modalità di trattamento

Ai fini dello svolgimento delle attività sopra descritte vengono utilizzate modalità di trattamento cartacee ed elettroniche:

- le **risorse informatiche** su cui si basa il trattamento coincidono con il Portale SaaS, descritto nei seguenti documenti:
  - ***Manuale d'uso del Portale SaaS*** (EQS-Manuale_V3_**Allegato C)**
  - ***MISURE TECNICHE & DOCUMENTAZIONE SULLA SICUREZZA DELLE INFORMAZIONI EQS*** *(qualificato dal fornitore come "**DPIA**")* (fornitore del Portale SaaS) (**Allegato D**)
  - ***Elenco delle Misure tecniche ed organizzative di protezione dei dati – ADACTA*** (Elenco misure tecniche e organizzative di sicurezza ADACTA ver LDM 26.04.2022_**Allegato E**),
- le **risorse cartacee** impiegate potrebbero essere costituite, in ipotesi, da saltuarie stampe cartacee di elaborazioni elettroniche dei dati di whistleblowing effettuati tramite Portale da coloro che gestiscono la ricezione e la valutazione delle segnalazioni.
  Tali supporti sono custoditi come definito nella ***Procedura Whistleblowing***.

  FOR.MA configura il Software in modo da inibire di default la possibilità di scarico in locale di dati dal software da parte dei Gestori delle Segnalazioni; il download richiede l'intervento da back-end dell'amministratore di sistema per modificare tale configurazione.

4.4. Ambito di comunicazione dei dati

Le **risorse umane interne** autorizzate al trattamento dei dati di whistleblowing sono indicate nell'***Elenco degli autorizzati*** e sono destinatarie della ***Nomina ad autorizzato***, mediante la quale vengono impartite ***istruzioni scritte*** per i trattamenti di propria rispettiva competenza. In tale nomina sono incluse istruzioni scritte per la custodia degli archivi e dei documenti. Le nomine hanno una rilevanza anche disciplinare.

Il trattamento coinvolge inoltre alcuni **soggetti esterni** (meglio indicati nel ***Registro trattamenti*** e nell'***Informativa Privacy sul Whistleblowing***.
I terzi agiscono nella veste privacy di i) responsabili del trattamento ai sensi dell'Art 28 GDPR o, secondo il caso, di ii) titolari autonomi.

Nel caso di responsabili viene comunque contrattualizzata la ***Nomina Responsabile*** che contiene specifiche direttive a carico del fornitore dirette al corretto trattamento dei dati trattati.

La struttura aziendale preposta per la privacy analizza tutti i nuovi contratti di acquisto di servizi da terzi fornitori, correlati al trattamento whistleblowing in esame, prima della firma, per valutarne preventivamente i rispettivi impatti privacy e decidere la veste privacy da attribuire ai terzi fornitori/partners che partecipano dall'esterno al trattamento., provvedendo ad aggiornare il sopra menzionato Registro dei trattamenti.

Tra i Responsabili esterni del trattamento rivestono un ruolo rilevante, in particolare, ii fornitore dei servizi di set-up e licenza dei Portale SaaS e il fornitore del Portale SaaS, autorizzati a configurare e svolgere servizio di help desk di primo e secondo livello (vedi Cap. 1.3 Ruoli).

Nel caso di segnalazioni di fatti criminosi, i dati sono inoltre messi a disposizione delle Autorità competenti, da parte di FOR.MA, anche nel caso dovessero contenere dati identificativi di Segnalanti, nel rispetto di quanto previsto dal D.lgs. 23/24.

Non vi è alcuna diffusione dei dati.

5. CONFORMITÀ AI PRINCIPI DELLA NORMATIVA APPLICABILE

5.1. Finalità determinate, esplicite e legittime

Il trattamento dei dati sul whistleblowing da parte di FOR.MA è diretto a perseguire le finalità seguenti:

i) valutare l'ammissibilità e fondatezza della segnalazione di illeciti di cui arriva comunicazione,

ii) applicare le misure di tutela e supporto dei soggetti protetti dalla normativa in materia di whistleblowing,

iii) dare seguito alla segnalazione e fornire misure di risposta ai risultati di una segnalazione (es azioni di remediation), per garantire il rispetto delle normative presupposto previste dal Decreto Whistlebowing;

iv) applicare eventuali misure disciplinari contro chi segnala con dolo o colpa grave, o contro eventuali soggetti coinvolti ai quali sia addebitabile la violazione segnalata,

v) usare gli esiti delle segnalazioni come prova in procedimenti giudiziari,

vi) adempiere a qualsiasi obbligo e/o esercitare un diritto previsto da una legge, da un regolamento o da un'altra normativa applicabile (es. partecipare alle procedure conciliative obbligatorie previste dal codice procedura civile per la rinunzia o transazione di diritti settanti ai Soggetti Tutelati).

I dati trattati non costituiranno il presupposto per l'adozione di forme di ritorsione e/o discriminazione sui segnalanti e sui soggetti tutelati.

Le citate finalità sono esplicitate dei seguenti tre documenti aziendali, da intendersi a ogni effetto quali allegati alla presente DPIA:

- ***Procedura Whistleblowing***,
- ***Informativa Privacy sul Whistleblowing***
- ***Registro dei trattamenti***

Le modalità di distribuzione dei diversi documenti agli interessati destinatari sono effettuate nel rispetto di quanto previsto dal D.lgs. 23/24.

5.2. Liceità del trattamento

In relazione ai dati di whistleblowing, FOR.MA garantisce inoltre i requisiti di conformità del trattamento previsti come obbligatori dal GDPR, con specifico riguardo alla liceità del trattamento stesso, come segue.

5.2.1. Base giuridica

Tenuto conto della normativa di riferimento, il trattamento dei dati personali si fonda

- sull'obbligo di legge a cui è soggetta la Società in quanto Titolare del trattamento (art. 6, par. 1, lett. *c)* del GDPR) ai fini del rispetto delle prescrizioni di cui al Decreto Whistleblowing nonché di cui alla normativa in materia protezione dei dati personali, e,
- per quanto concerne gli eventuali dati particolari riportati volontariamente dal Segnalante, la condizione abilitante è da rinvenirsi nei motivi di interesse pubblico rilevante sulla base del diritto dell'Unione e degli Stati Membri in relazione alla motivazione per cui è stata disposta la normativa whistleblowing (art 9, par. 2, lett. *g)* del GDPR ed art. 2 sexies par. 1 del D.lgs. 196/03), nonché nell'assolvimento di obblighi e sull'esercizio di diritti specifici del Titolare del trattamento e dell'Interessato in materia di diritto del lavoro (art. 9, par. 2, lett. *b)*, GDPR).

Ulteriori precisazioni sulle basi legali

Sarà, di caso in caso, richiesto il preventivo consenso del Segnalante (art. 6 par. 1 lettera *a)* del GDPR) come previsto dal Decreto Whistleblowing, in particolare:

- nel caso in cui il dar Seguito alla Segnalazione comporti, da parte della Società, l'adozione di procedimenti disciplinari e qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione ricevuta e la conoscenza dell'identità della persona sia indispensabile per la difesa dell'incolpato, detta Segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità;
- quando la Segnalazione è effettuata tramite sistema di messaggistica vocale registrato (come previsto nella ***Procedura Whistleblowing***), per poter consentire, a cura del personale addetto, la relativa documentazione mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante trascrizione integrale. In caso di trascrizione, la persona segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione;
- quando, su richiesta della persona segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con il personale addetto, per cui previo consenso della persona segnalante, la segnalazione è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale (come previsto nella Procedura). In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.

In relazione alle finalità di attuare misure di risposta ai risultati di una segnalazione, eventualmente diverse da quelle strettamente necessarie per rimuovere le conseguenze della Violazione segnalata, la base giuridica è l'interesse legittimo del Titolare di migliorare l'assetto dell'organizzazione.

In relazione alle finalità disciplinari o sanzionatorie (5.1 iv), la base giuridica è l'interesse legittimo del Titolare di perseguire in sede disciplinare eventuali inosservanze della Procedura Whistleblowing del Titolare e/o, più in generale, della normativa relativa al whistleblowing, da parte dei dipendenti.

Il Titolare reputa che l'interesse legittimo invocato è **attuale** (cioè non fittizio o speculativo), poiché costituirebbe una condotta non conforme ai criteri di diligenza professionale l'eventuale inerzia del titolare che, a fronte dell'accertamento di un'eventuale responsabilità di un segnalante per dolo o colpa grave, non facesse seguire ad esso alcuna iniziativa disciplinare/sanzionatoria verso lo stesso, diretta a stigmatizzare la condotta del segnalante anche in chiave preventiva di ulteriori illeciti.

In tal caso, infatti, l'inerzia del Titolare sminuirebbe pesantemente la rilevanza della ***Procedura Whistleblowing*** a fini di prevenzione e punizione degli illeciti in essa previsti, causando nei destinatari della stessa l'impressione che un'eventuale inosservanza della Procedura possa restare senza alcuna punizione concreta e quindi aumentando la probabilità di inosservanza stessa.

In relazione alle finalità di uso dei dati come prova in procedimenti giudiziari (inclusi precontenziosi) (5.1 v) la base giuridica è l'interesse legittimo del Titolare di esercitare la difesa dei propri diritti.

Le suddette basi giuridiche risultano puntualmente declinate nell'***Informativa Privacy sul Whistleblowing*** aziendale distribuita agli interessati.

5.2.1.1 Legittimo interesse

Il parziale ricorso alla base giuridica del legittimo interesse in relazione alle finalità disciplinari sopra menzionate, nonché alle eventuali finalità di remediation organizzativa, implica l'obbligo del titolare di eseguire una specifica valutazione di bilanciamento dell'interesse invocato dal Titolare rispetto ai contrapposti interessi delle persone segnalanti interessate. A tale scopo il Titolare provvede a tale valutazione, applicando i seguenti tre criteri previsti dalla Linee Guida EDPB in materia di DPIA:

Coincidenza di interessi

Vi sono **libertà fondamentali** degli individui interessati – in particolare: segnalanti e c.d. soggetti coinvolti - che vengano astrattamente in rilievo per effetto del trattamento in esame (es. dignità della persona, riservatezza, libertà di espressione), tuttavia l'impatto su detti interessati, alla luce delle finalità previste del trattamento, è reputato come ragionevolmente accettabile.

Il trattamento "whistleblowing" avviene per finalità di prevenzione e repressione di illeciti che costituiscono violazione di requisiti normativi che contribuiscono alla compliance dell'impresa, alla conseguente **riduzione del rischio di impatti negativi**, alla **brand reputation** e al suo **posizionamento di mercato**. Il whistleblowing supporta la **continuità** del business e l'**occupazione** ad essa correlata.

Il whistleblowing, dunque, in tal modo tutela, indirettamente, gli stessi segnalanti che appartengono all'organizzazione del Titolare (dipendenti, fornitori, soci, amministratori, ecc.), e/o ai quali si riferiscono fatti oggetto delle segnalazioni (es. le vittime degli illeciti segnalati, c.d. "persone offese" da un reato) e altri interessati appartenenti o meno all'organizzazione del Titolare. Tali soggetti, infatti, possono fare affidamento sulla continuità e lo standing dell'organizzazione, come sopra supportati.

Ciò è vero sia per tutte le azioni di risposta a una segnalazione, dirette in concreto a eliminare o ridurre le cause o le conseguenze della violazione segnalata, ivi incluse eventuali azioni che - non limitandosi a ciò che è strettamente necessario a garantire la conformità dei processi aziendali ai requisiti previsti dalle normative presupposto previste dalla normativa in materia di Whistleblowing - si traducano, caso per caso, in iniziative con un impatto migliorativo più sull'organizzazione del Titolare.

Inoltre, lo specifico **complessivo regime di tutele e supporto** previsto dalla normativa sul whistleblowing in favore dell'interessato segnalante, e più in generale dei c.d. "soggetti tutelati" individuati dalla normativa sul whistleblowing, costituisce un ulteriore elemento di bilanciamento, poiché garantisce a tali categorie di soggetti un vantaggio concreto e inderogabile.

Elemento sorpresa

Tale criterio prende in considerazione le **ragionevoli aspettative degli interessati**, **alla luce della relazione esistente con il Titolare**.

Al riguardo, si può ben presumere che le varie categorie di interessati (segnalante, soggetto segnalato, soggetti tutelati, testimoni, Case Manager, Admin, ecc.) nutrano una **ragionevole aspettativa ex ante** circa il fatto che il Titolare, durante il rapporto con gli interessati stessi, possa attuare un trattamento di dati sul whistleblowing che riguardino gli interessati stessi, per finalità, tra l'altro, disciplinare e di remediation tecnico-organizzativa. Tale presunzione si fonda sulle seguenti considerazioni:

- ✓ **Non è una sorpresa** per l'interessato la volontà del Titolare di garantire il rispetto delle Normative Presupposto, tramite la ***Procedura Whistleblowing*** che prevede anche la possibilità di azioni disciplinari e di rimedio quale possibile esito di una segnalazione ed è portato a previa conoscenza dei destinatari mediante varie modalità meglio descritte altrove nella presente DPIA.
- ✓ Agli interessati viene comunicata inoltre la ***Informativa Privacy sul Whistleblowing*** prima del momento di raccolta dei dati. Le finalità perseguite dal Titolare del trattamento sono quindi correttamente e preventivamente comprensibili dall'interessato. Non sono presenti, e risultano anzi tassativamente vietate, eventuali finalità ulteriori rispetto a quelle ivi dichiarate.
- ✓ Il Titolare ha predisposto e comunicato all'interno dell'organizzazione (es. tramite internet o altre forme di messa a disposizione dei destinatari) specifiche **procedure, protocolli o istruzioni, dirette a pubblicizzare l'obbligo di seguire determinate regole di condotta funzionali al rispetto delle normative presupposto** (esempio, le procedure privacy, la procedura in materia di prevenzione del rischio di commissione di determinati reati a vantaggio o nell'interesse del Titolare).

5.2.2. Portale SaaS e mezzi alternativi

5.2.2.1 Portale SaaS

Tale canale di segnalazione appare il più idoneo e completo rispetto ai requisiti applicabili di sicurezza e privacy (GDPR), in quanto:

- ✓ permette la libera personalizzazione e modifica del form di raccolta segnalazioni e delle avvertenze al segnalante, secondo un principio di minimizzazione (es. sono preventivamente escluse domande non pertinenti);
- ✓ garantisce l'anonimato del Segnalante, non solo in fase di raccolta della segnalazione bensì anche durante l'intero ciclo di gestione della stessa, potendo prescindere dalla raccolta di dati identificativi o di contatto del segnalante;
- ✓ non richiede alcun scarico materiale delle Segnalazioni (sono attivi alert automatici a favore dei Case Manager; tali alert contengono solo il riferimento alla Società cui si riferisce la segnalazione e l'avviso e-mail che sul Portale SaaS sono disponibili nuovi contenuti destinati al Case Manager; questi deve poi autenticarsi in autonomia al Portale SaaS per materialmente accedere al nuovo contenuto oggetto dell'alert pervenutogli);
- ✓ garantisce l'integrità, disponibilità e riservatezza delle Segnalazioni (il database dei dati a riposo e il canale di segnalazione sono cifrati); conserva i dati a riposo in un datacenter esterno certificato ISO 27001;

- ✓ garantisce un log monitoring granulare e integrato di tutte le attività svolte dai vari utenti del Portal SaaS (accessi, modifica delle configurazioni, alterazione di contenuti registrati, attivazione di nuovi utenti, ecc.);
- ✓ permette di subordinare alcune operazioni (attivazione nuovo utente, cancellazione segnalazioni) al principio dei 4 occhi (doppia autorizzazione lato Case Manager);
- ✓ funziona h 24, 7/7, da qualsiasi luogo connesso ad internet, quindi non richiede un accesso fisico del segnalante alla/e sede/i del Titolare;
- ✓ include canali di interazione bidirezionale da/verso il Segnalante e tra i Gestori della Segnalazione per lo scambio di messaggi e documenti;
- ✓ può gestire adeguatamente i diversi ruoli (e conseguenti profili di accesso e privilegio, suddivisi nei 3 ruoli "Case Manager", "Admin" e "SuperAdmin") tramite un sistema di cartelle segregate sia per singola segnalazione sia per ruolo autorizzato di accesso alla medesima) e il processo di escalation della segnalazione;
- ✓ segrega gli admin dall'accesso al contenuto delle segnalazioni (l'admin ha accesso solo alle impostazioni generali funzionali e di sicurezza del Portale SaaS; solo i Case Manager possono visionare e gestire le singole segnalazioni pervenute);
- ✓ gestisce con modalità multilingua il canale di segnalazione stesso (riducendo quindi la necessità di comunicare all'esterno i testi delle segnalazioni pervenute, per eventuali traduzioni in una lingua diversa da quella usata dal segnalante);
- ✓ include una casella vocale ad hoc (durata: 5 minuti) con funzione nativa di cifratura del file audio e morphing (anonimizzazione voce),
- ✓ è in grado di collegare automaticamente tra loro segnalazioni effettuate in tempi diversi relative a una stessa violazione;
- ✓ la cancellazione periodica dei dati è automatizzabile (NB: essa elimina i documenti allegati alla singola segnalazione);
- ✓ dispone di funzioni automatiche di reporting interno sia in favore del Case Manager (es. ricerca di segnalazioni in base a vari criteri selezionabili dall'utente) sia a favore del segnalante (in quest'ultimo caso: mediante creazione di una Secure Inbox interna al Portale SaaS e invio al segnalante di un file cifrato e zippato con password);
- ✓ dispone di funzionalità di anonimizzazione automatica dei contenuti della segnalazione (da attivarsi manualmente), che permettono di creare una seconda versione della segnalazione, depurata di ogni dato personale;

  (tale funzione se attivata elimina i documenti allegati alla segnalazione, poiché potrebbero contenere dati personali);
- ✓ permette di attribuire un workflow status predeterminato per classificare e comunicare l'avanzamento delle singole segnalazioni;
- ✓ include funzionalità - che può essere inibita - di estrazione automatica in locale dei dati (in formato Excel-PDF);
- ✓ può fungere da unico hub centralizzato in cui convogliare, previa raccolta svolta con altri canali interni ed esterni, la trascrizione di eventuali segnalazioni pervenute extra Portale SaaS, e gestire le stesse con una stessa logica;
- ✓ ha un'interfaccia "user friendly" che rende agevole l'uso anche da parte di utenti con basso tasso di alfabetizzazione informatica.

Per contro: la soluzione Portale SaaS non è accessibile a potenziali segnalanti che siano totali "analfabeti informatici" (es. operai del Titolare) e/o che non dispongano del necessario collegamento internet funzionante.

