VALUTAZIONE D' IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

ai sensi dell'art. 35 del Regolamento UE 2016/679

GESTIONE SEGNALAZIONI WHISTLEBLOWING

ASL Foggia, Via Michele Protano n.13, 71121 Foggia (FG) - C.F. e P.I. 03499370710

Redatto da	**UFFICIO ANTICORRUZIONE – RPCT**
Validato da	**Direttore Generale**

Data	Ed.	Rev.	Parti modificate
25/03/2019	1	0	Prima emissione
04/08/2021	1	1	Revisione misure
10/07/2023	1	2	Aggiornamento normativo ai sensi del D.lgs 24/2023

INDICE

Informazioni sulla DPIA

La DPIA, acronimo di *Data Protection Impact Assessment*, è una valutazione preliminare, eseguita dal Titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati. In linea con l'approccio basato sul rischio adottato dal Regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:
a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

In particolare, la presente DPIA è stata condotta considerando l'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto, secondo l'allegato 1 al Provvedimento del Garante n. 467 dell'11 ottobre 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018).

La valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Nel percorso di analisi sono stati presi in considerazione i seguenti criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

L'istituto del whistleblowing è uno strumento a disposizione del settore pubblico che si prefigge di regolamentare e facilitare la segnalazione di illeciti di cui il soggetto segnalante, il cosiddetto "whistleblower", sia venuto a conoscenza nell'ambito del proprio contesto lavorativo, anche mediante la previsione di significative forme di tutela nei confronti dello stesso segnalante e degli altri soggetti coinvolti. In Italia, il whistleblowing è regolato dal nuovo decreto entrato in vigore dal 15 luglio 2023 "D.Lgs. 10 marzo 2023, n. 24" e dalle "Linee guida dell'Autorità Nazionale Anticorruzione", approvate con Delibera n. 311 del 12 luglio 2023.

L'ASL di Foggia mette a disposizione dei dipendenti e collaboratori di imprese fornitrici di beni e servizi, un nuovo strumento per contrastare la corruzione. Si tratta di una piattaforma informatica (https://www.sanita.puglia.it/web/asl-foggia/segnalazioneilleciti-whistleblowing-) che permette di inviare segnalazioni di illeciti di cui si è venuti a conoscenza in maniera sicura e confidenziale.

Il trattamento dei dati riguarda pertanto i dati di cui agli artt. 6-9-10 del Reg. UE 2016/679 riconducibili al segnalante ma esteso anche ai seguenti soggetti:

- al facilitatore (persona fisica che assiste il segnalante nel processo di segnalazione e operante all'interno del medesimo contesto lavorativo);
- alle persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente.

Quali sono le responsabilità connesse al trattamento?

Responsabilità connesse al trattamento	Titolare del trattamento: ASL FOGGIA Responsabile del trattamento: NB Consulting per la gestione del rapporto contrattuale Sub-Responsabile del trattamento: Tecnolink per la gestione contrattuale del servizio IAAS tramite il supporto tecnologico della società Interzen.

L'ASL di Foggia ha affidato all'esterno la gestione della piattaforma informatica per la gestione delle segnalazioni di illeciti, in modalità cloud, attraverso la quale il segnalante ha la possibilità di inviare la segnalazione accedendo tramite il sistema di autenticazione SPID, in considerazione della preferenza secondo cui tra i dati obbligatori da fornire ci sono quelli inerenti l'identità personale, così da proteggere e tutelare nel modo più completo possibile il segnalante. Il fornitore è stato designato Responsabile del trattamento dei dati, ai sensi dell'art. 28 del Reg. UE 2016/679.

SEGNALAZIONI CON TUTELE	SEGNALAZIONI SENZA TUTELE
Le segnalazioni possono essere inviate alla piattaforma web, a seguito di autenticazione con SPID, all'indirizzo seguente: https://wb.anticorruzioneintelligente.it/anticorruzione/index.php?codice=4PRKA8&dipendente=1	Per le segnalazioni anonime è possibile utilizzare il seguente indirizzo, nella consapevolezza di non poter essere tutelati in caso di ritorsioni: https://wb.anticorruzioneintelligente.it/anticorruzione/index.php?codice=4PRKA8&dipendente=0

La riservatezza è garantita attraverso idoneo sistema di crittografia.