Il Titolare reputa che la gestione del sistema di whistleblowing principalmente tramite Portale SaaS trovi ragionevole e oggettiva giustificazione in base agli **specifici vantaggi tecnico organizzativi** sopra menzionati, che tale soluzione garantisce al Titolare del trattamento, rispetto alle soluzioni alternative teoricamente ipotizzabili.

5.2.2.2 Altri canali adottati

In ogni caso, il Titolare ha deciso di attivare, quale canale di segnalazione parallelo al Portale SaaS, l'**incontro personale** eventualmente richiesto dall'interessato, in conformità al Decreto Whistleblowing (trattasi di obbligo di legge).

5.2.2.3 Soluzioni alternative, analizzate ma non adottate

Il Titolare reputa utile esaminare qui di seguito, in via comparativa, gli ipotetici canali di segnalazione alternativi rispetto al Portale SaaS che è si è scelto di adottare per gestire l'intero ciclo di vita delle segnalazioni, ritenendo che tale analisi sia un elemento metodologico utile in fase di pianificazione by design dei processi di trattamento dei dati connessi al sistema whistleblowing.

Dall'analisi sottostante, emerge come le criticità proprie di ciascuna soluzione alternativa

- **Casella E-mail ordinaria / P.E.C.**

Tale soluzione ha il vantaggio di essere disponibile h 24 7/7, a partire da una qualsiasi connessione internet. È inoltre user friendly.

Essa per contro presenta numerose criticità:

- ✓ è un canale non cifrato;

  un'eventuale associazione al servizio e-mail di un account/servizio di cifratura e-mail erogato da un terzo fornitore (es. del tipo "Protonmail"), oltre ad avere un costo aggiuntivo non potrebbe risolvere la criticità suddetta, perché la cifratura sarebbe applicata ai singoli account di tutti i Case Manager predefiniti, non anche ai possibili segnalanti (che, per definizione, non sono noti ex ante);

  richiede pertanto ulteriori separati canali - adeguatamente protetti - di interazione bidirezionale sicuro verso il segnalante per lo scambio di messaggi e documenti;
- ✓ se il Segnalante non è così esperto da ricorrere autonomamente, a monte, a sistemi di oscuramento dell'indirizzo IP (es. tipo "Tor"), l'opzione non garantisce l'oscuramento nativo dell'indirizzo IP del dispositivo usato per inviare la segnalazione;
- ✓ i messaggi nel Mail Server sono potenzialmente accessibili da parte dell'amministratore di sistema del server (salvo si configuri a livello di Active Directory o di server di posta una segregazione/profilazione a monte da parte di un super admin che tecnicamente venga a sua volta inibito dall'accedere ai messaggi e-mail);
- ✓ se l'e-mail proviene da altre aziende è visibile l'indirizzo IP di queste; è pur vero che tale indirizzo IP cambia ogni volta che i device usati si collegano ad una rete, ma teoricamente non si può escludere il rischio che, tramite tecniche sofisticate note al mercato, un amministratore di sistema infedele del Titolare andare a ritroso e identificare l'IP singolo dell'utente;
- ✓ non può gestire eventuali diversi Case Manager con privilegi tra loro diversi (assegna a chiunque acceda ai messaggi i medesimi privilegi);
- ✓ non segrega gli admin dall'accesso potenziale al contenuto delle segnalazioni (per motivi di manutenzione tecnica del database) cioè il ruolo admin ha potenziale accesso non solo alle impostazioni di sicurezza bensì anche ai messaggi)

  (tale problema si può ridurre, in parte tramite patti di riservatezza, in parte tramite un sistema di log management che includa i logs delle azioni dell'amministratore di sistema ed emetta un alert automatico a fronte di eventuale accesso ai messaggi);
- ✓ non gestisce lato Segnalante la possibilità di attivare una credenziale di autenticazione aggiuntiva rispetto alla singola segnalazione (usa cioè, tramite Active Directory e/o Microsoft 365, la sola user id e password dell'utente relativa alla rete locale);
- ✓ non dispone di funzionalità di anonimizzazione automatica dei contenuti della segnalazione (l'anonimizzazione va cioè eseguita manualmente);
- ✓ non gestisce comunicazioni orali per via elettronica perché eventuali file audio da allegare eccedono la capacità del sistema (problema superabile se il segnalante si limita a comunicare un link ad un file audio esterno al messaggio);
- ✓ non garantisce la cifratura dei dati e-mail a riposo (problema risolvibile se lo storage viene ubicato in datacenter gestiti da big players come es. AWS);
- ✓ non dispone di funzione automatiche di reporting centralizzato classificato, per singola segnalazione e multi-segnalazione;
- ✓ non permette di attribuire dall'interno del sistema un workflow status predeterminato per classificare e comunicare al segnalante e tra Case Manager l'avanzamento delle attività di gestione delle singole segnalazioni;
- ✓ non include funzionalità di traduzione automatizzata del testo della segnalazione tra diverse lingue, né una gestione nativa multilingua degli utenti tramite workflow predefiniti a sistema,
- ✓ non garantisce un logging centralizzato, granulare e integrato di tutte le attività svolte dai vari utenti del Portal SaaS (accessi, modifica delle configurazioni, alterazioni del contenuto delle segnalazioni, ecc.).
- ✓ non gestisce la cancellazione periodica automatica dei dati per singola pratica di segnalazione, secondo criteri prefissati.

La soluzione PEC presenta le medesime criticità della e-mail ordinaria, fatto salvo per quanto riguarda la garanzia tipica circa l'integrità del contenuto dei messaggi e sulla loro provenienza da un determinato soggetto certo.

Le Linee Guida ANAC hanno sottolineano come l'e-mail sia esposta a più probabili rischi di riservatezza, rispetto alla soluzione software. Il Titolare ritiene che tali rischi non vengano superati dall'ipotetica introduzione di misure organizzative aggiuntive di protezione.

NB: Dopo la ricezione della segnalazione comunicata tramite tale e-mail, il Case Manager può in ogni caso caricare la stessa sul Portale SaaS (v. oltre), così che le successive attività di gestione seguano le modalità più garantite - di quest'ultimo.

- **Raccomandata a.r.**

Tale canale ha il vantaggio di essere accessibile anche ad analfabeti informatici, ma presenta diverse criticità, se comparato al Portale SaaS:

- ✓ non garantisce l'anonimato del segnalante (perché la racc.a.r. è sempre inviata da un soggetto identificato o da un terzo identificato soggetto dallo stesso incaricato - es. avvocato, con conseguente rischio per l'esigenza di eventuale anonimato, se non altro nel rapporto interno tra segnalante ed eventuale incaricato);
- ✓ non garantisce l'integrità dei dati contenuti nella segnalazione (in teoria la persona ricevente – intermedia o finale - potrebbe alterare il contenuto della segnalazione trascritto su supporto cartaceo, senza lasciare traccia, o addirittura distruggere od occultare la segnalazione senza possibile controllo di terzi; in ogni caso, in caso di contestazione manca la prova che il contenuto della comunicazione sia esattamente quello invocato da parte del segnalante);
- ✓ tecnicamente non garantisce la riservatezza della segnalazione (la riservatezza è affidata a meri patti di riservatezza a carico del ricevente e a favore del Titolare); infatti l'eventuale ricevente (finale o intermedio es. postino, segreteria) – pur se obbligato alla riservatezza potrebbe aprire la busta e visionarne o alterarne o cancellarne il contenuto;
- ✓ richiede in ogni caso l'attivazione di successivi separati canali di interazione bidirezionale da/verso il segnalante, e tra Case Manager, riproducendo le stesse criticità che connoterebbero tutti i canali eventualmente diversi dal Portale SaaS;
- ✓ lascia inevasa l'esigenza di gestione tecnica dei diversi ruoli / profili di accesso nel ciclo di vita della segnalazione, che deve quindi essere affrontata tramite separati strumenti (incluso il Portale SaaS);
- ✓ non dispone di funzionalità di anonimizzazione automatica dei contenuti della segnalazione (l'anonimizzazione va eseguita manualmente, e potrebbe risultare un'attività time spending nel caso di segnalazioni quantitativamente corpose);
- ✓ non gestisce segnalazioni vocali, che quindi richiedono un canale aggiuntivo;
- ✓ non include funzioni di reporting centralizzato in tempo reale delle segnalazioni (va creato un reporting separato, da aggiornare manualmente) e di estrazione in locale dei dati (salvo previo caricamento dati su Portale SaaS).
- ✓ non include un workflow status predeterminato e protetto per gestire, classificare e comunicare tra Case Manager o al segnalante l'avanzamento delle segnalazioni (va creato separatamente, vedi Portale SaaS);
- ✓ non garantisce un logging granulare e integrato di tutte le attività svolte dai vari Case Manager, dal ruolo Admin e dal segnalante durante il processo di gestione della segnalazione (accessi, attività istruttorie, comunicazioni, modifiche testi, ecc.).
- ✓ non gestisce in automatico l'invio di alert relativi alle scadenze di legge (7 giorni, 90 giorni, ecc.) (serve una separata agenda, che però non permette di rendicontare agevolmente le azioni automatiche ad essa connesse).

NB: Dopo la ricezione della segnalazione comunicata tramite tale racc.a.r., il Case Manager dovrebbe caricare la stessa sul Portale SaaS (v. oltre), così che le successive attività di gestione seguano le modalità di quest'ultimo.

- **Cassetta postale fisica**

Tale soluzione ha il vantaggio di essere disponibile anche ad eventuali potenziali segnalanti "analfabeti informatici" e con continuità durante l'orario di lavoro.

Criticità della soluzione:

- ✓ richiede una "vicinanza fisica" del segnalante alla cassetta (sono impossibili le segnalazioni da remoto), con conseguente impossibilità o alta difficoltà d'uso da parte di segnalanti che non frequentano, o frequentano solo sporadicamente, i locali fisici in cui è essa è collocata (es. soci, consulenti, candidati, ex dipendenti, organi di controllo, ma anche moltissimi fornitori);
- ✓ se la cassetta è collocata in un luogo anche accidentalmente visibile ad altro personale aziendale, non è garantito l'anonimato del segnalante (problema risolvibile mediante eventuale collocazione in luoghi discreti, se presenti in azienda);
- ✓ richiede uno scarico manuale periodico delle segnalazioni, che potrebbe dover essere svolto da personale aziendale diverso dai Case Manager nel caso in cui questi ultimi siano impossibilitati a eseguire personalmente lo scarico con la frequenza ragionevolmente richiesta (es. a causa di ferie, malattia, trasferte, ecc.), quindi come minimo infrasettimanale il segnalante ha diritto di ricevere conferma di ricevuta della segnalazione entro i tassativi 7 giorni dalla data della stessa);
- ✓ non garantisce l'integrità, disponibilità e riservatezza del contenuto della segnalazione (la segnalazione è provvisoriamente custodita e gestita in modalità cartacea da parte del personale aziendale ricevente); riproponendosi le identiche problematiche illustrate in relazione alla soluzione "racc.a.r.", con l'aggravante data dal fatto che – a differenza di quanto avviene per la racc.a.r., che prevede l'obbligo di firma di una ricevuta postale da parte del Titolare – manca una prova documentale che a posteriori permetta di dimostrare l'effettivo ricevimento del plico;
- ✓ ripresenta tutte le identiche altre numerose criticità già descritte in relazione al canale "racc.a.r.".

NB: Dopo la ricezione della segnalazione comunicata tramite cassetta postale fisica, il Case Manager potrebbe comunque caricare la stessa sul Portale SaaS (v. oltre), così che le successive attività di gestione seguano le modalità di quest'ultimo.

- **Chat aziendale**

Tale soluzione può gestire la segregazione di funzioni tra ruolo Case Manager e ruolo Admin, impedendo l'accesso Admin alla chat, tuttavia l'accesso al database del servizio può essere inibito solo tramite patto di riservatezza o altrimenti mediante profili di autorizzazione differenziati tra più amministratori di sistema, se presenti.

Criticità del canale:

- ✓ è disponibile per il segnalante solo durante l'orario di lavoro; funziona in modalità sincrona, quindi non gestisce eventuali problemi di fuso orario;
- ✓ richiede la presenza costante di un operatore specializzato, con costo aggiuntivo se esterno (problema in teoria risolvibile in parte assegnando il presidio direttamente al Case Manager, che però potrebbe non essere fisicamente disponibile nel preciso momento in cui il segnalante lo desidera);
- ✓ richiede successivi canali di interazione bidirezionale con il Segnalante, separati e sicuri, perché di regola non supporta lo scambio interattivo di documenti;
- ✓ non risolve le altre numerose criticità già descritte in relazione al canale "e-mail".

NB: Dopo la ricezione della segnalazione comunicata tramite tale chat, il Case Manager dovrebbe caricare la stessa sul Portale SaaS (v. oltre), così che le successive attività di gestione seguano le modalità di quest'ultimo.

- **Area riservata di raccolta segnalazione sul sito web aziendale**, **o su servizio Google Moduli o altro cloud di terzi**

Tale soluzione potrebbe garantire vari requisiti necessari, in particolare:

- cifratura canale di transito dei dati,
- cifratura dati a riposo, controllo accessi, 2FA,
- inibizione allo scarico in locale delle segnalazioni,
- integrità disponibilità riservatezza dei dati, datacenter ISO 27001,
- disponibilità h 24 7/7 Worldwide,
- hub centralizzato per trascrizione di segnalazione di segnalazioni pervenute con eventuali canali offline, personalizzazione iniziale dei forms di segnalazione predistribuiti ai potenziali segnalanti (ferma la difficoltà di garantire l'aggiornamento della distribuzione stessa in caso di successive variazioni del questionario),
- log monitoring delle azioni degli utenti (pur con solo limitata possibilità di ricerca ex post dei log, per filtri granulari),
- cancellazione automatica dei dati a scadenze predeterminate,
- possibilità di usarla come canale bidirezionale di scambio messaggi e documenti da/verso il segnalante e tra Case Manager,
- possibilità di gestire diversi ruoli (e conseguenti profili di accesso e privilegio, suddivisi nei 3 ruoli "Case Manager", "Admin" e "SuperAdmin") ma con un livello di granularità assai inferiore al Portale SaaS per quanto riguarda il set di privilegi di volta in volta associabile a ciascun ruolo e a ciascun utente di back-end.

Tuttavia, anche tale soluzione presente vari limiti e **criticità** rilevanti, tra cui:

- ✓ costo/tempo di realizzazione; il rapporto costo/beneficio risulta oltremodo incerto (necessità di ricorrere in ogni caso a consulenti legali);
- ✓ raccolta necessaria l'indirizzo IP del segnalante (necessità di uso a monte di servizio tipo "Tor" di anonimizzazione IP, che il segnalante inesperto di regola non è in grado di utilizzare agevolmente) e quindi rischi per anonimato e riservatezza;
- ✓ impossibilità di subordinare alcune operazioni (attivazione nuovo utente, cancellazione segnalazioni) al principio dei 4 occhi;
- ✓ assenza di modalità multilingua/traduzione automatica (necessità di comunicare all'esterno i testi delle segnalazioni pervenute, per eventuali traduzioni in una lingua diversa da quella usata dal segnalante);
- ✓ assenza di una casella vocale con funzione nativa di cifratura del file audio e morphing (anonimizzazione voce) (necessario uso di una linea telefonica separata dedicata, con costo aggiuntivo se gestita in outsourcing da terzi fornitori);
- ✓ assenza di funzioni automatiche di reporting interno sia in favore del Case Manager (es. ricerca di segnalazioni in base a vari criteri selezionabili dall'utente, statistiche) sia a favore del segnalante;
- ✓ assenza di funzionalità di anonimizzazione automatica dei contenuti della segnalazione pervenuta da un segnalante non anonimo (serve attività manuale);
- ✓ assenza di un "workflow status" nativo per classificare e gestire l'avanzamento delle singole segnalazioni.

NB: Dopo la prima segnalazione pervenuta tramite tale canale, il Case Manager può caricare la stessa sul Portale SaaS, proteggendo le successive attività di gestione.

- **Linea Telefonica dedicata (interna o esterna) / Sistema di messaggistica vocale extra Portale SaaS**

Tale soluzione ha il vantaggio di essere usabile anche da analfabeti informatici purché dotati di telefono,

- ✓ Al contempo, presenta vari limiti e **criticità**:
- ✓ non garantisce tecnicamente contro il rischio di potenziale accesso del ruolo Admin ai logs delle chiamate effettuate da e verso il dispositivo del segnalante, nel caso in cui si tratti di un dispositivo assegnato in uso dal Titolare (accesso volontario o accidentale nel corso di eventuali attività di manutenzione);
- ✓ tale problema è solo in parte riducibile tramite istruzioni scritte al ruolo Admin (es. divieto di consultare i logs).
- ✓ Non permette di ricontattare in modalità bidirezionale il Segnalante anonimo che non comunica al Titolare un proprio eventuale recapito.
- ✓ Non include una funzionalità di morphing (anonimizzazione della voce), quindi il segnalante è a rischio di identificazione; l'eventuale anonimizzazione del file audio dovrebbe quindi essere effettuata manualmente dai Case Manager, tramite un separato applicativo, prima dell'ascolto, con rischio di errore/dolo (es. creazione di duplicati) e possibile riconoscimento del segnalante che volesse invece restare anonimo.
- ✓ Non dispone di un sistema automatico di scambio bidirezionali di messaggi e documenti, e quindi ripropone le possibili criticità di sicurezza di necessari canali alternativi (es. e-mail, plichi postali, telefonate, ecc.).
- ✓ Non può gestire in automatico i diversi ruoli (e conseguenti profili di accesso Case Manager vs. Admin) nel processo escalation della segnalazione (chiunque acceda ai messaggi ha infatti i medesimi privilegi); il problema è in parte evitabile in presenza di un unico Case Manager o di più Case Manager, o se vi è un centralino telefonico evoluto eventualmente in grado di gestire i diversi profili di accesso ai messaggi;
- ✓ Non dispone di funzioni automatiche di creazione/distribuzioni del reporting, che deve quindi essere create e gestite manualmente.
- ✓ Non dispone di un sistema di log management centralizzato che consenta una vigilanza ex post sull'operato dei singoli utenti del canale, dal lato del Titolare;
- ✓ Richiede la presenza di un personale dedicato, non possibile al di fuori del normale orario di lavoro. La linea se è gestita in outsourcing da fornitori implica un costo aggiuntivo.
- ✓ Non permette la cifratura dei dati in transito sul canale telefonico dedicato. Non garantisce di default la cifratura a riposo dei dati.

NB: Dopo la prima segnalazione pervenuta tramite tale canale, il Case Manager può caricare la stessa sul Portale SaaS, così proteggendo adeguatamente le successive attività di gestione della segnalazione stessa.