La piattaforma garantisce che l'identità del segnalante non sia rivelata neanche al destinatario della segnalazione, il quale, nel corso della istruttoria, potrà accedere al dato relativo alla identità del segnalante solo qualora ciò si renda strettamente necessario ai fini della analisi di contenuti della segnalazione e solo informando preventivamente il segnalante. La riservatezza dell'identità del segnalante è garantita anche nell'ambito dell'eventuale procedimento disciplinare avviato nei confronti del segnalato. L'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità.

Ci sono standard applicabili al trattamento?

● Qualifica AGID
● Certificazione CSA Star

- Visualizza la scheda di qualificazione del Marketplace ACN Cloud
- Visualizza la scheda di Whistleblowing su Cloud Security Alliance
- Visualizza la scheda del produttore su Cloud Security Alliance

L'ANAC ha pubblicato, con delibera n. 311 del 12 luglio 2023, le nuove "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne."
Tali linee guida forniscono indicazioni e princìpi di cui gli enti pubblici e privati possono tener conto per i propri canali e modelli organizzativi interni, su cui ANAC si riserva di adottare successivi atti di indirizzo. Si fa presente che, laddove possibile, i contenuti della nuova disciplina sono stati messi a confronto con quella previgente al fine di consentire agli interessati di poter valutare le principali innovazioni introdotte a seguito della Direttiva (UE) 2019/1937.

Le presenti LLGG sono da intendersi sostitutive delle LLGG adottate dall'Autorità con Delibera n. 469/2021, fatto salvo quanto precisato nella Parte Quarta relativa al regime transitorio.

Valutazione: Accettabile
Commento di valutazione:
Le misure tecniche ed organizzative previste nell'accordo sulla protezione dei dati, ai sensi dell'art. 28 del Reg. UE 2016/679 risultano adeguate al rischio, ai sensi degli artt. 25-32 del Reg. UE 2016/679 e garantiscono un buon livello di sicurezza e riservatezza dei dati grazie anche alle ulteriori garanzie di qualificazione ACN e CSA.

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS così come pattuito tra le parti. Dati di registrazione Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio whistleblowing (es. Responsabile Anticorruzione). Categorie particolari di dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati. Dati relativi a condanne penali e reati. Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

Attraverso il portale whistleblowing possono essere trattati dati personali e particolari di cui agli artt. 6-9-10 del Reg. UE 2016/679, considerando che il segnalante ha facoltà di riportare i fatti accaduti integrando informazioni molto riservate riconducibili a terzi.

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

Di seguito le macro fasi del trattamento dei dati mediante piattaforma web:

1) Attivazione della piattaforma
2) Configurazione della piattaforma
3) Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti
4) Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore

La piattaforma informatica consente di acquisire segnalazioni con accesso SPID ma anche segnalazioni anonime al fine di considerarle nei procedimenti di vigilanza "ordinari" tenendole separate dalle segnalazioni di Whistleblowing.

La piattaforma informatica di Whistleblowing pubblica o contiene un link all'informativa sul trattamento dei dati personali, ai sensi degli artt. 13 e 14 del GDPR.