5.2.3. Distribuzione dei vantaggi

Vi sono particolari implicazioni etiche derivanti dal trattamento in esame,

Si considerano inoltre le seguenti circostanze:

- ✓ Il Titolare può trarre particolari vantaggi da un utilizzo diretto dei dati sul whistleblowing all'interno del proprio business, ad esempio in termini di compliance, trasparenza, reputazione. Infatti, i fatti oggetto di segnalazione potrebbero riguardare violazioni rientranti nel campo di applicazione del D.Lgs. 231/2001 o violazioni di atti settoriali dell'unione previsti dal Decreto Whistleblowing. Pertanto, i trattamenti dei dati sono funzionali ad obiettivi aziendali di trasparenza, fiducia e compliance.

  Il raggiungimento di tali obiettivi crea "salute aziendale" (intesa come continuità operativa, e riduzione dei rischi ad essa correlati) e quindi avvantaggia indirettamente gli stessi interessati (es. segnalanti).
- ✓ I segnalanti grazie all'utilizzo dei canali di segnalazione approntati da FOR.MA sono ammessi al godimento inderogabile di un regime di tutela tecnico-legale specifica ed articolata, che altrimenti non potrebbe essere loro garantito con lo stesso livello di efficacia.
  Inoltre, tale tutela si estende automaticamente per legge anche una serie di ulteriori soggetti collegati al segnalante a vario titolo, i cui dati personali sono trattati tramite i suddetti canali di segnalazione approntati (es. software).
- ✓ L'agevole fruibilità del Portale SaaS costituisce esso stesso un fattore di vantaggio per i segnalanti, rispetto ad altri canali meno agevoli.

Alla luce degli elementi sopra riportati, il rischio inerente di una comunicazione non autorizzata a terzi da parte del Titolare appare dunque medio-alto.

5.2.4. Minimizzazione del trattamento. Necessità e proporzionalità

5.2.4.1 Minimizzazione

FOR.MA opera predisponendo affinché i dati personali siano adeguati, pertinenti e limitati a quanto necessario (c.d. minimizzazione dei dati).

A tal riguardo si precisa:

- ✓ Il trattamento (operato mediante l'utilizzo dei mezzi sopra menzionati) è di **ausilio** concreto al raggiungimento delle descritte finalità, essendo in **rapporto di stretta funzionalità** rispetto agli obiettivi sopra descritti.
- ✓ Il trattamento appare ragionevolmente **proporzionato** rispetto alle finalità, anche sotto il profilo delle modalità;
- ✓ Gli **scopi** perseguiti dal Titolare **difficilmente si potrebbero raggiungere** senza il trattamento in esame.
- ✓ Il segnalante ha la facoltà discrezionale di piena decisione sia in relazione ai contenuti comunicati inizialmente al Titolare sia per eventuali modifiche, integrazioni, modifiche o cancellazioni comunicate in seguito al Titolare.
- ✓ I dati personali acquisiti tramite il Portale SaaS sono congrui con le finalità del sistema. Il **questionario** proposto al segnalante tramite il Portale SaaS prevede una serie predeterminata di campi compilabili di testo, specificatamente preconfigurati dal Titolare, tramite i quali il Titolare raccoglie dal segnalante il **minimo** degli elementi utili a soddisfare le finalità dichiarate. Solo alcuni campi devono essere obbligatoriamente compilati dal segnalante, a pena di impossibilità di inviare la segnalazione, ferma la facoltà del segnalante di compilare anche altri campi facoltativi. Ciò garantisce che le informazioni contenute nella segnalazione siano quelle, almeno minime, necessarie alle finalità previste, cioè sufficienti a permettere di i) qualificare come segnalazione "ammessa" o "non ammessa" la comunicazione pervenuta e ii) nel caso di segnalazione "ammessa", approfondire nel merito la fondatezza o meno della stessa.
- ✓ La comunicazione della segnalazione in via orale, previo consenso del segnalante, è documentata a cura del Case Manager mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, il segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.

  Il medesimo processo di trascrizione, registrazione su Portale SaaS e separata conferma da parte del segnalante avviene, infine, nel caso di segnalazione inviata tramite il numero telefonico dedicato extra Portale SaaS.

  Quanto sopra limita ex ante in rischio che vengano dal Titolare informazioni palesemente superflue rispetto alle finalità previste.
- ✓ Il Titolare preventivamente **determina gli ambiti di autorizzazione** attribuiti ai singoli incaricati del trattamento e definisce profili di accesso differenziato ai dati e alle risorse con cui avviene il trattamento. Ai dati sul whistleblowing accedono solo le persone previamente individuate e debitamente designate tramite lettera di nomina e **istruite per iscritto** dal Titolare, che includono l'espresso obbligo di eliminare immediatamente eventuali dal testo delle segnalazioni pervenute eventuali dati personali che non appaiono necessari alla valutazione della segnalazione.

  Grazie ai diversi profili utente del Portale SaaS Integrity Line e alla sua gestione granulare dei permessi, il Titolare può attuare una chiara **segregazione dei compiti**. A titolo esemplificativo:

  Autorizzazioni generali per gli utenti:
  - visualizzazione e modifica delle traduzioni (personalizzazione);
  - visualizzazione e creazione di criteri (personalizzazione);
  - visualizzazione e creazione di promemoria automatici (personalizzazione);
  - visualizzazione e creazione di moduli/questionari (personalizzazione);
  - visualizza l'audit trail;
  - esportazione di tutti i casi.

  Permessi dei Case manager:
  - visualizza la segnalazione (in base alla cartella selezionata / al paese);
  - creare una nuova segnalazione (tramite l'interfaccia di amministrazione);
  - chiudere una segnalazione;
  - inviare messaggi ad un segnalante;
  - modifica del Case manager responsabile, dell'accesso alle cartelle e della classificazione;
  - cancellare le segnalazioni;
  - privilegi bloccati (non è possibile modificare le impostazioni dell'utente e l'accesso alle pagine per sé stessi);
  - annullamento dell'accesso alle cartelle (per la dashboard, per visualizzare la reportistica completa indipendentemente dal caso);
  - esportazione delle segnalazioni;
  - visualizza solo segnalazioni anonimizzate;
  - anonimizzare le segnalazioni.

  Autorizzazioni per la gestione degli utenti:
  - può accedere alla gestione degli utenti;

- creare nuovi utenti
- disattivare o eliminare gli utenti;
- modifica dei dati personali degli utenti;
- modificare le autorizzazioni di accesso;
- ripristino della password utente.

È possibile suddividere gli utenti amministratori in sottogruppi per ciascuna delle aree sopra indicate o avere un super amministratore per tutti i permessi. In base alle autorizzazioni dei singoli utenti, i Case Manager possono accedere a tutti o a un sottoinsieme di segnalazioni.

Per alcune dei privilegi più critici (creazione di un utente, cancellazione di un caso, ecc.) è possibile attivare la funzione "4 Eyes Principle". Invece di un solo utente che esegue queste attività, un secondo utente dovrà confermare l'azione per ogni caso specifico.

Il livello di accesso al sistema e/o di utilizzo delle informazioni deve intendersi in ogni caso limitato, per ciascun autorizzato, a quanto strettamente necessario al corretto esercizio delle mansioni e operazioni di trattamento affidategli.

Pertanto, se un'informazione non viene raccolta o viene cancellata da parte del Case Manager, non potrà essere usata successivamente e, quindi, in caso di scelte avventate, si potrebbe compromettere l'accertamento e la punizione di un illecito e si rischia la contestazione di condotte favoreggiatrici o di complicità. Al contrario, se un'informazione inutile viene conservata, il Titolare si espone alla contestazione della conservazione indebita di un dato e, quindi di violazione della privacy. Gli opposti e simmetrici rischi comportano sanzioni per il Titolare e quindi non è facile evitare i pericoli.

In effetti, stabilire cosa è "manifestamente non utile" può essere, in concreto, complicato, visto che un giudizio di questo tipo lo si può formulare solo dopo avere completato una istruttoria che in molti casi potrebbe risultare lunga e complessa.

L'alea potenziale residua dell'operazione di "filtro" delle informazioni è quindi collegata all'eventuale **dolo o errore umano** di chi valuta la segnalazione.

La possibilità di errore viene prevenuta dal Titolare tramite l'erogazione di specifiche attività di formazione ai Case Manager e Admin designati.

A monte, inoltre le attività informative erogate dal Titolare ai potenziali segnalanti mira, tra l'altro, a rendere consapevoli gli stessi circa la opportunità di non comunicare al Titolare informazioni palesemente irrilevanti.

- ✓ I contenuti delle singole segnalazioni e della messaggistica interna ad esse collegata **non sono materialmente accessibili dai soggetti non autorizzati, neppure nel caso di amministratori di sistema**: questi ultimi, infatti, per default possono accedono solo a configurazioni tecniche (segregazione di funzioni).
- ✓ Per quanto concerne i **profili di autenticazione**, l'accesso ai dati personali da parte del personale autorizzato interno o esterno avviene esclusivamente mediante il proprio profilo di autenticazione personale (es. password univoca), soggetta a policy rigorose, che includono funzionalità di 2FA (vedi ***Manuale Portale SaaS***).
- ✓ La Società **registra tramite log sia tutti gli accessi logici** degli utenti **sia tutte le operazioni compiute** sui dati del Portale SaaS dagli utenti, **compresi i relativi riferimenti temporali**. Tali dati sono necessari a garantire la sicurezza del sistema, permettendo di accertare in qualsiasi momento, a posteriori se, per esempio, le condotte degli utenti siano conformi ai requisiti previsti dal Decreto Whistleblowing.
- ✓ I **metadati che potrebbero rivelare l'identità dell'segnalante nei file caricati vengono rimossi** nel processo di File Detox dei file. Sul punto vedasi il capitolo 7.2.10 "protezione da software dannoso".

5.2.4.2 Limitazione della conservazione

FOR.MA opera predisponendo affinché debba essere rispettato il principio di limitazione della conservazione, in relazione alle finalità del trattamento.

I termini di conservazione dei dati sul whistleblowing coincidono con il tempo necessario a gestire i processi di ricezione e trattamento della singola segnalazione. Dopo la scadenza, i dati sono anonimizzati permanentemente oppure sono cancellati.

Tali termini vengono espressamente menzionati nel ***Registro trattamenti***, nella ***Procedura Whistleblowing***, e nell'***Informativa Whistleblowing***.

Il Portale SaaS permette al ruolo Admin di configurare manualmente nel back-end il termine di conservazione massimo dei dati ivi contenuti concernenti la singola segnalazione.

Il termine di conservazione previsto dal Decreto Whistleblowing e configurato nel Portale SaaS è di 5 anni dalla data di decisione finale sulla segnalazione. Tale termine assorbe in sé la scadenza minima prevista per il log dal Provvedimento del Garante del 7 novembre 2008 in materia di amministratori di sistema, che è di 6 mesi.

In ogni caso, nel caso in cui la segnalazione ricevuta dia luogo ad una comunicazione ad una Autorità competente (es. in caso di attivazione in sede penale di indagini relativi a illeciti rilevati), o a un contenzioso (es. disciplinare, o giudiziale civile, giuslavoristico, amministrativo), il termine di conservazione è prorogato fino all'esaurimento del contenzioso tramite provvedimento avente valore di giudicato o successiva azione esecutiva

Il Portale SaaS, previa configurazione ad hoc nel back-end da parte dell'Admin in sede di set-up, invia di default ai Case Manager specifici remainder con cui avverte della futura cancellazione alla scadenza stabilita. È quindi possibile per il Case Manager richiedere all'Admin una proroga del termine di conservazione, ove ne ricorra il presupposto di cui sopra.

Il Portale SaaS, inoltre, conserva tutti i log della distruzione stessa (trail audit), che sono quindi disponibili per qualsiasi eventuale verifica interna o da parte dell'Autorità di controllo.

5.2.5. Esattezza e aggiornamento

I dati personali devono essere esatti ed aggiornati.

Il segnalante ha il pieno e discrezionale controllo sia delle informazioni inizialmente comunicate al Titolare sia del contenuto di eventuali modifiche, integrazioni o cancellazioni che in seguito egli intenda comunicare al Titolare.

I Case Manager possono sempre richiedere aggiornamenti dei dati al segnalante, in sede di istruttoria della segnalazione, se ritengono che i dati ricevuti siano obsoleti o inesatti.

I Case Manager possono valutare se le informazioni ricevute tramite la segnalazione sono sufficientemente accurate rispetto alle finalità del trattamento.
Per tale motivo, la ***Procedura Whistleblowing*** del Titolare, non contiene norme di maggiore dettaglio circa le modalità di verifica della manifesta non utilità (parametri) della segnalazione, affidando alla sensibilità professionale dei Case Manager il compito di effettuare tale valutazione, in base a criteri di diligenza, caso per caso.

L'alea potenziale dell'operazione di aggiornamento è quindi collegata perlopiù all'eventuale **dolo o errore** umano di chi valuta la segnalazione.

Circa le modalità dell'operazione di aggiornamento, invece, il Portale SaaS conserva tutti i log dell'aggiornamento stesso (trail audit), che sono quindi disponibili per qualsiasi eventuale verifica interna o da parte dell'Autorità di controllo.

6. VALUTAZIONE DEI RISCHI

Le Linee Guida WP248 impongono che in relazione al trattamento dei dati personali oggetto del sistema whistleblowing in esame:

- l'**origine**, la **natura**, la **particolarità** e la **gravità** dei **rischi** (cfr. considerando 84 del GDPR) o, più in particolare, di ciascun rischio (rischio di accesso illegittimo, modifica indesiderata e indisponibilità dei dati, cd. **valutazione "RID** – Riservatezza – Integrità – Disponibilità") vengano determinate **dalla prospettiva degli interessati**, secondo una metodologia che:
  - ✓ consideri le **fonti** di rischio (considerando 90 del GDPR);
  - ✓ individui gli **impatti** potenziali **per i diritti e le libertà degli interessati** in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la indisponibilità dei dati;
  - ✓ individui le **minacce** che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la indisponibilità dei dati; e
- vengano stimate la **probabilità** e la **gravità** dei **rischi** di volta in volta valutati (considerando 90 del GDPR).

Rispetto ai requisiti suddetti, il Titolare applica nella presente DPIA la metodologia prevista nelle **Linee Guida 2017 ENISA** (Agenzia Europea per la Sicurezza delle Informazioni), che prevedono allo scopo la necessaria combinazione dei due criteri di **IMPATTO** (x) **PROBABILITÀ**, come di seguito indicato.

Per "IMPATTO" si intende la **GRAVITA'** delle conseguenze, in particolare il **danno potenzialmente arrecabile all'interessato**, a seguito di rischi di perdita di riservatezza, integrità e/o disponibilità dei dati.

Secondo le Linee ENISA, le **metriche** di possibile IMPATTO da utilizzare sono 4: **BASSO; MEDIO, ALTO**, **MOLTO ALTO** e l'impatto concretamente si può distinguere in tre categorie generali: fisico, morale, materiale, come segue:

METRICHE DEL LIVELLO DI IMPATTO	DESCRIZIONE LIVELLO DI IMPATTO	Esempi di impatto fisico	Esempi di impatto materiale (I = Integrità, D = Disponibilità, R = Riservatezza A = Altro)	Esempi di impatto morale
BASSO/TRASCURABILE	**Gli interessati non incontrano inconvenienti, o possono incontrare alcuni piccoli inconvenienti, che supereranno senza alcun problema**	- Inaccessibilità temporanea dei canali di segnalazione, risolta in tempi brevi (D)	- Alterazione/Perdita di dati, ripristinabili in toto da backup (I-D) - Violazione della privacy senza pregiudizio (es. uso senza consenso di immagini ripristinabili in toto da backup) (R)	- Paura di perdita del contenuto della segnalazione effettuata / sensazione di invasione della privacy, senza oggettivo pregiudizio (sistema funzionante, dati ripristinabili da backup) (A) Timore di segnalare per la promiscuità dei locali condivisi con colleghi o terzi (es. postazione visibile a terzi) (R)
MEDIO/ LIMITATO	**Gli interessati possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà.**	- Inaccessibilità prolungata e/o uso difettoso dei canali di segnalazione (D)	- Alterazione/Perdita di dati, ripristinabili in parte da backup (I+D) Tentativi di ritorsione o discriminazione (A)	- Paura di potenziali ritorsioni / discriminazioni (demansionamento / licenziamento) benché vietati (A)
ALTO/ SIGNIFICATIVO	**Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà**	n.a.	- Segnalazione concreta a soggetto sbagliato /i per i) errore o carenza di consapevolezza del segnalante e/o del Case Manager (es. comunico al superiore gerarchico accusato anziché ad un organo terzo e indipendente) o ii) cattiva gestione del cambio mansione o dimissioni del naturale destinatario e subentro di una nuova risorsa (change management) (R) - Alterazione/Perdita di dati, non ripristinabili da backup (I+D) - Atti di ritorsione o discriminazione	- Disturbi psicologici minori ma oggettivi (diffamazione, reputazione, paura, mancanza di comprensione) - Serenità compromessa del potenziale segnalante dovuta a i) mancato accesso o uso difettoso di un canale di segnalazione, o ii) segnalazione concreta a soggetto sbagliato

			(necessità del soggetto tutelato di invocare la tutela legale) (A) - Rischio di ostacolare le indagini sulle condotte illecite segnalate se le persone accusate sono a conoscenza delle segnalazioni (A)	
MOLTO ALTO/ MASSIMO	**Gli interessati possono subire conseguenze significative, o addirittura irreversibili, che non possono superare**	Suicidio, Morte	- Incorretta applicazione della Procedura di whistleblowing, in particolare: i) mancata anonimizzazione / accesso non autorizzato a dati particolari relativi al segnalante o all'accusato, o ii) mancato/tardivo riscontro al segnalante) (A), iii) istruttoria inidonea (A)	- Disturbi psicologici gravi (shock, ansia sociale / difficoltà relazionali, depressione, attacchi di panico)

Alla luce dei suddetti criteri, il valore "**IMPATTO**" viene così prudentemente determinato come segue da FOR.MA:

- il **livello** di impatto causato da una **perdita di riservatezza** viene considerato da **MEDIO** a **MOLTO ALTO**,

poiché la comunicazione non autorizzata (es. ad un errato destinatario e/o a terzi) o diffusione di dati personali riferibili ad un interessato (R), potrebbero astrattamente causare, a seconda dei casi, dal punto di vista dell'**impatto morale**, effetti progressivamente maggiori, quali, in particolare, ad esempio (vedi sopra):

i) una sensazione di invasione della propria privacy / paura di perdita del dato in sé, pur senza un danno reale per esso ove esista un idoneo sistema di integrale back-up e ripristino) o

ii) la paura di potenziali ritorsioni o discriminazioni passive (su cui vedi oltre), o

disturbi psicologici minori ma oggettivi (paura, disagio per effetto di eventuale diffamazione, calunnia; mancanza di comprensione (quest'ultimo rischio viene però molto ridotto da FOR.MA tramite adeguata **preventiva formazione** dei potenziali segnalanti (es. tramite messa a disposizione della ***Procedura Whistleblowing*** con modalità comprovabili), e dalla **normativa** che prevede uno specifico diritto dei segnalanti potenziali ed effettivi ad ottenere il supporto nelle forme previste dalla stessa) fino ad arrivare, in casi estremi, a

veri e propri disturbi psicologici gravi (shock, ansia sociale / difficoltà relazionali, depressione, attacchi di panico); tali ultimi impatti non sono escludibili a priori sulla base della comune esperienza, specie nel caso in cui la violazione della riservatezza includa dati particolari riferibili ad un segnalante o accusato, tuttavia, la possibile rivelazione non autorizzata dei dati, viene mitigata nei suoi potenziali effetti pregiudizievoli dall'insieme dei presidi meglio descritti nel capitolo PROBABILITA'.

e, dal punto di vista dell'impatto **materiale**:

i) tentativi o atti di ritorsione o discriminazione (tali atti e tentativi sono però vietati tassativamente dalla vigente normativa, che, pertanto, riduce così drasticamente il rischio in esame); e/o

ii) rischio di ostacoli alle indagini sulla violazione segnalata, se le persone accusate sono a conoscenza della stessa. Tali ostacoli appaiono però superabili senza difficoltà, poiché il processo di gestione delle segnalazioni risulta analiticamente e formalmente normato tramite apposita procedura aziendale che limita la possibilità di diffusione non autorizzata del contenuto delle segnalazioni.