La piattaforma informatica fornisce ai segnalanti tutte le informazioni relative alle procedure di segnalazione: i tempi dell'esame preliminare e del termine dell'istruttoria; i fatti segnalati e come segnalare; misure adottate per assicurare la riservatezza e le tutele. Il RPCT ed i suoi collaboratori designati quali soggetti autorizzati al trattamento dei dati, accedono alla piattaforma informatica autenticandosi con password forti. La piattaforma per l'acquisizione e gestione delle segnalazioni prevede una procedura per l'assegnazione, da parte del RPCT, della trattazione di specifiche segnalazioni all'eventuale personale di supporto. Il RPCT è l'unico soggetto che può creare e revocare le credenziali di accesso dei collaboratori alla piattaforma informatica. Il sistema informatico assicura l'accesso selettivo ai dati delle segnalazioni da parte dei diversi soggetti autorizzati. Ad esempio, il collaboratore può vedere solo i contenuti delle segnalazioni che gli sono state affidate dal RPCT attraverso la procedura informatica. L'attività degli utenti del sistema (RPCT ed eventuale personale di supporto) è tracciata nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione. I dati di log sono consultabili in qualsiasi momento dal RPCT. La piattaforma informatica non richiede al segnalante nome utente e password e garantisce la rintracciabilità del segnalante nel momento in cui viene stabilita la connessione, anche mediante l'impiego di strumenti di anonimizzazione dei dati di navigazione. Il sistema informatico consente al RPCT di accedere al contenuto della segnalazione senza obbligatoriamente dover vedere anche i dati identificativi del segnalante. Sono utilizzati strumenti di crittografia per garantire la riservatezza dell'identità del segnalante, del contenuto delle segnalazioni e della relativa documentazione. Nel corso dell'istruttoria è reso possibile lo scambio di messaggi o documenti tra segnalante e RPCT/collaboratore mediante meccanismi interni alla piattaforma che tutelano l'identità del segnalante. È esclusa l'adozione della posta elettronica quale mezzo di invio di tali comunicazioni. Nei messaggi inviati dalla piattaforma, (es. in caso di variazione dello stato di avanzamento dell'istruttoria, riscontro del segnalante a una richiesta di integrazione, riscontro del segnalante a una richiesta di consenso a rivelare la propria identità nell'ambito di un procedimento disciplinare, ecc.) sulla casella di posta elettronica individuale del RPCT e/o collaboratore, tali messaggi non contengono riferimenti all'identità del segnalante o all'oggetto della segnalazione. L'applicazione informatica identifica ogni segnalazione ricevuta mediante l'attribuzione di un codice univoco progressivo, registrando la data e l'ora di ricezione. Il segnalante ha la possibilità di rientrare nella segnalazione dopo averla già inviata e aggiungere informazioni, non solo quando gli vengono sollecitate dal RPCT. La piattaforma di Whistleblowing registra i diversi "Stati" in cui può trovarsi la segnalazione. La procedura informatica controlla i tempi dell'iter di valutazione della segnalazione: Il modulo di segnalazione consente di allegare file multimediali. La piattaforma web tiene traccia dell'esito della valutazione finale, registrando anche data e ora. Il segnalante può verificare in ogni momento lo stato in cui è la segnalazione. La piattaforma elabora report anche grafici, sul numero di segnalazioni ricevute per anno, il loro stato, l'esito, la tipologia di farti segnalati, ecc.

Quali sono le risorse di supporto ai dati?

Il portale whistleblowing è collocato su Service provider data center Microsoft Azure.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati personali sono trattati nel rispetto dei principi di cui all'art. 5 del Reg. UE 2016/679. fornendo adeguata informativa ai segnalanti attraverso il sito internet istituzionale e prima dell'accesso alla piattaforma web, ai sensi degli artt. 13-14 del Reg. UE 2016/679.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

I dati personali sono trattati dal Responsabile della prevenzione della corruzione e della trasparenza dell'ASL di Foggia per obbligo di legge e nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, con particolare riferimento al compito di accertare eventuali illeciti denunciati nell'interesse pubblico e dell'integrità dell'ASL di Foggia, ai sensi del d.lgs 24/2023.

Valutazione: Accettabile

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

I dati personali raccolti sono pertinenti e limitati a quanto necessario per l'analisi preliminare, valutazione, avvio del procedimento per il riscontro al segnalante, fino alla chiusura o archiviazione della segnalazione.

Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, E-mail di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e P.IVA). Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione. Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo vede abilitata la possibilità di navigazione tramite Tor Browser per finalità di accesso anonimo sulla rete internet, con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

I dati personali sono raccolti dal sistema web con procedure interne a garanzia della qualità e dell'aggiornamento delle informazioni rilasciate. L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per il tempo necessario al trattamento della specifica segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione («limitazione della conservazione»).

Valutazione: Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

I segnalanti sono informati tramite apposita informativa ex artt. 13 del Reg. UE 2016/679 pubblicata nella pagina web di accesso al Portale whistleblowing e sul sito internet istituzionale, nell'apposita sezione Privacy.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

I dati personali del segnalante sono raccolti e trattati dal Responsabile della prevenzione della corruzione e della trasparenza per obbligo di legge e dagli autorizzati dell'Ufficio Anticorruzione, con particolare riferimento al compito di accertare eventuali illeciti denunciati nell'interesse pubblico e dell'integrità aziendale, ai sensi del d.lgs. n. 24 del 10 marzo 2023, recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

Il trattamento dei dati è necessario per dare attuazione agli obblighi di legge e ai compiti d'interesse pubblico previsti dalla disciplina di settore la cui osservanza è condizione di liceità del trattamento (artt. 6, par. 1, lett. c) ed e) e parr. 2 e 3, 9, par. 2, lett. b) e g), 10 e 88 del Regolamento, nonché 2-ter e 2-sexies del Codice).

In alcuni casi, inoltre, in base a quanto previsto dai seguenti articoli del D.Lgs. 10 marzo 2023 n. 24, potrebbe essere richiesto il consenso espresso, specifico e libero dell'interessato (art. 6, par. 1, lett. a) GDPR:

- Art. 12 comma 2: la rivelazione dell'identità della persona segnalante a persone diverse da quelle competenti a ricevere o dare seguito alle segnalazioni può avvenire solo previo consenso espresso della stessa persona segnalante;
- Art. 12 comma 5: qualora, nell'ambito del procedimento disciplinare, la conoscenza dell'identità del segnalante fosse indispensabile per la difesa dell'incolpato, verrà domandato

al segnalante se intende rilasciare il consenso ai fini della rivelazione della propria identità.

Valutazione: Accettabile

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

Per il segnalante il diritto di accesso è garantito mediante istanza al RPCT mentre non è garantito il diritto alla portabilità.

La persona segnalata o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, divulgazione pubblica o denuncia, non possono esercitare – per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata - i diritti che normalmente il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento). Dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante. In tali casi, dunque, al soggetto segnalato o alla persona menzionata nella segnalazione è preclusa anche la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della protezione dei dati personali (limiti previsti ai sensi dell'art. 2-undecies del Codice).

Valutazione: Accettabile

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

Per il segnalante il diritto di rettifica dei propri dati è garantito mediante istanza al RPCT mentre non è garantito il diritto alla cancellazione.

La persona segnalata o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, divulgazione pubblica o denuncia, non possono esercitare – per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata - i diritti che normalmente il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento). Dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante. In tali casi, dunque, al soggetto segnalato o alla persona menzionata nella segnalazione è preclusa anche la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della protezione dei dati personali (limiti previsti ai sensi dell'art. 2-undecies del Codice).

Valutazione: Accettabile

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

Per il segnalante il diritto di limitazione ed opposizione al trattamento dei dei propri dati è garantito mediante istanza al RPCT nei limiti imposti dal d.lgs 24/2023.

La persona segnalata o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, divulgazione pubblica o denuncia, non possono esercitare – per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata - i diritti che normalmente il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento). Dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante. In tali casi, dunque, al soggetto segnalato o alla persona menzionata nella segnalazione è preclusa anche la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della protezione dei dati personali (limiti previsti ai sensi dell'art. 2-undecies del Codice).

Valutazione: Accettabile

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

Il fornitore del portale web per la gestione delle segnalazioni di illeciti è nominato quale Responsabile del trattamento dei dati ex art. 28 del Reg. UE 2016/679. L'accordo sulla protezione dei dati riporta nel dettaglio le istruzioni del Titolare e le misure di sicurezza tecniche ed organizzative garantite dal Responsabile e sub-Responsabili del trattamento.