- il **livello** di impatto causato da una **perdita dell'integrità** viene considerato **BASSO**, poiché l'inaccessibilità / l'uso difettoso di un canale di segnalazione o l'alterazione accidentale o dolosa dei dati potrebbero causare:

i) un danno in capo all'interessato (che dovrebbe nuovamente ricostruire la dinamica di eventuali fatti illeciti segnalati;

tale rischio è però ridotto al minimo, come vedremo, dall'utilizzo di un tool software che garantisce la cifratura a riposo del dato e di un data center del terzo fornitore che garantisce inoltre l'integrale ripristino da supporto di backup dei dati originari a fronte di incidenti gravi; il rischio concreto residuo permane in sostanza solo per l'ipotesi di un mancato funzionamento dei sistemi di backup ridondati ubicati presso il suddetto datacenter del terzo fornitore); e/o

ii) un danno (A) al processo di gestione della segnalazione, o al processo di tutela dei soggetti tutelati dalla normativa whistleblowing, in particolare lievi ritardi in attesa del ripristino dei dati originari oggetto di incidente (ripristino facilmente eseguibile utilizzando le copie di back-up dei dati, nella disponibilità del Titolare).

- il **livello** di impatto causato da una **perdita della disponibilità** viene considerato **BASSO**, per le stesse considerazioni svolte, *mutatis mutandis*, in tema di integrità dei dati personali e perché l'inaccessibilità temporanea dei canali di segnalazione, è ragionevolmente rimediata in tempi brevi (D), mentre l'inaccessibilità prolungata e/o uso difettoso dei canali di segnalazione (D) è presidiata dalla garanzia software del terzo fornitore.

Secondo ENISA, tra i tre livelli di rischio sopra indicati deve prevalere il livello **più alto** e cioè quello **MOLTO ALTO**, pertanto:

VALUTAZIONE DI IMPATTO		
Riservatezza	Integrità	Disponibilità
MEDIO-MOLTO ALTO	BASSO	BASSO
VALUTAZIONE COMPLESSIVA DI IMPATTO		**MOLTO ALTO**

*

In relazione, invece, al livello di **PROBABILITA'** del rischio connesso al trattamento dati avente finalità di gestione whistleblowing, la scala di possibile punteggio ENISA da applicare è: **BASSO**, **MEDIO**, **ALTO/MOLTO ALTO**.

I criteri di **PROBABILITA'** in base alle Linee guida ENISA sono calcolati sulla base delle risposte date dal Titolare ad una serie di 20 domande (n. 5 domande per i seguenti n. **4 argomenti operativi**:

- Rete e risorse tecniche (hardware e software);
- Processi/procedure relative al trattamento dei dati;
- Parti e persone coinvolte nel processo di trattamento;
- Settore di attività e scala (intesa come "volume") del trattamento)

[Il contenuto di dettaglio delle domande ENISA è descritto in maggiore dettaglio nel documento **DOMANDE.ENISA.CLASSIFICAZIONE.RISCHIO** redatto dal Titolare, costituente **Allegato F** alla presente DPIA.]

Tanto premesso, FOR.MA con riferimento ai quattro aspetti sopra elencati è pervenuta alla seguente stima:

- **Rete e risorse tecniche** (hardware e software):

  la probabilità di avverarsi del rischio è **BASSA**, perché
  i sistemi di trattamento sono interconnessi ad altri sistemi esterni (quelli di EQS Group S.R.L fornitore affidatario del servizio di Portale SaaS in outsourcing), ma questi sono altamente presidiati tramite misure di sicurezza reputate adeguate ai rischi.

- **Processi/procedure relative al trattamento dei dati**:

  la probabilità di avverarsi del rischio è **BASSA**, perché
  i processi di whistleblowing sono ben definiti tramite la ***Procedura Whistleblowing*** e i terzi fornitori specializzati che agiscono quali responsabili e/o sub-responsabili del trattamento ai sensi dell'art. 28 del GDPR per conto di FOR.MA (ADACTA STUDIO ASSOCIATO e EQS Group S.R.L e) aderiscono a best practice di sicurezza in materia (vedi documentazione disponibile sui rispettivi siti internet dei sopra menzionati fornitori, nelle condizioni generali di servizio applicate al rapporto con il Titolare, nei termini privacy e/o nelle ***Nomine dei responsabili esterni*** del trattamento, applicati/e nei rapporti con il Titolare) e come verificato tramite ***Audit periodici dei Responsabili*** pianificati su base annuale dal Titolare.

- **<u>Parti e persone coinvolte nel processo di trattamento</u>**:

  La probabilità di verificarsi dell'evento è **BASSA**, perché:

  i) il trattamento è adeguatamente presidiato mediante le ***Nomine Autorizzati*** contenenti precise istruzioni circa le corrette modalità dei trattamenti dei dati/documenti cartacei e mediante la ***Procedura Whistleblowing*** contenente specifiche indicazioni circa le corrette modalità del trattamento, e

  ii) una parte del trattamento è svolta da Responsabili ex Art 28 GDPR (vedi Cap. 1.3 Ruoli) e, quindi, il Titolare, seppur nel pieno controllo dei dati, è esposto a minacce aggiuntive (rischio inerente) proprie dell'organizzazione del terzo responsabile.

  Tuttavia, i suddetti responsabili esterni aderiscono alle best practice di sicurezza di settore (es. ISO 27001 con riguardo ai servizi EQS), e inoltre assumono contrattualmente in favore di FOR.MA specifici obblighi di protezione dei dati in favore di FOR.MA (es. tramite la ***Nomina Responsabile*** che prevede obblighi di adozione di adeguate misure tecniche e organizzative di sicurezza a presidio dei trattamenti)) il cui rispetto è altresì verificato da parte di FOR.MA tramite l'esecuzione pianificata di ***Audit periodici dei Responsabili***.

  iii) Inoltre, i Gestori delle Segnalazioni sono stati scelti in base alla posizione funzionali di **neutralità e indipendenza** rispetto al contenuto delle segnalazioni pervenute e hanno ricevuto adeguata **specifica formazione** preventiva circa le loro mansioni, in conformità a quanto prescritto dl Decreto Whistleblowing.

  Quanto al primo requisito suddetto, l'indipendenza discende, a seconda dei casi:

  a) dal ruolo che il Gestore della Segnalazione assume, in parallelo, quale membro dell'Organismo di Vigilanza 231 del Titolare (dotato di poteri autonomi, ai sensi dell'art. 6 del D.Lgs. 231/2001, comma 1, lettera b), o
  b) dal ruolo autonomo che il Gestore della Segnalazione assume all'interno dell'organigramma funzionale dell'organizzazione del Titolare (quale ad esempio, responsabile dell'area Internal Audit & Compliance).

  Per quanto riguarda invece il secondo requisito (formazione), il **bagaglio tecnico-professionale** connesso ai predetti ruoli è reputato in questa sede come idoneo a garantire l'esistenza di competenze ed esperienze che lo mettono in grado di gestire adeguatamente il ruolo stesso.

  iv) Eventuali condotte - colpose o dolose – dei fornitori o dei Gestori interni della Segnalazione attuate in eventuale difformità alle regole previste nelle predette policies di FOR.MA – sono inoltre **sanzionate** secondo i rispettivi contratti.

- **<u>Settore di attività e scala (intesa come "volume") del trattamento</u>**:

  la probabilità di verificarsi del rischio è **BASSA**, perché

  i) il settore economico in cui opera FOR.MA non appartiene alla categoria delle infrastrutture critiche nazionali,
  ii) FOR.MA svolge attività ed è generalmente esposto al rischio di cyberattacchi;
  iii) FOR.MA non è stata destinataria storicamente di violazioni che abbiano causato gravi impatti di tipo RID sui dati;
  iv) il volume di dati di whistleblowing è tendenzialmente ridotto, poiché il numero di segnalazioni annue prevedibili non è elevato (stima: 4-5), alla luce del fatto che esistono tutta una serie di procedure interne a presidio dei processi di business (*Modello Organizzativo 231*, Modello Organizzativo Privacy, Sistema di Gestione ISO 9001).

ARE DI VALUTAZIONE	**LIVELLO**
Rete e risorse tecniche	BASSO
Processi/Procedure relative ai trattamenti dei dati	BASSO
Parti/Persone coinvolte nel trattamento dei dati	BASSO
Settore di business e scala del trattamento	BASSO
VALUTAZIONE COMPLESSIVA DI PROBABILITÀ	**BASSO**

Alla luce del suddetto Assessment, il complessivo esito medio della valutazione di PROBABILITÀ è: **BASSO**.

***

Utilizzando, pertanto, i risultati della valutazione di GRAVITÀ di impatto (alto) e di PROBABILITÀ di impatto (basso), il RISCHIO FINALE relativo al trattamento dei dati di whistleblowing di FOR.MA è calcolato come segue:

		GRAVITA' DI IMPATTO		
		Basso	Medio	Alto/Molto Alto
PROBABILITA' DI IMPATTO	Basso			**X**
	Medio			
	Alto			

*

Inoltre, rispetto alle tre macrocategorie di rischio sopra individuate, ovvero

- ✓ perdita di **riservatezza** (divulgazione/accesso non autorizzato),
- ✓ perdita di **integrità** (modifica indesiderata),
- ✓ perdita di **disponibilità** (distruzione, perdita, scomparsa dei dati - inclusa indisponibilità momentanea),

sono state individuate le potenziali correlate **minacce**, classificandole le stesse a seconda della fonte della minaccia, come di seguito riportato:

Classi (in relazione alla fonte della minaccia)	
U	comportamento umano
S	eventi relativi agli strumenti
C	eventi relativi al contesto (fisico-ambientale)

Di seguito alcuni esempi delle **minacce** rilevanti ai fini del rischio (per un elenco completo delle stesse si rinvia al file ***MINACCE_EFFETTI*** (incluso a propria volta nel più ampio file del Titolare denominato ***ASSESSMENT ENISA-ISDP***) sub ***Allegato G***:

Fonte	**Minaccia**	**Rischio**	**Casistiche**	
U	Errori umani di dipendenti (es per scarsa formazione/consapevolezza/competenza, disattenzione, incuria)	RID	Errori umani nella gestione della sicurezza della sala CED	Accesso non autorizzato all'hardware, agli strumenti o ai dati Esempio: Impostazioni di autorizzazione errate (gli utenti Case Manager ricevono l'accesso a tutti i casi anziché solo a quelli che dovrebbero essere a loro accessibili). Uso improprio del Portale SaaS da parte del Case Manager che elimina accidentalmente i dati.
U	Cambio mansione, dimissioni di dipendente non presidiato	R	Utilizzo illecito di informazioni da parte di utenti non più abilitati ad accedere a strumenti	
U	Comportamenti sleali o fraudolenti dei dipendenti	RIDC		Le credenziali del personale autorizzato per accedere ai comportamenti illeciti segnalati sono rubate/accessibili a persone non autorizzate. Uso improprio del Portale SaaS da parte del Case Manager che elimina intenzionalmente i dati.
U	Attacco di ingegneria sociale per carpire informazioni	R	Simulazione/ furto di identità	Sciopero

U	Affidamento di attività di progetto/servizio a fornitori	RIDC	Rischi di guasto tecnico al terzo provider di rete virtualizzata in cloud	Rischio di indisponibilità dei dati trattati da terzi providers (a causa di guasti, malfunzionamenti, interruzioni dei servizi)
S	Infezioni da virus/malware	RID		Attacchi Hacker
S	Errori/vulnerabilità nel software utilizzato	RID		Utilizzo di software non più supportato.
S	Sistema di autenticazione/profilazione/gestione delle credenziali non adeguato	RD		Procedure di registrazione non sicure da parte dei Case Manager.
S	Trasmissione di dati in maniera non sicura	RIC		Utilizzo di crittografia TLS non più supportata.
S	Guasto o malfunzionamento hardware	IDC	Indisponibilità, malfunzionamento o degrado degli strumenti o di singoli componenti	
S	Mancata collaborazione dei responsabili esterni o dei terzi co-titolari	C	Mancata adesione alle proposte di nomina o di accordi sui trattamenti	Inadempimento agli obblighi previsti dalle nomine o dagli accordi sui trattamenti
C	Evento naturale catastrofico	IDC	Incendio	Fulmine
C	Interruzioni o non disponibilità della rete (guasti)	DC	Danni sulle linee o ai sistemi interni di comunicazione	Guasto tecnico al terzo provider di rete di connettività
C	Interruzioni o non disponibilità dei sistemi complementari	ID	Disturbi elettromagnetici, sbalzi di tensione	Interruzioni / indisponibilità dell'energia e/o dei sistemi ausiliari (UPS, generatori, ecc.).

*

7. MISURE PREVISTE PER AFFRONTARE I RISCHI

7.1. MISURE DI SICUREZZA DI FOR.MA

Le singole **misure di protezione** previste e applicate dal Titolare per gestire (cioè, prevenire e/o ridurre) gli specifici tre **rischi** (riservatezza, disponibilità, integrità) sopra individuati nonché il rischio di non conformità privacy per aspetti diversi da quello di protezione dei dati personali (articolo 35, paragrafo 7, lettera d) e considerando 90 del GDPR) sono **indicate:**

i) nella ***Procedura Whistleblowing*** nonché
ii) nei ***documenti aziendali*** (procedure, linee guida, eventi formativi) ***in materia di sicurezza fisica e logica nonché*** nel sistema documentale predisposto ***in materia di privacy*** (da intendersi come qui interamente richiamati).

Si osserva, peraltro, che:

- la **funzionalità di scarico dati (download) dal Portale/Software sia inibita di default**, ed eventualmente riattivata solo caso per caso dall'Admin; sicche le suddette separate misure di FOR.MA vengono a rilevare, in concreto, solo per l'eventuale caso in cui i Case Manager effettuino tale download;

- le misure FOR.MA suddette possono rilevare, inoltre, per l'ipotesi in cui una Segnalazione pervenga al Titolare tramite un canale diverso dal Portale/Software.

***

7.2. MISURE DI SICUREZZA DI EQS

Inoltre, con riguardo ai rischi di sicurezza delle informazioni, il terzo sub-fornitore del Portale SaaS (EQS Group S.R.L), utilizzato in trasparenza dal fornitore ADACTA:

- ha implementato un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) conseguendo la ***Certificazione ISO 27001*** per soddisfare i più elevati requisiti di sicurezza e le normative sulla protezione dei dati riconosciute a livello internazionale. Inoltre, gli elementi chiave, come i data center, dove sono custoditi i dati operativi e di backup, sono certificati secondo la medesima norma garantendo la protezione e la prevenzione dei rischi a livello organizzativo.

  Copia della certificazione è stata messa a disposizione del Titolare. Un efficace ISMS certificato ISO 27001 soddisfa numerosi elementi chiave previsti di requisiti normativi sulla privacy dei dati, tra cui vari obblighi presentati nel GDPR dell'UE.

- Il Portale SaaS è conforme ai requisiti del GDPR nella fornitura dei suoi servizi, soddisfando i suoi obblighi in aree quali la crittografia, la cancellazione, la rettifica, l'anonimizzatine, il trasferimento, l'accesso e il trattamento dei dati personali.

  Il sistema EQS Integrity Line supporta attivamente i Case Manager nell'adempimento dei requisiti di privacy dei dati con varie funzionalità quali avvisi dinamici, impostazioni di disclaimer, anonimizzazione, archiviazione, audit trail e altro ancora;
- ha istituito un Comitato per la sicurezza informatica, il quale ha formalizzato un elenco di processi/istruzioni che costituisce una parte significativa dell'ISMS;
- si è sottoposto ad un ***Audit European Privacy Seal***, con esito positivo. Il relativo Report di audit è pubblico (visionabile sul sito internet www.eqs.com);
- ha eseguito una ***DPIA sul Portale SaaS***, i cui contenuti sono stati assorbiti nella presente DPIA. In particolare, la DPIA di EQS coincide con il *documento* ***Elenco misure tecniche e organizzative di*** **EQS** (EQS-Misure tecniche organizzative Servizi Cloud TOMs_it-en_211210_) – *sul punto vedasi capitolo 7.2.15*.

  La DPIA di EQS è visionabile in **Allegato D**. La DPIA di EQS ha ottenuto il parere favorevole del DPO di EQS GROUP AG.

7.2.1. Crittografia dei dati

L'architettura del sistema (EQS Integrity Line) applica una tecnologia di crittografia all'avanguardia per i dati in trasferimento e i dati inattivi. Al fine di garantire la riservatezza delle segnalazioni, tutte le informazioni riservate (contenuto del caso, allegati, ecc.) sono crittografate. Ciò impedisce l'accesso non autorizzato di terzi e amministratori di server.

Il concetto di crittografia consente l'applicazione di un rigoroso principio di "necessità di sapere". Gli utenti che non hanno alcun permesso di accedere ai casi segnalati non hanno accesso crittografato agli stessi. Ciò assicura la confidenzialità delle segnalazioni anche nel caso improbabile di un errore del software.

Solo gli utenti con il ruolo "User Admin" hanno accesso crittografico a tutti i casi, al fine di assegnare permessi a nuovi utenti o modificare eventuali permessi già assegnati (nuovo personale, mutate competenze, ecc.).

Ogni sistema client è crittografato con chiavi di crittografia individuali.