Valutazione: Accettabile

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

Non sono previsti trasferimenti di dati personali verso Paesi extra UE

Valutazione: Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

Protocollo HTTPS
Certificato SSL erogato da Network Solutions, LLC
Criptaggio database e documenti
Database. Chiave di criptazione dati a sua volta criptata mediante un algoritmo per un ulteriore livello di sicurezza. Il dato resta criptato nel database e la sua decriptazione avviene solo quando viene visualizzato
Documenti. Criptazione e decriptazione mediante stessa chiave

Valutazione: Accettabile
Commento di valutazione:
Misura adeguata al rischio di accesso illecito agli archivi delle segnalazioni.

Controllo degli accessi logici

Sistema di permessi granulari che consente di gestire:

- l'accesso (consentito/non consentito) alle singole aree/funzionalità e la successiva azione (consentita/non consentita) di creazione, modifica, cancellazione dell'informazione/documento
- su singolo utente, ruolo utente oppure gruppi di utenti.

Valutazione: Accettabile

Tracciabilità

Gli accessi del RPCT sono tracciati a livello applicativo. Non sono tracciati gli accessi dei segnalanti.

Valutazione: Accettabile
Commento di valutazione:
Misura adeguata al contesto

Vulnerabilità

E' garantita la manutenzione periodica del software con aggiornamenti della sicurezza sempre monitorati

Valutazione: Accettabile
Commento di valutazione:
Misura adeguata al contesto

Lotta contro il malware

Il server applicativo e di database è gestito tramite sistemi antimalware evoluti.

Valutazione: Accettabile
Commento di valutazione :
Misura adeguata al contesto

Sicurezza dei siti web

È stato configurato un accesso limitato alle macchine virtuali, il minimo indispensabile per rispondere alle necessità di monitoraggio e manutenzione della piattaforma. Protocollo HTTPS attivo.

Valutazione: Accettabile
Commento di valutazione :
Misura adeguata al contesto

Backup

E' garantito un piano di disaster recovery e business continuity. Le copie dei dati sono cifrate.

Valutazione: Accettabile
Commento di valutazione :
Misura adeguata al contesto

Manutenzione

E' garantita la manutenzione periodica del server applicativo e di database.

Valutazione: Accettabile
Commento di valutazione :
Misura adeguata al contesto

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

E' definita specifica procedura per la gestione delle violazioni di dati (data-breach)

Valutazione: Accettabile
Commento di valutazione:

Misura adeguata al contesto

Anonimizzazione

Per ogni segnalazione viene assegnato un codice (pseudonimo) che il segnalante riceve al momento dell'inserimento e che deve conservare per poter accedere nuovamente alla segnalazione, verificare la risposta del Responsabile per la Prevenzione della Corruzione e della Trasparenza (RPCT), dialogare ed eventualmente rispondere a richieste di chiarimenti o approfondimenti. La piattaforma informatica per la gestione delle segnalazioni non traccia le attività (accessi e operazioni) effettuate dal segnalante.

Valutazione: Accettabile
Commento di valutazione:

Nuove funzionalità della piattaforma:

• Guida alla verifica dei requisiti essenziali per accordare la tutela al segnalante prevista dall'art.54 bis . Il sistema mostrerà una serie di indicatori ritenuti necessari e indispensabili per accordare le tutele. Il RPCT sarà chiamato a confermare o meno con un segno di spunta la presenza di tali requisiti e in automatico la piattaforma registrerà la segnalazione come segnalazione di Whistleblowing o meno.