Né EQS né il provider di hosting (sub-subfornitore di EQS) né ADACTA (con ruolo di Admin) hanno accesso alle chiavi di crittografia necessarie per decrittografare i dati e quindi non possono leggere le informazioni sensibili negli incidenti segnalati.

Dati a riposo

Una procedura basata su chiave pubblica-privata (basato su standard OpenPGP) è applicata e le chiavi sono conservate in un archivio chiavi su server. Ciò permette l'uso di chiavi di cifratura più lunghe. Le chiavi degli utenti individuali sono protette da password univoche assegnate a ciascun utente (applicate tramite varie procedure)

Tutti i dati personali sensibili sono crittografati nel database tramite le seguenti misure di sicurezza:

› Crittografia asimmetrica: algoritmo RSA a 2048 bit (per utenti front end).

› Crittografia simmetrica: algoritmo RSA a 2048 bit (per utenti back end).

› FOR.MA può autonomamente definire la policy di password (lettere, maiuscole e minuscole, caratteri speciali, numeri, e la lunghezza password).

Vengono utilizzati due livelli di chiavi di crittografia: la "chiave master" e le "chiavi di crittografia dei dati". La chiave master è molto grande ma lenta da crittografare/decodificare. Questa chiave viene utilizzata per proteggere le chiavi dei dati. Le chiavi dati sono più brevi (e più veloci) ma vengono cambiate regolarmente.

La chiave master e le chiavi dei dati sono crittografate in modo tale che solo un utente amministratore/gestore del caso può decrittografare e leggere i rapporti inviati. Nemmeno gli sviluppatori IT di EQS sono in grado di decrittare e leggere i report inviati.

Le password degli utenti amministratori non sono memorizzate nel sistema in chiaro. Viene memorizzato solo un hash salted pbkdf2 (Password-Based Key Derivation Function 2) delle password.

AWS (sub-subfornitore di EQS) esegue anche la crittografia dei dati memorizzati a livello hardware, che è AES256.

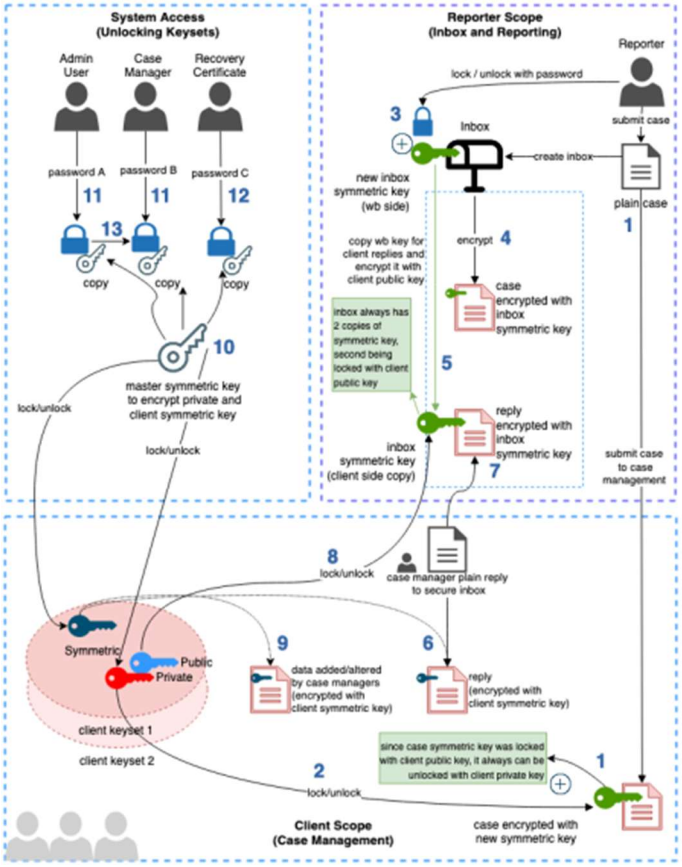


Figura 3: Gestione delle chiavi

Dati in transito

Sono adottate le seguenti misure di controllo della trasmissione dei dati tra server e cliente tra server e server per garantire che i dati personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante la trasmissione o il trasporto elettronico:

- Tutto il traffico tra server e client (es. browser web) è crittografato con Amazon AWS Certificate Manager (ACM) che gestisce la connessione HTTPS Transport Layer Security TLS (standard 1.2) con TLS 1.2.

  L'ultimo certificato SSL/TLS emesso e gestito da ACM è Amazon Trust SHA256.

  Il termine SHA256 si riferisce all'algoritmo di hash utilizzato per la firma digitale del certificato. SHA256 è una funzione di hash crittografico della famiglia SHA-2 (Secure Hash Algorithm 2) e viene utilizzato per garantire l'integrità dei dati e prevenire modifiche non autorizzate durante il processo di verifica del certificato.

  Alcuni vantaggi specifici di utilizzare certificati SSL con algoritmo SHA256 includono:
  - ✓ Maggiore sicurezza: SHA256 è un algoritmo di hash più sicuro rispetto ai precedenti come SHA-1, che è stato deprecato a causa di vulnerabilità note.
  - ✓ Compatibilità con la maggior parte dei browser: i certificati SSL SHA256 sono compatibili con tutti i principali browser web e dispositivi.
- Autenticità e fiducia: I certificati SSL Amazon Trust sono emessi da una Certificate Authority (CA) affidabile, che garantisce l'autenticità del sito web. Il traffico interno tra i server è crittografato con certificati RSA forti di almeno 2048 bit.
- Il server è configurato in modo tale da evitare c.d. "fallback" verso versioni di protocollo obsolete e insicure (es.TLS_FALLBACK_SCSV).
- Gestione delle chiavi di crittografia: il client genera la chiave di crittografia master. Durante il primo accesso dell'utente (amministratore), la crittografia del sistema viene inizializzata utilizzando le credenziali dell'utente amministratore. In quel momento viene generato il set di chiavi del client (chiavi RSA e AES) e quindi le chiavi private vengono crittografate con la chiave master (AES) generata. La chiave master è bloccata con la password del primo utente.
- Ritenzione cifrata delle chiavi di password durante la sessione (AES-256).
- Tutte le attività di accesso degli utenti e le attività di gestione dei casi vengono registrate in un Audit Trail.

Valutazione: accettabile.

7.2.2. Anonimizzazione dati

Il sistema (Portale SaaS) consente tramite la funzionalità "Anonymise" di effettuare tale operazione sul contenuto del report e quindi di rendere invisibili agli utenti tutti i dati personali e/o identificativi delle persone.

Valutazione: accettabile.

7.2.3. Partizionamento dati

Crittografia per singola segnalazione. Ogni caso ha una chiave separata in modo che solo gli utenti autorizzati possano accedere ai dati.

Inoltre, il sistema Portale SaaS è archiviato in server virtualmente separati su data center certificati ISO 27001 in:

Configurazione predefinita: Cloud pubblico (AWS) / Francoforte, Germania
Il centro di hosting Amazon Web Services EMEA è una struttura indipendente conforme al GDPR.
Tutti i dati sui server sono criptati: né EQS né il sub-provider di hosting AWS hanno accesso ai dati criptati.
Certificazioni AWS disponibili:

- ISO/IEC 27001:2013;
- ISO/IEC 27017:2015;
- ISO/IEC 27018:2019;
- ISO/IEC 27701:2019;
- ISO/IEC 22301:2019;
- ISO/IEC 9001:2015;
- CSA STAR CCM v4;
- ISAE 3402 SOC 2 Tipo II (disponibile su AWS Artifact).

Per maggiori info: https://aws.amazon.com/compliance/soc-faqs/ https://aws.amazon.com/de/compliance/isocertified/.

Valutazione: accettabile.

7.2.4. Controllo logico degli accessi

Il Portale è sviluppato su 3 livelli (o "tier"): presentazione (tier che gestisce le interazioni degli utenti, come segnalante e Case Manager), logica (tier che gestisce la logica dell'applicazione), dati (tier che contiene i dati del Portale).

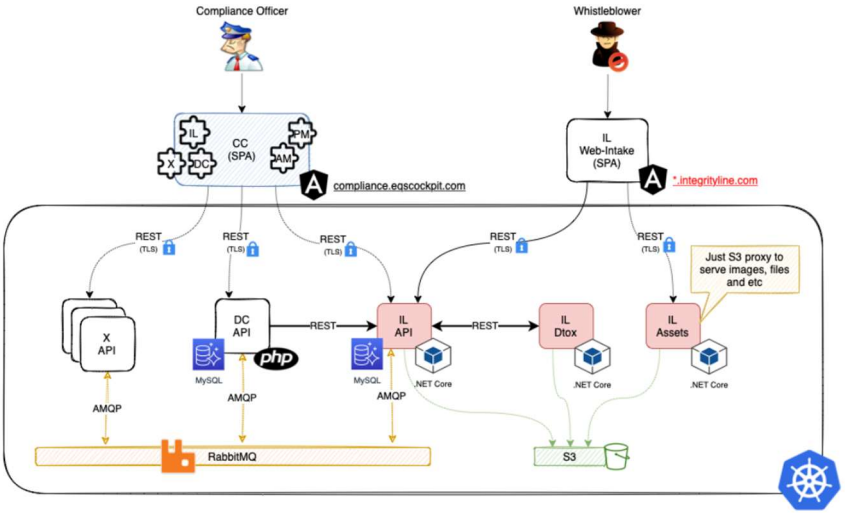


Figura 4: Architettura di sistema di alto livello

Il sistema distingue i ruoli che organizzano l'esecuzione dei diversi compiti del sistema, nonché le autorizzazioni su un caso che possono essere assegnate ai Case Manager.

Ci sono 3 ruoli disponibili sul sistema (EQS Integrity Line). I ruoli Case Manager e User Admin e Content Admin possono essere assegnati agli utenti.

› I Case Manager sono in grado di vedere e lavorare sui casi.

› Gli User Admin gestiscono:

- ✓ i permessi degli utenti del back-end

  (creazione, disattivazione, assegnazione o rimozione dei permessi, facoltà o divieto di scaricare le segnalazioni al di fuori del Portale SaaS, ...);
- ✓ i testi sul Portale SaaS;

  (esempio: domande del questionario al segnalante nel front-end, elenco paesi, elenco possibili materie della segnalazione, ecc.);
- ✓ l'ambiente di back-end

  (es. configurare la possibilità di invio di una segnalazione da determinati paesi inclusi in elenco e se in tal caso la segnalazione può essere o meno anonima, configurare il numero di lingue attive, inserire nel back-end i testi destinati ai segnalanti nelle lingue attive, configurare le tipologie generali di stato di avanzamento di una segnalazione quali ad esempio "da esaminare", "in corso di esame", "decisa", "archiviata" e simili).

Uno stesso utente di back-end può assumere contemporaneamente il ruolo di Case Manager e di eventuale Admin, diventando così SuperAdmin.

Per maggiori dettagli si vedano i controlli A.9.2.1, A.9.4.1 nel documento ***Information Security Management System (ISMS)*** di EQS GROUP AG.

L'accesso alle macchine virtuali di produzione da parte dei dipendenti di EQS può avvenire unicamente con il gestore di sessioni AWS e con le autorizzazioni appropriate.

Valutazione: accettabile.

7.2.5. Tracciabilità (registrazione)

Ci sono due audit trail sul sistema (EQS Integrity Line) per registrare tutte le azioni rilevanti svolte dagli utenti del Portale SaaS.

Il primo è l'audit trail visibile agli User Admin, che permette di vedere tutte le azioni e gli eventi registrati relativi a un utente. Questo audit trail è visibile solo agli utenti amministratori di sistema e può essere filtrato per distinguere meglio le varie categorie operazioni eseguite dall'utente o le singole operazioni su un caso.

Il secondo audit trail è collegato al rapporto / caso e consente di registrare tutte le azioni relative a un singolo rapporto / caso. Questo audit trail è visibile a ogni utente che ha accesso al singolo caso e l'autorizzazione a visionare l'Audit Trail.

Valutazione: accettabile.

7.2.6. Archiviazione dati

Il sistema EQS Integrity Line consente l'archiviazione di report e allegati (modalità di sola lettura) non appena sono stati chiusi e resi anonimi.

I casi vengono esaminati dal team competente e vengono archiviati una volta che il caso viene chiuso e vengono definiti i rimedi. Le pratiche sono rese anonime prima dell'archiviazione e conservate nel sistema come previsto dalla legge.

Valutazione: accettabile.

7.2.7. Sicurezza dei documenti cartacei

Di solito non viene utilizzata documentazione cartacea. Il tutto avviene direttamente sul Case Management del sistema EQS Integrity Line.
Nel caso in cui venga utilizzata la carta, è in atto una politica di distruzione della documentazione riservata, interna e riservata.

Valutazione: accettabile.

7.2.8. Minimizzazione dei dati personali

Il questionario e le raccomandazioni sul processo di segnalazione (compresa la pagina iniziale e la sezione FAQ) istruiscono gli informatori a limitare la quantità di dati personali lasciati al momento della presentazione della segnalazione.

Le ***Nomine degli Autorizzati*** e la ***Procedura Whistleblowing*** prevedono che i dati non necessari vengano resi anonimi o cancellati senza indugio.

Vedere anche il capitolo "anonimizzazione/cancellazione dei dati".

Valutazione: accettabile.

7.2.9. Sicurezza del funzionamento del sistema

Livelli di crittografia, ruoli utente separati e diritti per utente configurabili dal back-end del Portale SaaS, garantiscono standard di sicurezza molto elevati e riducono il rischio di esfiltrazione di dati.

L'hosting, l'alloggio, lo sviluppo e la manutenzione del sistema in uso sono certificati ISO 27001.

Il sistema fornisce versioni IT regolari su base annuale e patch di sicurezza ogni due settimane e ad evento se necessario. AWS gestisce automaticamente gli aggiornamenti di sicurezza delle patch minori, mentre le versioni maggiori richiedono un intervento manuale a causa della necessità di eseguire test e altre verifiche.

Valutazione: accettabile.

7.2.10. Protezione da software dannoso

Il sistema (EQS Integrity Line) fornisce uno scanner di virus e malware, che esegue la scansione di tutti i file caricati alla ricerca di malware e virus prima di salvarli nel sistema.
In ottica di prevenzione dai virus zero-day, EQS ha sviluppato il proprio sistema antivirus "File Detox". File Detox analizza i file caricati nel sistema e crea una nuova versione di questi in cui vengono copiate solo le informazioni che vengono valutate come sicure (a titolo esemplificativo, file di documenti (ad esempio, word) in un nuovo documento pdf; file audio (ad esempio, file mp3) in un nuovo file mp3; file video (ad esempio file mp4) in un nuovo file mp4; file immagine (ad esempio, jpg e png) in un nuovo file jpg).
Questo processo rimuove i virus (anche quelli di tipo zero-day), le macro e il codice di backup dai file. Inoltre, i metadati vengono rimossi durante il processo, eliminando la data di creazione, l'autore e qualsiasi altro dato relativo al file caricato. File Detox supporta i formati di file più utilizzati.
È attivo il rilevamento automatico del malware per tutte le workstation, in particolare per gli amministratori dei server.
Valutazione: accettabile.

7.2.11. Gestione della postazione di lavoro

L'utente Admin e Case Manager utilizza un doppio fattore di autenticazione (2FA) per connettersi al suo profilo di autorizzazione. Il fattore di doppia autenticazione è comunicato all'utente via e-mail.

Inoltre, se l'utente non esegue alcuna azione nel suo spazio di lavoro, la sessione termina dopo 5 minuti e deve riconnettersi per continuare il suo lavoro.

Sviluppo e manutenzione sicuri Vedi controllo A.14.2.6 e successivi del documento ***ISMS*** di EQS GROUP AG.

Valutazione: accettabile.

7.2.12. Sicurezza del sito web EQS

Vedere Sicurezza delle informazioni A.9.1.2 del documento ***ISMS*** di EQS per un elenco dettagliato delle restrizioni di accesso.

Alcune misure di sicurezza:

- Utilizzo della crittografia **TLS** (https://) e del concetto di crittografia.
- Procedure di accesso sicure.
- **Monitoraggio delle operazioni**, inclusa misure contro gli attacchi DDoS atte ad impedire un knockout critico del server.
- **Test di penetrazione interni** condotti in base alla metodologia OWASP Top 10:2021, comprendendo hacking manuale e scansione automatizzata delle vulnerabilità. Inoltre, i test di penetrazione esterni vengono eseguiti da un fornitore di servizi interno su base annuale.
  Questi test di penetrazione sono eseguiti da professionisti della sicurezza informatica con una conoscenza di lunga data del mercato della sicurezza informatica.

Figura 5: Qualsys SSL test di 9 agosto 2022; Internal Penetration Test

- **Memorizzazione dei dati di ogni cliente in un database condiviso nel server MySQL Aurora e separazione dei tenant basata su discriminatori**. Lato web server, ogni sistema client viene creato in sottodomini separati. L'interpretazione dei sottodomini è gestita a livello di web server (nginx).

Valutazione: accettabile.

7.2.13. Backup

Generalità

Per proteggere dalla perdita di dati, garantire la continuità delle operazioni di elaborazione dei dati e fornire la possibilità di ripristinare le operazioni di elaborazione dei dati dopo un evento critico, il backup del sistema (EQS Integrity Line) si trova in un data center di backup geo-separato (certificato ISO27001). Sono previste e implementate procedure per consentire il ripristino del sistema entro un ragionevole periodo di tempo dopo un evento critico (in base a specifici accordi contrattuali stipulati il fornitore del Portale SaaS).

Il backup viene gestito, come segue: Cloud pubblico - AWS: I backup giornalieri completi vengono eseguiti tramite servizio Aurora.

Aurora è un servizio di database relazionale sviluppato da Amazon Web Services (AWS) che offre compatibilità con MySQL e PostgreSQL, ma con prestazioni significativamente superiori rispetto ai tradizionali database open-source. Amazon Aurora è progettato per essere altamente scalabile, sicuro, e affidabile, supportando sia carichi di lavoro transazionali che di analisi.

Le principali caratteristiche di Amazon Aurora includono:

- ✓ Alta disponibilità e affidabilità: Aurora replica automaticamente i dati in più zone di disponibilità (AZ) e offre un failover rapido, garantendo la continuità del servizio in caso di guasti.
- ✓ Scalabilità: Aurora può scalare automaticamente in base alle esigenze, gestendo fino a 64 terabyte di storage e supportando decine di migliaia di connessioni simultanee.
- ✓ Prestazioni elevate: Con prestazioni fino a 5 volte superiori a MySQL e 2 volte superiori a PostgreSQL, offre un'architettura che sfrutta il parallelismo per migliorare le prestazioni di lettura e scrittura.
- ✓ Sicurezza: Aurora integra opzioni di crittografia dei dati sia a riposo che in transito, ed è compatibile con i controlli di accesso IAM di AWS.
- ✓ Gestione semplificata: Non è necessario gestire l'infrastruttura sottostante, poiché Aurora si occupa della gestione automatica delle patch, dei backup e delle operazioni di failover

Ogni giorno (standard: ogni 12 ore) viene eseguito un backup del database. I backup del sistema vengono eseguiti regolarmente (standard: ogni 24 ore).

Il **backup giornaliero viene conservato per 90 giorni** dopodiché viene eliminato.

La ridondanza viene gestita come segue: Cloud pubblico - AWS: tutti i dati di Francoforte sono replicati tra 3 data center in Germania. Viene utilizzato il livello di astrazione Amazon.

Le procedure di Disaster Recovery usate da EQS vengono testate regolarmente (almeno due volte l'anno).

Piano di continuità operativa (BCP) disaster recovery di AWS

- ✓ Il Piano di continuità aziendale AWS illustra le misure da adottare per evitare e ridurre l'impatto di eventi ambientali. Descrive inoltre nel dettaglio le diverse fasi da seguire prima, durante o dopo il verificarsi di un evento.
- ✓ Il Piano di continuità aziendale prevede dei test, tra cui la simulazione di scenari diversi. Durante e in seguito a tali test, AWS documenta le prestazioni di persone e processi, le azioni correttive e le lezioni apprese, con l'obiettivo di migliorare continuamente la reazione agli eventi di sicurezza.

Valutazione: accettabile.

7.2.14. Manutenzione

I controlli di accesso fisico vengono utilizzati per impedire a persone non autorizzate di accedere ai server del sub-fornitore.

EQS utilizza data center certificati ISO 27001 e terze parti per fornire la manutenzione fisica dell'hardware.

I data center in cui è archiviata EQS Integrity Line includono i seguenti controlli di sicurezza:

› I server di sistema si trovano in contenitori di server certificati ISO27001 nella UE

› Sistema di lettura elettronica delle tessere di accesso

› Gestione delle chiavi / documentazione del titolare delle chiavi

› Recinzione a palizzata

› Esterno del massiccio edificio in cemento armato

› Guardie di sicurezza 24x7x365 con personale

› Servizio di vigilanza, reception con accesso obbligatorio per tutti i visitatori

› Sistema di allarme antifurto

› Panning, inclinazione e zoom a infrarossi interni ed esterni CCTV Sistema di gestione dell'edificio monitorato

› Scanner biometrico

› Videosorveglianza permanente dell'impianto, inclusi tutti gli ingressi e le sale server, con archiviazione delle registrazioni su hard disk

› Rilevamento movimento e intrusioni

› Monitoraggio di tutte le porte e parti importanti del data center

› Videosorveglianza di sale server (pre)sale server

› Autenticazione di tutti i visitatori del data center

Garanzia di disponibilità e sicurezza dell'infrastruttura di rete

Per garantire i livelli di disponibilità richiesti, l'infrastruttura del server fisico è progettata in modo ridondante. Ciò significa che ogni componente del cluster (switch, server delle applicazioni o server di archiviazione) può guastarsi senza avere un impatto importante sul servizio fornito.

Valutazione: accettabile.

7.2.15. Elaborazione dei contratti

Uno specifico allegato su Trattamento Dati ***Accordo per la designazione del Responsabile del Trattamento ai sensi dell'Art. 28 del Regolamento Europeo 2016/679 (GDPR) - Basato sulle Clausole Contrattuali Tipo pubblicate dalla Decisione di Esecuzione (EU) 2021/915*** fa parte del contratto con il terzo fornitore ADACTA coinvolto nella gestione del software/Portale SaaS.

Sono inoltre applicati i seguenti documenti al contratto con il terzo fornitore ADACTA:

- ***Condizioni Generali ADACTA (Italia)***
- ***Offerta tecnica – economica denominata "Proposta Software Gestione Digitale Segnalazioni"***

Valutazione: Accettabile.

Il contratto con il terzo fornitore ADACTA (di cui è subfornitore EQS Group SRL) coinvolto nella gestione del software/Portale SaaS include uno specifico allegato sul Trattamento Dati ***Allegato al trattamento dei dati per i servizi Cloud di EQS (ai sensi dell'art. 28 GDPR) – Basato sulle Clausole Contrattuali Tipo pubblicate dalla Decisione di Esecuzione (EU) 2021/915***).

Al contratto con il terzo fornitore EQS GROUP SRL sono inoltre applicati i seguenti documenti:

- ***Termini ADACTA-EQS (Italia)***
- ***Misure Tecniche e Organizzative per i Servizi Cloud di EQS***

I suddetti documenti sono disponibili in https://www.eqs.com/it/about-eqs/condizioni-generali/?switchedLanguageTo=it.

Valutazione: Accettabile.

7.2.16. Sicurezza della rete

Il sistema stesso Portala SaaS si basa su un sistema su cui si basano le varie interfacce (front end, back end, traduzione). Per le comunicazioni con il database, è usato un framework ORM. Le richieste e le risposte dal web server passano attraverso una WAF (applicazione web) e quindi attraverso un comune firewall.

Lo sviluppo del sistema e il suo continuo mantenimento della sicurezza seguono linee guida comuni per la produzione di applicazioni sicure sin dalla fase di progettazione, come le linee guida e i principi Open Web Application Security Project (OWASP Top 10:2021). Il sistema viene sottoposto a una scansione di conformità a ogni rilascio del software.

Valutazione: accettabile.

7.2.17. Controllo dell'accesso fisico

I server sono gestiti da AWS con le più alte misure di sicurezza fisica e né ADACTA nè EQS possono in alcun modo accedere all'edificio in cui sono collocati.
Esse includono (cfr. https://aws.amazon.com/de/compliance/data-center/controls/).

Accesso ai data center dei dipendenti

AWS offre l'accesso fisico ai data center solo ai dipendenti autorizzati. Tutti i dipendenti che devono accedere al data center devono prima richiedere l'autorizzazione all'accesso e fornire una motivazione aziendale valida. L'autorizzazione di tali richieste viene fatta sulla base del principio del privilegio minimo, secondo cui è necessario specificare il layer del data center a cui il dipendente deve accedere, e ha una durata limitata nel tempo. Le richieste vengono vagliate e approvate da personale autorizzato e l'accesso viene revocato alla sua scadenza. Una volta ottenuta l'autorizzazione, le persone possono accedere solo alle aree consentite.

Accesso al data center di terzi

L'accesso di terzi deve essere richiesto da dipendenti AWS designati che devono chiedere l'autorizzazione e fornire una motivazione aziendale valida. L'autorizzazione di tali richieste viene fatta sulla base del principio del privilegio minimo, secondo cui è necessario specificare il layer del data center a cui il dipendente deve accedere, e ha una durata limitata nel tempo.
Tali richieste vengono approvate da personale autorizzato e l'accesso viene revocato alla sua scadenza. Una volta ottenuta l'autorizzazione, le persone possono accedere solo alle aree consentite. Tutti coloro che sono autorizzati all'accesso con il badge visitatore devono presentare al proprio arrivo un documento d'identità, firmare al momento dell'ingresso ed essere scortati dal personale autorizzato.

Accesso ai data center AWS GovCloud

L'accesso fisico ai data center nella regione AWS GovCloud (Stati Uniti) è consentito solo ai dipendenti che hanno dimostrato di essere in possesso di cittadinanza statunitense.

Monitoraggio e registrazione di log

Revisione degli accessi al data center

Gli accessi ai data center vengono regolarmente rivisti. L'accesso è revocato automaticamente quando il profilo di un dipendente viene eliminato dal sistema delle risorse umane di Amazon. Inoltre, quando l'accesso di un dipendente o di un appaltatore scade in base alla richiesta di durata approvata, alla persona viene revocato l'accesso, anche se continua a essere alle dipendenze di Amazon.

Log degli accessi ai data center

Ogni accesso fisico ai data center AWS è registrato, controllato e archiviato. In base alle esigenze, AWS mette in relazione le informazioni ottenute da sistemi logici e fisici di monitoraggio per migliorare la sicurezza.

Monitoraggio degli accessi ai data center

Monitoriamo i data center grazie ai nostri Security Operations Center (SOC) globali che monitorano, valutano e mettono in pratica programmi di sicurezza. Tali centri offrono un supporto globale 24 ore su 24, 7 giorni su 7, gestendo e monitorando le attività di accesso ai data center e offrendo ai team locali e ad altri team di supporto gli strumenti per reagire a incidenti di sicurezza e valutare, analizzare, consultarsi e fornire una risposta.

Sorveglianza e rilevamento

Videocamere a circuito chiuso (CCTV)

I punti di accesso fisico alle sale server sono controllati da videocamere a circuito chiuso (CCTV). Le immagini vengono archiviate in base a requisiti legali e di conformità.

Punti di accesso ai data center

L'accesso fisico viene controllato presso i punti di ingresso dell'edificio dal personale addetto alla sicurezza che si avvale di sistemi di sorveglianza, di rilevamento delle intrusioni e di altri dispositivi elettronici. Per accedere ai data center il personale autorizzato utilizza meccanismi di autenticazione a più fattori. Gli ingressi alle sale server sono protetti da dispositivi che attivano un allarme e una risposta agli incidenti nel caso in cui la porta rimanga aperta o venga forzata.

Rilevamento delle intrusioni

Nel layer dei dati vengono installati sistemi elettronici di rilevamento delle intrusioni che monitorano, rilevano e avvisano automaticamente il personale preposto della presenza di incidenti di sicurezza. I punti di ingresso e di uscita verso le sale server sono protetti da dispositivi che richiedono a ogni persona l'autenticazione a più fattori prima di autorizzare l'entrata e il badge prima dell'uscita. Questi dispositivi emettono allarmi quando la porta viene aperta forzatamente senza autenticazione, tenuta aperta o aperta per l'uscita durante un'emergenza. I dispositivi di allarme delle porte sono anche configurati per rilevare istanze in cui una persona entra nel layer di dati senza fornire l'autenticazione a più fattori, oppure esce senza aver utilizzato il badge in maniera adeguata. Gli allarmi vengono immediatamente inviati ai Security Operations Center di AWS 24 ore su 24, 7 giorni su 7, per registrazione, analisi e risposta immediate.

alle sedi AWS

Valutazione: accettabile.

7.2.18. Monitoraggio dell'attività della rete EQS

Ogni singolo server client virtuale è un'installazione separata di un sistema operativo Debian Linux.

Il Portale SaaS (Integrity Line) utilizza server standard e componenti di sistema per fornire le sue funzionalità che vengono regolarmente testate internamente e tramite audit esterni (es. Report tipo ISAE 3000).

L'elenco sottostante distingue tra servizi altamente o relativamente integrati:

<u>Servizi altamente integrati</u>

- MySQL/Maria database che conserva tutte le informazioni.
- Apache webserver per recapitare tutti i contenuti al browser.
- PHP come linguaggio di programmazione/scripting.
- GnuPG per autenticazione utenti tramite informazioni confidenziali cifrate.
- Asterisk per segnalazione telefonica.

<u>Servizi meno integrati</u>

- Postifix per invio di notifiche e-mail.
- Icinga per monitoring dei parametri di funzionamento dell'host e del Portale.
- Cron per eseguire tasks schedulati, come l'escalation.
- VPN per scopi di backup e monitoraggio.

Valutazione: accettabile.

7.2.19. Sicurezza hardware EQS

La politica di sicurezza dell'hardware EQS include i seguenti principi:

A.11.2 Equipaggiamento

A.11.2.1 Localizzazione e protezione delle apparecchiature

Le apparecchiature devono essere posizionate e protette per ridurre i rischi derivanti da minacce e pericoli ambientali e opportunità di accesso non autorizzato.

A.11.2.2 Utilità di supporto

Le apparecchiature devono essere protette da interruzioni di corrente e altre interruzioni causate da guasti nelle utenze di supporto.

A.11.2.3 Sicurezza del cablaggio

I cavi di alimentazione e telecomunicazioni che trasportano dati o servizi informativi di supporto devono essere protetti da intercettazioni, interferenze o danni.

A.11.2.4 Manutenzione delle apparecchiature

L'attrezzatura deve essere sottoposta a corretta manutenzione per garantirne la disponibilità e l'integrità continua.

A.11.2.5 Rimozione di beni

Apparecchiature, informazioni o software non devono essere portati fuori sede senza previa autorizzazione.

A.11.2.6 Sicurezza delle apparecchiature e dei beni fuori sede

La sicurezza dovrebbe essere applicata alle risorse fuori sede tenendo conto dei diversi rischi del lavoro al di fuori dei locali dell'organizzazione.

A.11.2.7 Smaltimento o riutilizzo di sicurezza delle apparecchiature

Tutti gli elementi dell'apparecchiatura contenenti supporti di memorizzazione devono essere verificati per garantire che tutti i dati sensibili e il software concesso in licenza siano stati rimossi o sovrascritti in modo sicuro prima dello smaltimento o del riutilizzo.

A.11.2.8 Apparecchiature per utenti non presidiati

Gli utenti devono garantire che le apparecchiature incustodite dispongano di una protezione adeguata.

A.11.2.9 Criteri di cancellazione scrivania e schermo trasparente

Dovrebbero essere adottate una chiara policy desk per documenti e supporti di memorizzazione rimovibili e una policy clear screen per le strutture di elaborazione delle informazioni.

Valutazione: accettabile.

7.2.20. Localizzazione data center

I dati vengono archiviati in data center geograficamente separati, il cui rischio di disastri ambientali è minimo.
È garantita la residenza dei dati nel data center scelto. Nessun dato viene trasferito tra i data center utilizzati per ospitare l'applicazione, tranne che per scopi di backup dei dati. Sul punto vedasi il capitolo 7.2.3 "Partizionamento dati", nonché quanto segue:

Selezione del sito

Prima di scegliere una sede, il sub-fornitore AWS esegue valutazioni preliminari di natura ambientale e geografica. AWS sceglie attentamente la sede dei propri data center per limitare il rischio di danni di natura ambientale, come alluvioni, condizioni climatiche estreme e attività sismiche. Le zone di disponibilità sono costruite in modo da essere indipendenti e fisicamente separate le une dalle altre.

Ridondanza

I data center sono stati progettati per anticipare e tollerare i guasti mantenendo gli stessi livelli di servizio. In caso di problemi, i processi automatizzati spostano il traffico dall'area colpita. Le applicazioni strategiche sono distribuite seguendo una configurazione N+1 standard; in questo modo, in caso di problemi al data center, viene garantita una capacità sufficiente per permettere al traffico di essere distribuito sui siti rimanenti.

Valutazione: accettabile.

7.2.21. Protezione da fonti di rischio non umane

Certificazione ISO 27001 dei processi di EQS GROUP AG per evitare tutte le fonti di rischio non umane.

(controllo A.11.1.4) Protezione contro le minacce esterne e ambientali. Viene progettata e applicata la protezione fisica contro disastri naturali, attacchi dannosi o incidenti.

Vedere la sezione "7.2.14 Manutenzione" della presente DPIA per ulteriori analisi.

Valutazione: accettabile.

7.2.22. Organizzazione

Separazione dei ruoli e dei profili di autorizzazione in base al concetto "need-to-know". I ruoli sono definiti nella ***Procedura Whistleblowing***.

Il DPO di EQS è responsabile delle attività di vigilanza di competenza della stessa relative alla protezione dei dati.

Il Fornitore EQS ha, inoltre, istituito un comitato direttivo dell'ISMS composto dalla direzione, dal dipartimento di sicurezza delle informazioni e da tutto il personale coinvolto nel mantenimento e nel miglioramento dell'ISMS.

Valutazione: accettabile.

7.2.23. Politica

L'obiettivo e le regole di protezione dei dati sono definiti nell'***Informativa Whistleblowing*** di FOR.MA il cui scopo è garantire che il trattamento dei dati raccolti tramite l'uso del Portale SaaS in relazione alle segnalazioni sia conforme con le leggi e i regolamenti applicabili.

Valutazione: accettabile.

7.2.24. Integrare la protezione dei dati nei progetti

Il fornitore EQS è un fornitore globale di soluzioni software in cui i dati personali sono coinvolti da 20 anni. La valutazione della protezione della privacy è integrata in ogni progetto di soluzioni software nuove e attuali (Politica ISMS di EQS Group – Secure Development Policy) per i quali vengono attuate policy formali di sicurezza delle informazioni, aggiornate regolarmente – rispetto ai concetti di sicurezza implementati – da sviluppatori senior congiuntamente al team di sviluppo.

FOR.MA applica un approccio di privacy by design by default fin dalla progettazione delle nuove iniziative di trattamento dei dati, e anche il progetto di gestione dei dati del whistleblowing si è attenuto a tale filosofia.

Valutazione: accettabile.

7.2.25. Gestione dei data breach

A livello di rete EQS, sono attivi controlli per monitorare le attività svolte nel software in uso per trattare i dati (incluso il Portale SaaS).

EQS Group AG dispone di una politica sulla violazione dei dati i cui termini sono inclusi nelle clausole contrattuali stipulate con FOR.MA.

EQS GROUP AG dispone di una specifica ***Procedura di Gestione Incidenti***, visibile in Internet a tutti i dipendenti EQS. Gli incidenti sono riportati e gestiti in tale ambito. Gli incidenti possono essere segnalati direttamente dai dipendenti tramite un form dedicato. In base all'incidente un team specifico viene coinvolto nella relativa gestione.

Valutazione: accettabile.

7.2.26. Gestione del personale

La consapevolezza del personale EQS viene aumentata attraverso webinar regolari e sessioni di e-learning, inclusi nuovi e vecchi dipendenti.

Materiale e informazioni sulla protezione dei dati sono disponibili per i dipendenti EQS sulla intranet.

La valutazione del personale comprende anche la verifica periodica della corretta gestione dei dati.

L'audit regolare del fornitore EQS sul proprio personale dipendente include anche la consapevolezza dei dipendenti.

I candidati vengono "valutati" (nella misura consentita dalla legge applicabile nel paese di destinazione come, a titolo esemplificativo, verifica del casellario giudiziale), e prima di entrare in azienda, devono sottoscrivere obblighi di riservatezza e segretezza dei dati.

Infine, viene verificata l'identità dei nuovi dipendenti tramite documento d'identità personale.

Valutazione: accettabile.

7.2.27. Relazioni con terze parti

Le relazioni con le terze parti (sub-fornitori di EQS, n.d.r.) sono regolarmente monitorate tramite audit interni ed esterni.

I contratti in essere includono accordi sulla protezione dei dati personali e livelli di servizio per garantire la conformità con le leggi e i regolamenti applicabili.

Il Service Level Agreement generale di EQS per i servizi cloud si applica e definisce l'uptime e i tempi di risposta in caso di errori e tempi di servizio. Esso è disponibile in https://www.eqs.com/en-us/about-eqs/terms-and-conditions.

Le informazioni sulle terze parti sono costantemente aggiornate.

Inoltre, non vi è accesso delle terze parti ai dati degli interessati.

Valutazione: accettabile.

7.2.28. Supervisione (Vigilanza)

Si veda al capitolo Gestione del personale circa la supervisione via e-learning e le regolari verifiche (annuali).

EQS inoltre fornisce procedure e prassi per ottenere un'organizzazione in grado di gestire e controllare la protezione dei dati in essa detenuti.

Valutazione: accettabile.

7.2.29. Gestione delle modifiche del software

Sono state adottate procedure di gestione delle modifiche del Portale SaaS Integrity Line che assicurano:

- la separazione dell'ambiente di sviluppo dall'ambiente di test e dall'ambiente produttivo;
- la documentazione delle richieste di modifica e dei test in un sistema di gestione dei problemi;
- la revisione del codice da parte di uno sviluppatore diverso da colui che ha originariamente scritto il codice;
- un'accurata fase di testing del codice, effettuata sia attraverso test manuali che automatizzati, comprendente diverse forme di test, tra cui test di sistema, di integrazione, di accettazione da parte dell'utente e di accettazione operativa. La realizzazione dei test avviene in diversi ambienti prima del rilascio nell'ambiente di produzione:
    a. ambiente di sviluppo da parte degli ingegneri del software;
    b. ambiente QA da parte del product management;
- lo sviluppo e il collaudo del Portale SaaS Integrity Line nell'UE.

Valutazione: accettabile.

7.2.30. Gestione dei rischi per la privacy

Il Portale SaaS Integrity Line si basa sul concetto di privacy by design e di default, per il quale il monitoraggio del trattamento dei dati è fondamentale.
L'uso della crittografia (segnalazione per segnalazione) e in generale della crittografia di dati inattivi e in transito riducono al minimo il rischio di accedere al contenuto dei dati trapelati personale non autorizzato.
Le valutazioni formali dei rischi vengono effettuate regolarmente e la policy di sicurezza informatica, le valutazioni dei rischi e l'elenco delle istruzioni vengono discussi regolarmente e aggiornati in caso di modifiche.
Con cadenza bisettimanale, tutti i dipendenti EQS partecipano a riunioni interne in cui vengono discusse le esigenze di sviluppo del sistema.

Valutazione: accettabile.

7.2.31. Traduzione automatica

Per i servizi di traduzione automatica il Portale SaaS Integrity Line utilizza l'API Microsoft Translator Text V3.0.

- Nessuna tracciabilità delle richieste al sistema EQS Integrity Line;
- I dati non vengono mai scritti nella memoria persistente (solo CPU e RAM).
- I dati vengono crittografati durante il transito da e verso l'API.
- I dati non vengono mai trasferiti al di fuori dell'UE.

Questa opzione può essere disattivata in qualsiasi momento.

Figura 6: Traduzione automatica

Valutazione: accettabile.

7.2.32. Controlli di accesso per gli utenti

Policy di sicurezza delle password degli Utenti

Il sistema è predefinito con un criterio di password che soddisfa gli standard di buona pratica in materia di password. Il criterio delle password può essere definito dal cliente. È possibile configurare i seguenti parametri:

- Lunghezza minima della password;
- La password deve contenere:
  - almeno 1 lettera maiuscola e 1 minuscola;
  - almeno 1 numero;
  - almeno 1 carattere speciale.

Per una maggiore sicurezza, il sistema supporta l'autenticazione a due fattori via e-mail.

Recupero delle password degli Utenti

Gli utenti creati per l'accesso al Portale SaaS Integrity Line non possono reimpostare autonomamente la password, ma richiede l'interazione con un utente amministratore sul lato client. Il flusso di lavoro è composto dalle seguenti fasi:

1. Il Case manager fa clic su Password dimenticata.
2. Il Case manager (che ha dimenticato la password) riceve un link che gli/le permette di scegliere una nuova password per la chiave master.
3. Tutti gli esistenti Case manager ricevono una notifica che indica che c'è un utente in attesa di reset conferma nella linea di integrità.
4. Un utente amministratore accede alla gestione dei casi e vede che c'è un utente che ha dimenticato la propria password.
5. L'utente amministratore approva la reimpostazione della password nell'amministrazione utenti (Data Center), che crea una copia della sua chiave master per l'utente che ha dimenticato la password. La password fornita dall'utente target viene quindi utilizzata per bloccare la chiave master con la sua nuova password.
6. Il Case manager (che ha dimenticato la password) riceve una notifica quando viene concesso l'accesso a Integrity Line.

Timeout sessione

Nel sistema di gestione dei casi e nella casella di posta elettronica protetta è implementato un sistema di timeout automatico della sessione degli Utenti dopo 30 minuti.

Canale di comunicazione

Quando un segnalante invia una segnalazione tramite il Web Intake, gli viene fornito un ID segnalazione generato dal sistema e gli viene chiesto di creare una password specifica per la segnalazione. L'ID della segnalazione e la password vengono utilizzati per accedere al sistema e comunicare successivamente con il Case manager.
I requisiti di complessità della password possono essere configurati nel sistema (caratteri minimi consentiti, caratteri maiuscoli/minuscoli obbligatori, numeri obbligatori, caratteri speciali obbligatori).

Procedure di accesso sicure

Il Portale SaaS Integrity Line permette a FOR.MA di configurare i parametri di protezione brute force (si applica sia all'accesso web che alla gestione dei casi):

- Numero massimo di accessi non riusciti prima della sospensione dell'account.
- Numero di minuti di sospensione dell'account.

Gestione e configurazione degli utenti

FOR.MA supervisiona la gestione degli utenti (Data Center) e la configurazione (impostazioni di personalizzazione) del sistema. Il personale di EQS Group non ha accesso al sistema dopo che è stato configurato ed è operativo.
Tutti gli utenti del sistema hanno un login unico che non deve essere condiviso con nessuno.
Quando viene creato un utente amministratore, gli vengono automaticamente inviati il login (indirizzo e-mail) e una password temporanea limitata nel tempo. Quando l'utente amministratore accede al sistema per la prima volta, la password deve essere modificata con un'altra password conforme ai requisiti di complessità della password configurati nel sistema.
Se un utente amministratore dimentica la password, una nuova password temporanea limitata nel tempo deve essere inviata manualmente da un altro amministratore del sistema per evitare il rischio di accesso non autorizzato al sistema. La password temporanea scade dopo un periodo predefinito (personalizzabile).
I diritti di accesso e privilegi degli utenti amministratori sono personalizzabili in modo che ogni utente acceda alle sole funzionalità specifiche del sistema necessarie per svolgere il proprio lavoro.

Valutazione: accettabile.

7.2.33. Configurazione informatica

FOR.MA ha implementato diverse misure per garantire l'anonimato dei dipendenti durante l'invio delle segnalazioni tramite dispositivi e reti aziendali. In particolare:

- La registrazione e il tracciamento degli indirizzi IP dei dipendenti all'interno della rete aziendale sono stati disattivati.
- La cronologia del browser relativa all'accesso ai collegamenti web del Portale SaaS Integrity Line (Web Intake URL) è stata disattivata.

Per garantire la massima riservatezza, ai dipendenti è inoltre consigliato di inviare le segnalazioni utilizzando dispositivi privati al di fuori della rete aziendale, con un accesso facilitato al link di Portale SaaS Integrity Line anche dall'esterno dell'organizzazione.
Inoltre, per garantire una comunicazione efficace, FOR.MA ha inserito nella white list del firewall aziendale gli indirizzi e-mail di notifica del sistema (eqscockpit@eqs.com), assicurando così la corretta ricezione delle notifiche da parte degli utenti e dei Case manager.
Infine, è stata prestata particolare attenzione all'utilizzo di estensioni del browser durante la gestione dei casi, assicurandosi che eventuali componenti aggiuntivi, come quelli di traduzione automatica, non interferiscano con la corretta visualizzazione dei contenuti.

Valutazione: accettabile.

7.3. VALUTAZIONE GRANULARE E QUADRO SINOTTICO DEI RISCHI E DELLE MISURE ESPLICITATO DA EQS

I rischi valutati da EQS e conseguentemente da FOR.MA in relazione al trattamento in esame, sono i seguenti.

7.3.1. Accesso illegittimo ai dati (violazione della riservatezza)

Principali **impatti** sugli interessati se si verificasse il rischio:

- I dati personali o l'autore della segnalazione possono essere divulgati al pubblico (violazione della riservatezza dei dati), con il rischio di ritorsioni verso l'autore della segnalazione.
- Rischio di ostacolare le indagini sulle condotte illecite segnalate se le persone accusate sono a conoscenza delle segnalazioni.
- Danno reputazionale se il segreto aziendale, comprese le violazioni della legge, è pubblicamente noto.
- Qualsiasi responsabilità per illeciti operati dalla Società.

Principali **minacce** che potrebbero portare al rischio:

- (S) Procedure di registrazione non sicure da parte dei Case manager.
- (S) Attacchi hacker.
- (S) Difetti di sicurezza.
- (S) Utilizzo di software o crittografia TLS non più supportato/a.

Fonti di rischio:

- (U) Le credenziali del personale autorizzato per accedere ai comportamenti illeciti segnalati sono rubate/accessibili a persone non autorizzate.
- (S) Problemi di sicurezza dell'infrastruttura.

- (U) Impostazioni di autorizzazione errate (gli utenti ricevono l'accesso a tutti i casi anziché solo a quelli che dovrebbero essere a loro accessibili).

Controlli pianificati individuati che contribuiscono ad affrontare il rischio (= **Misure**):

Crittografia dei dati (7.2.1), Anonimizzazione dei dati (7.2.2.), Partizionamento dei dati (7.2.3.), Controllo logico degli accessi (7.2.4.), Tracciabilità (logging) (7.2.5.), Archiviazione Dati (7.2.6.), Sicurezza dei documenti cartacei (7.2.7.), Minimizzazione dei dati personali (7.2.8), Sicurezza del funzionamento del sistema (7.2.9.), Protezione da software dannoso (7.2.10.), Gestione delle postazioni di lavoro (7.2.11.), Sicurezza del sito Web EQS (7.2.12.), Backup (7.2.13.), Manutenzione (7.2.14.), Elaborazione dei Contratti di trattamento dati (7.2.15), Sicurezza della rete (7.2.16), Controllo dell'accesso fisico (7.2.17), Monitoraggio dell'attività di rete EQS (7.2.18.), Sicurezza dell'hardware (7.2.19.), Localizzazione data center (7.2.20.), Protezione da fonti di rischio non umane (7.2.21.), Organizzazione (7.3.22.), Politica (7.2.23), Integrare la protezione dei dati nei progetti (7.2.24.), Gestione dei dati breach (7.2.25.), Gestione del personale (7.2.26.), Relazione con terze parti (7.2.27.), Supervisione (7.2.28.), Gestione delle modifiche del software (7.2.29), Gestione dei rischi per la privacy (7.2.30), Traduzione automatica (7.2.31), Controlli di accesso per gli utenti (7.2.32), Configurazione informatica (7.2.33), Valutazione granulare e Quadro sinottico dei rischi e delle misure esplicitato da EQS (7.3).

Gravità stimata del rischio, soprattutto in base ai potenziali impatti e ai controlli pianificati:

Limitato sulla base dei seguenti controlli:

- Certificazione ISO 270001 di EQS e relativi subappaltatori nello sviluppo, manutenzione, supporto, housing e hosting del sistema (Portale SaaS)
- Le misure di sicurezza includono controlli regolari della rete e test di penetrazione
- Misure di hardening
- Requisiti di sicurezza della password: autenticazione forte o a 2 fattori (ruoli di back-end)
- Sensibilizzazione periodica del personale dedicato
- Definizione e distinzione dei ruoli in base al concetto "need-to-know".

Probabilità stimata del rischio, in particolare per quanto riguarda le minacce, le fonti di rischio ei controlli pianificati:

Limitato, sulla base della valutazione di cui sopra.

Valutazione: accettabile

7.3.2. Modifica indesiderata dei dati (violazione dell'integrità)

Principali **impatti** sugli interessati se si verificasse il rischio:

- Rischio di ostacolare le indagini sulle condotte scorrette segnalate se le persone accusate sono a conoscenza delle segnalazioni.
- Perdita di dati.

Principali **minacce** che potrebbero portare al rischio:

- (S) Procedure di registrazione non sicure da parte dei Case manager.
- (U) Uso improprio del Portale SaaS da parte del Case Manager che elimina accidentalmente o intenzionalmente i dati.

Fonti di rischio:

- (U) Le credenziali del personale autorizzato per accedere ai comportamenti illeciti segnalati sono rubate/accessibili a persone non autorizzate.
- (U) Impostazioni dei permessi errate (gli utenti hanno accesso a tutti i casi anziché solo a quelli che dovrebbero essere a lui accessibili).

Controlli individuati che contribuiscono ad affrontare il rischio (= **Misure**):

Crittografia dei dati (7.2.1.), Anonimizzazione dei dati (7.2.2.), Partizionamento dei dati (7.2.3.), Controllo dell'accesso logico (7.2.4.), Tracciabilità (logging) (7.2.5.), Dati di archivio (7.2.6.), Minimizzazione dati personali (7.2.8.), Sicurezza del funzionamento del sistema (7.2.9.), Protezione da software dannoso (7.2.10.), Sicurezza del sito Web (7.2.12.), Manutenzione (7.2.14.), Sicurezza della rete (7.2.16.), Controllo fisico accessi (7.2.17.), Monitoraggio dell'attività di rete (7.2.18.), Sicurezza hardware (7.2.19.), Prevenzione delle fonti di rischio (7.2.21), Organizzazione (7.2.22.), Policy (7.2.23.), Gestione del personale (7.2.26.), Relazioni con terze parti (7.2.27), Supervisione (7.2.28), Gestione delle

modifiche del software (7.2.29), Gestione dei rischi per la privacy (7.2.30), Traduzione automatica (7.2.31), Controlli di accesso per gli utenti (7.2.32), Configurazione informatica (7.2.33).

Gravità stimata del rischio, soprattutto in base ai potenziali impatti e ai controlli pianificati:

Limitato, in base all'ISMS di EQS in atto, ai controlli e alla consapevolezza.

Probabilità stimata del rischio, soprattutto in relazione a minacce, fonti di rischio e controlli pianificati:

Limitato

Valutazione: Accettabile

7.3.3. Scomparsa dei dati (violazione della disponibilità)

Principali **impatti** sugli interessati se si verificasse il rischio:

- Rischio di ostacolare le indagini sulle condotte scorrette segnalate se le persone accusate sono a conoscenza delle segnalazioni.
- Perdita di dati.

Principali **minacce** che potrebbero portare al rischio:

- (S) Attacchi hacker.
- (U) Uso improprio del Portale SaaS da parte del Case Manager.

Quali sono le **fonti** di rischio?

- (U) Le credenziali del personale autorizzato per accedere ai comportamenti illeciti segnalati sono rubate/accessibili a persone non autorizzate.
- (U) Impostazioni dei permessi errate (gli utenti ricevono l'accesso a tutti i casi anziché solo a quelli che dovrebbero essere a lui accessibili).
- (S) Problemi di sicurezza dell'infrastruttura.

Controlli individuati che contribuiscono ad affrontare il rischio (= **Misure**):

Crittografia dei dati (7.2.1.), Anonimizzazione dei dati (7.2.2.), Partizionamento dei dati (7.2.3.), Controllo logico dell'accesso (7.2.4.), Tracciabilità (logging) (7.2.5.), Archiviazione Dati (7.2.6.), Minimizzazione dati (7.2.8.), Sicurezza operativa del sistema (7.2.9), Protezione da software dannoso (7.2.10.), Sicurezza del sito Web (7.2.12.), Backup (7.2.13.), 7.3.15 Contratti di trattamento dati (7.2.15), Sicurezza della rete (7.2.16.), Controllo dell'accesso fisico (7.2.17.), Sicurezza hardware (7.2.19.), Localizzazione data center (7.2.20.), Protezione da fonti di rischio non umane (7.2.21.), Organizzazione (7.2.22.), Gestione delle modifiche del software (7.2.29), Gestione dei rischi per la privacy (7.2.30), Traduzione automatica (7.2.31), Controlli di accesso per gli utenti (7.2.32), Configurazione informatica (7.2.33).

Gravità stimata del rischio, soprattutto in base ai potenziali impatti e ai controlli pianificati?

Limitato,

Probabilità stimata del rischio, soprattutto in relazione a minacce, fonti di rischio e controlli pianificati?

Limitato.

Valutazione: Accettabile.

*

La **interconnessione** tra i principali rischi rilevanti per il trattamento, i potenziali impatti, le minacce e le fonti di minaccia, considerati/e nella **DPIA dal terzo fornitore EQS** e quindi altresì in questa sede da FOR.MA, e le misure di protezione applicate, sono rappresentate nella seguente **Tabella**:

IMPATTI POTENZIALI	Accesso illegittimo ai dati (riservatezza)	Modifica indesiderata dei dati (integrità)	Perdita dei dati (disponibilità)
Comunicazione di dati personali o del segnalante	▪		
Rischio di ostacolare le investigazioni	▪	▪	▪
Danno reputazionale se il segreto diviene noto	▪		
Quasiasi responsabilità per cattiva condotta	▪		
Perdita dei dati		▪	▪

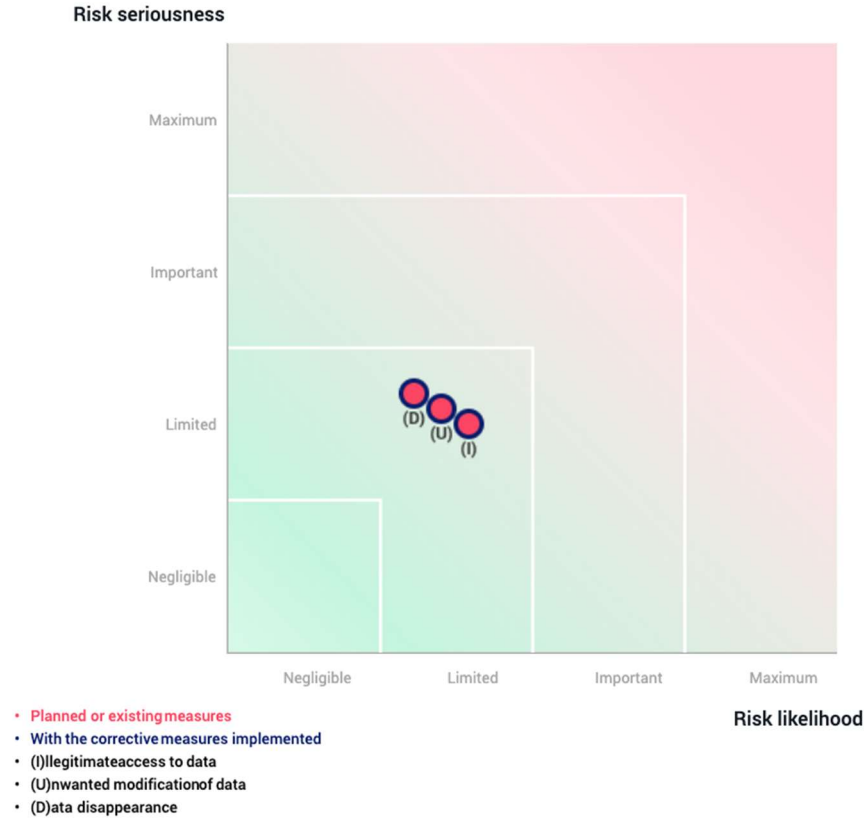
MINACCE			
Procedure registrazione non sicure	▪	▪	▪
Attacchi hacker	▪		▪
Difetti di sicurezza	▪		
Utilizzo di software non più supportato o crittografi	▪		
Uso improprio del canale di segnalazione		▪	▪

RISORSE			
Credenziali autorizzate del personale	▪	▪	▪
Problemi di sicurezza delle infrastrutture	▪	▪	▪
Impostazioni di autorizzazione errate	▪	▪	▪

MISURE			
Crittografia dei dati	▪	▪	▪
Partizionamento dei dati	▪	▪	▪
Anonimizzazione dei dati	▪	▪	▪
Sicurezza del funzionamento del sistema	▪	▪	▪
Controllo logico degli accessi	▪	▪	▪
Quantità minima di personle	▪	▪	▪
Sicurezza del sito web EQS	▪	▪	▪
Contratto di elaborazione	▪	▪	▪
Protezione da software dannoso	▪	▪	▪
Sicurezza dell'hardware	▪	▪	▪
Tracciabilità (logging)	▪	▪	▪
Monitoraggio dell'attività della rete	▪	▪	
Manutenzione	▪	▪	
Gestione della postazione di lavoro	▪		
Gestione del personale	▪	▪	
Gestione violazione dei dati personali	▪		
Sicurezza dei documenti cartacei	▪		
Backups	▪		▪
Sicurezza della rete	▪	▪	▪
Archiviazione dei dati	▪	▪	▪
Controlllo degli accessi fisici	▪	▪	▪
Evitamento fonti di rischio	▪	▪	▪
Protezione contro fnti di rischio non umane	▪		▪
Organizzazione	▪	▪	▪
Procedure	▪	▪	
Gestione rischi privacy	▪	▪	
Integrazione protezione privacy	▪		
Relazione con terze parti	▪	▪	
Supervisione	▪	▪	
Minimizzazione dei dati personali	▪	▪	▪
Localizzazione data center	▪	▪	▪
Protezione da fonti di rischio non umane	▪	▪	▪
Politica	▪	▪	
Secure Development Life Cycle			▪
Traduzione automatica		▪	
Controlli di accesso per gli utenti	▪	▪	▪
Configurazione informatica	▪	▪	▪

Severità	Probabilità	Severità	Probabilità	Severità	Probabilità
Limitata	Limitata	Limitata	Limitata	Limitata	Limitata

e la seguente mappa di validazione del rischio, che viene qui fatta propria da parte di FOR.MA:



(laddove la scala dei livelli possibili di rischio usata da EQS è composta di 4 livelli: Negligible, Limited, Important e Maximum).

7.4. MISURE DI SICUREZZA DI ADACTA

Il trattamento dei dati personali avviene **esclusivamente attraverso il Portale SaaS**.

Nell'ipotesi eccezionale in cui si renda necessario un trattamento al di fuori del Portale SaaS, purché espressamente consentito dalle regole previste dalla ***Procedura Whistleblowing*** (ad esempio, nel caso in cui si debba scaricare localmente uno o più allegati o dati dal Portale SaaS), il terzo fornitore ADACTA ha adottato le **misure di protezione e sicurezza delle informazioni previste nell'Allegato E**.

8. MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL GDPR

8.1. Gap Analysis

Il Titolare ha **individuato e valutato** i **rischi di (non) conformità** diversi quindi da quelli di protezione dei dati.

In particolare, tali rischi - gestiti di volta in volta tramite le regole previste dalla ***Procedura Whistleblowing*** - riguardano:

- l'eventuale mancata informativa whistleblowing ex art. 13-14 GDPR alle diverse categorie di interessati;
- l'eventuale mancata acquisizione dell'approvazione (consenso) del Segnalante circa il contenuto della trascrizione della Segnalazione eseguita dai Case Manager a seguito di una Segnalazione che sia avvenuta tramite una modalità non scritta;
- la mancata tempestiva cancellazione, da parte dei Case Manager, dei dati personali non pertinenti alla Segnalazione o superflui rispetto alle finalità di gestione della Segnalazione stessa.

8.2. Diritti dell'interessato

Con riguardo al criterio WP248 concernente le **misure che contribuiscono alla tutela dei diritti degli interessati** in materia di whistleblowing (*NB: diritti diversi da quelli come sopra già analizzati attinenti alla riservatezza, integrità e disponibilità dei dati personali*), il Titolare ritiene che vengano in rilievo i seguenti diritti:

- ✓ informazioni fornite all'interessato (articoli 12, 13 e 14);
- ✓ diritto di accesso (articolo 15);
- ✓ diritto alla rettifica, cancellazione (articoli 16, 17 e 19);
- ✓ diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21).
- ✓ (se il Segnalante ha rivelato la propria identità, o, in caso di Segnalazione anonima, ciò è possibile anche senza rivelare l'identità) diritto di controllare, correggere e approvare il testo di una segnalazione che sia stata trascritta dal Titolare dopo essere pervenuta in una forma che non prevede l'utilizzo di una forma scritta (es. tramite incontro personale, telefonata o altra forma orale non registrata, posta ordinaria); la revoca del consenso non pregiudica la liceità del trattamento e della comunicazione effettuata su base volontaria fino alla revoca;
- ✓ diritto di ricevere la notifica di una violazione dei dati nel caso in cui la stessa comporti un elevato rischio per i diritti o le libertà fondamentali degli interessati.

Come detto, inoltre, è prevista la cancellazione (automatica o manuale) dei dati di whistleblowing, conservati dal Titolare, allo scadere del termine di relativo utilizzo individuato nel ***Registro dei trattamenti***.

8.3. Garanzie supplementari adeguate

Ai fini della **gestione** dei rischi di conformità GDPR diversi da quelli di protezione dei dati, FOR.MA applica le seguenti regole:

- L'***Informativa Whistleblowing*** è messa preventivamente a disposizione degli interessati potenziali segnalanti sia all'interno del Portale SaaS sia tramite distribuzione nelle altre forme previste dalla ***Procedura Whistleblowing*** (tra cui la pubblicazione in una sezione separata del sito internet del Titolare, la messa a disposizione all'ingresso della sede centrale e di ogni unità locale di FOR.MA) nonché tramite la circolazione di un avviso scritto ai destinatari circa l'avvenuta messa a disposizione della stessa Procedura anche a loro favore.).

  Eventuali **facilitatori** della singola segnalazione e/o altri **soggetti tutelati** sono resi destinatari dell'***Informativa Whistleblowing*** da parte del Titolare sia all'interno del Portale SaaS, sia tramite la pubblicazione in una sezione separata del sito internet del Titolare, sia tramite la messa a disposizione all'ingresso della sede centrale e di ogni unità locale di FOR.MA) nonché tramite la circolazione di un avviso scritto ai destinatari circa l'avvenuta messa a disposizione della stessa Procedura anche a loro favore e in occasione del loro primo contatto con i Case Manager, che possa fare seguito al ricevimento della segnalazione (es. audizione da remoto, incontro personale).

  Infine, la persona **segnalata** (c.d. "soggetto coinvolto") riceve l'***Informativa privacy*** durante lo svolgimento dell'istruttoria relativa alla segnalazione da parte di OdV, salvo possibilità di discrezionale posticipo di tale comunicazione nel caso in cui lo stesso si renda ragionevolmente necessario per evitare qualsiasi ostruzione all'istruttoria da parte dell'interessato (es. distruzione od occultamento di prove).

- È attiva la ***Procedura di gestione dell'esercizio dei diritti degli interessati***. Nello specifico, mediante tale Procedura sono chiaramente **individuati i ruoli e le responsabilità** nonché le modalità e tempistiche di gestione delle richieste di esercizio dei diritti pervenute al Titolare da parte degli interessati.

  Rispetto alla ***Procedura di gestione dell'esercizio dei diritti degli interessati***, sono qui di seguito fornite alcune ulteriori valutazioni:

  - <u>Diritto di accesso e portabilità dei dati</u>

    Il diritto di accesso e di portabilità dei dati personali è indicato nell'**Informativa Whistleblowing** e in essa sono indicati i dati di contatto del DPO per esercitare tali diritti. Tali diritti si applicano ai segnalanti così come ai testimoni e facilitatori e alle persone segnalate. I Case Manager valuteranno le richieste per garantire che i dati di qualsiasi persona sia anonimizzato prima che i dati siano condivisi con qualsiasi interessato richiedete l'accesso. I dati sono condivisi in un formato leggibile da un umano e da un elaboratore. Esiste alcun obbligo legale di conservare i dati per 5 anni dalla data di decisione finale sulla segnalazione, e sarà quindi possibile riscontrare una richiesta di cancellazione pervenuta al Titolare entro tale termine.
  - <u>Diritto di rettifica e cancellazione</u>

    I segnalanti possono richiedere in qualsiasi momento che i Case Manager (che si occupano della segnalazione) rettifichino o cancellino i dati. I Case Manager sono in grado di eseguire tali operazioni all'interno del Portale SaaS di gestione delle segnalazioni. Il diritto di rettifica e di cancellazione è indicato

nell'***Informativa Whistleblowing*** e sono indicati i dati di contatto del Titolare e del DPO per esercitare tali diritti.

I Case Manager possono in qualsiasi momento rettificare o cancellare informazioni comprendenti loro dati personali, salvo la legge applicabile espressamente non lo impedisca.

Nel caso in cui prima della richiesta di rettifica o cancellazione oggettivamente rilevante vi sia stata già una eventuale comunicazione di dati personali alle Autorità competenti da parte del Titolare, quest'ultimo provvede senza ritardo ad aggiornare la comunicazione agli originali destinatari.

- Diritto di limitazione e di opposizione

  I segnalanti e gli altri interessati possono richiedere in qualsiasi momento che i Case Manager (che si occupano della segnalazione) limitino il trattamento o sospendano lo stesso per motivi derivanti dalla propria situazione particolare. I Case Manager sono in grado di eseguire tali operazioni all'interno del Portale SaaS di gestione delle segnalazioni. Inoltre, il diritto di limitazione e di opposizione al trattamento è indicato nell'***Informativa Whistleblowing*** e sono indicati i dati di contatto del DPO per esercitare tali diritti.

- Consenso

  Nel caso in cui il consenso del segnalante sia necessario ai sensi del Decreto Whistleblowing (e cioè allorché una segnalazione pervenga in forma orale, o tramite incontro personale con il segnalante o tramite e-mail o raccomandata a.r., e il relativo contenuto venga quindi trascritto da parte dei Gestori della Segnalazione per essere poi sottoposto alla approvazione scritta del segnalante, oppure in caso di rivelazione dell'identità del segnalante e/o di qualsiasi altra informazione da cui possa evincersi – direttamente o indirettamente – la sua identità a persone diverse dal Case manager, come prescritto dal Decreto Whistleblowing), **il consenso del segnalante è ottenuto tramite modalità tracciate (es. una comunicazione e-mail** tramite il Portale SaaS). Senza consenso non è possibile dare seguito alla segnalazione.

I suddetti diritti, nel caso specifico dei trattamenti Whistleblowing, saranno, come riportato nella Informativa Whistleblowing, gestiti osservando quanto segue nel rispetto di quanto previsto con l'Art 13 del D.lgs. 24/23 e l'Ar 2-undecies del D.lgs. 196/03:

Come regola generale, gli Interessati hanno il diritto, in qualunque momento, di ottenere la conferma dell'esistenza o meno dei dati forniti, chiedere, nelle forme previste dall'ordinamento, la rettifica dei dati personali inesatti e l'integrazione di quelli incompleti e di esercitare ogni altro diritto ai sensi degli artt. da 15 a 22 del GDPR, indirizzando la propria richiesta all'e-mail: **info@formazionemantova.it**.
Qualora invece gli Interessati ritengano che il trattamento sia avvenuto in modo non conforme al GDPR e al D.Lgs. 196/2003, potranno rivolgersi al Garante per la Protezione dei dati Personali (Garante Privacy, www.garanteprivacy.it), ai sensi dell'art. 77 del GDPR.

Con specifico riferimento ai trattamenti dati condotti dal Titolare come richiesto dalle normative applicabili in materia di whistleblowing, ai sensi dell'art. 13 par.3 del D.lgs. 24/23, si precisa che si procederà rispettando i limiti di quanto previsto dall'art. 2-undecies del D.lgs. 196/03, che prevede che i diritti di cui agli articoli da 15 a 22 del GDPR non possono essere esercitati con richiesta al Titolare del trattamento ovvero con reclamo ai sensi dell'art. 77 del GDPR presso il Garante Privacy qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del D.lgs. 24/23.

Ai sensi dell'art.2-undecies par.3 del D.lgs. 196/03, il Titolare informa gli Interessati che, nei suddetti casi i diritti sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del GDPR.

L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo dal Titolare all'Interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui alla riservatezza dell'identità di chi segnala. In tali casi, i diritti dell'Interessato possono essere esercitati anche tramite il Garante Privacy con le modalità di cui all'art. 160 del D.lgs. 196/03. In tale ipotesi, il Garante Privacy informa l'Interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'Interessato di proporre ricorso giurisdizionale.

Ove l'Interessato abbia dato il consenso nei casi indicati nella sezione "Ulteriori precisazioni sulle basi legali" dell'Informativa Whistleblowing, ha il diritto di revocare tale consenso in qualsiasi momento, senza che però ciò pregiudichi la liceità del trattamento, basato sul consenso, effettuato prima della revoca.

Tali diritti di cui agli artt. da 15 a 22 del GDPR e nonché la revoca del consenso ove prestato, possono essere esercitati con richiesta indirizzata a: **info@formazionemantova.it**.

- È implementata dal Titolare una ***Procedura privacy by design*** che garantisce la tutela della privacy degli interessati, fin dalla progettazione, nel caso di futura progettazione e implementazione eventuali nuovi sistemi e/o contratti di trattamento dati whistleblowing che possano sostanzialmente modificare quelli attuali. Gli impatti di tali modifiche dei sistemi vengono previamente analizzati ed eventuali requisiti privacy specifici vengono resi parte del capitolato di progetto.

- In conformità a quanto previsto dall'art. 4 del Decreto Whistleblowing, i canali di segnalazione di FOR.MA sono stati attivati, sentite le rappresentanze sindacali.

- Gli **obblighi del Titolare** sono chiaramente **identificati e regolati** tramite la ***Procedura Whistleblowing*** e la ***Informativa Whistleblowing***. Entrambi i documenti sono pubblicati nel Portale/Software adottato dal Titolare.

- Inoltre, un ***accordo contrattuale con il terzo fornitore del Portale SaaS*** (EQS GROUP SRL) e un ***accordo contrattuale con il terzo distributore autorizzato del Portale SaaS***, ***sviluppato da EQS, autorizzata a configurare e svolgere servizio di help desk di primo livello*** (ADACTA) definiscono le obbligazioni per essere conformi alla normativa applicabile.

- Sono state adottate specifiche misure tecniche e organizzative volte a garantire che i dati **non** possano essere **utilizzati** per adottare decisioni o intraprendere **altre azioni** ulteriori rispetto a quelle dichiarate nelle Informative. È infatti garantita la "separazione funzionale", che consente che vengano a conoscenza dei dati di whistleblowing i soli soggetti che ne hanno necessità per lo svolgimento delle proprie funzioni, rispettivamente individuate nelle ***Nomine autorizzati whistleblowing***.

8.4. Trasferimento dati extra-SEE

I dati sul whistleblowing vengono conservati in server residenti in data center certificati ISO 27001 ubicati in Germania (membro UE).

9. COINVOLGIMENTO DELLE PARTI INTERESSATE

In ottemperanza al disposto di cui all'art. 35 par. 2 GDPR:

- si consulta il Responsabile della protezione dei dati - DPO;
- si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno.

Consultazione del DPO

Non è presente un DPO designato.

Consultazione delle parti interessate

Nella fase di scouting del software di gestione delle segnalazioni, il Portale SaaS è stato reso oggetto di una apposita sessione demo on-line, via Microsoft Teams, alla quale hanno preso parte i ruoli più direttamente interessati e competenti per la tematica in oggetto (Funzione IT), i quali durante la successiva discussione interna all'organizzazione del Titolare hanno espresso un parere orale favorevole circa la **facilità di utilizzo** del Portale SaaS. Tale valutazione non è stata documentata dal Titolare.

Allo stato, non si è reputato necessario ricorrere ad alcun altro tipo di consultazione delle parti interessate (es. segnalanti potenziali).

Consultazione del fornitore del Portale SaaS

Il Titolare ha acquisito copia della ***DPIA eseguita da EQS fornitore del Portale SaaS***, da intendersi espressamente come parte essenziale della presente DPIA.

Il fornitore del Portale SaaS dichiara che la propria DPIA è stata compilata da esperti con diligenza e al meglio della propria esperienza, tuttavia non si assume responsabilità per l'accuratezza o completezza delle informazioni contenute nella presente DPIA stessa o per il buon fine delle raccomandazioni ivi contenute.

10. REMEDIATION PLAN

Principi generali

Il trattamento dei dati in esame, essendo di recente attivazione, non è associato ad uno specifico ulteriore action plan.

Misure esistenti o pianificate

Il piano dei controlli del Titolare relativo al trattamento dei dati in esame, prevede che a distanza di 1 anno dall'entrata in vigore della ***Procedura Whistleblowing***, venga sottoposto a riesame congiunto della Funzione Legale di FOR.MA, del DPO e della Direzione, diretto ad accertare l'effettiva applicazione della stessa e ad individuare eventuali azioni di miglioramento continuo delle regole aziendali di trattamento.

Rischi

Non è previsto un action plan.

§§§

11. CONCLUSIONI

Il Titolare reputa che, a valle delle variegate e granulari misure di gestione del rischio applicate al trattamento di whistleblowing:

- i rischi per i diritti e le libertà fondamentali degli interessati siano mantenuti entro un livello ragionevolmente accettabile e,
- conseguentemente, non sussista un rischio residuo rilevante tale da giustificare l'eventuale consultazione preventiva del Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR (ultimo criterio previsto dal WP248).

***