• Guida all'esame preliminare della segnalazione. La piattaforma presenterà una serie di voci che consentirà di condurre l'esame preliminare in modo conforme a quanto previsto dalle linee guida. Il RPCT sarà chiamato a confermare o meno con un segno di spunta tali criteri e in automatico il sistema chiuderà la segnalazione se questa non supera i punti di controllo preliminare. In caso di esame preliminare superato, la segnalazione verrà posta in automatico nel nuovo stato Istruttoria

• Creazione documento di Risultanze Istruttorie all'interno della piattaforma collegato ad una singola segnalazione, con editor di testo al fine di evitare upload e download di documenti, così come esplicitamente richiesto nelle Linee guida

• Registrazione delle motivazioni del RPCT per cui mette in chiaro i dati identificativi del segnalante (questa funzionalità permette di associare al RPCT anche la funzione di "Custode dell'Identità") e conseguente aggiunta della motivazione nella mail inviata automaticamente dal sistema al segnalante per informarlo sul fatto che i suoi dati identificativi sono stati messi in chiaro

• Pulsante "Acconsento" per il segnalante, con il quale potrà in modo inequivocabile dare il consenso a rivelare la sua identità nel corso del procedimento disciplinare. Il sistema acquisirà data e ora della dichiarazione e, in caso in cui il segnalante dia il consenso, il sistema non permetterà di revocarlo

• Dichiarazione iniziale. Il segnalante sarà invitato a confermare con un segno di spunta una serie di dichiarazioni prima di poter compilare il modulo di segnalazione, così come richiesto dalle nuove Linee guida, In assenza di conferma, non potrà procedere alla compilazione della segnalazione

Rischi

Accesso illegittimo ai dati

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

mobbing, discriminazione, isolamento, perdita dignità, perdita lavoro

Quali sono le principali minacce che potrebbero concretizzare il rischio?

comunicazione dati segnalante, diffusione dati segnalante

Quali sono le fonti di rischio?

fonti umane interne, fonti umane esterne, cause naturali

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Lotta contro il malware, Sicurezza dei siti web, Controllo degli accessi logici

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

Importante, Il livello di rischio è stimato come importante in considerazione degli impatti potenziali sui segnalanti e preso atto delle misure di sicurezza presenti che consentono di ridurre la probabilità di accadimento di un accesso illegittimo al Portale del whistleblowing

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

Limitata, La probabilità di accadimento di un accesso illegittimo risulta limitata in considerazione delle misure tecniche ed organizzative implementate.

Valutazione: Accettabile
Commento di valutazione:
Le misure tecniche ed organizzative applicate risultano adeguate e sufficienti a garantire un buon livello di sicurezza e riservatezza.

Rischi

Modifiche indesiderate dei dati

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

discriminazione, perdita lavoro, mobbing, isolamento

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

malfunzionamento software, alterazione volontaria di dati, virus, alterazione accidentale di dati, danno fisico hardware, vulnerabilità software, vulnerabilità database

Quali sono le fonti di rischio?

cause naturali, fonti umane esterne, fonti umane interne

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

Crittografia, Backup, Tracciabilità, Vulnerabilità, Lotta contro il malware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Anonimizzazione, Sicurezza dei siti web, Controllo degli accessi logici, Manutenzione

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

Importante, La gravità in caso di modifiche non desiderate ai dati è stimata con importante in considerazione del contesto e della vulnerabilità dei segnalanti e segnalati.

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

Limitata, La probabilità di accadimento del rischio di modifiche non desiderate ai dati è stimata come limitata in considerazione delle misure di sicurezza implementate.

Valutazione: Accettabile

Rischi

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

discriminazione, perdita di tempo, perdita del controllo sui dati

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

virus, danno fisico hardware, cancellazione volontaria, cancellazione accidentale

Quali sono le fonti di rischio?

cause naturali, fonti umane esterne, fonti umane interne

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

Crittografia, Backup, Sicurezza dei siti web, Lotta contro il malware, Anonimizzazione, Controllo degli accessi logici, Tracciabilità, Vulnerabilità, Manutenzione, Gestire gli incidenti di sicurezza e le violazioni dei dati personali

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

Importante, Gravità del rischio stimata come importante in considerazione dello stato di vulnerabilità dei soggetti interessati (segnalante e segnalato)

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

Limitata, La probabilità di accadimento del rischio di perdita è basso in considerazione delle misure di sicurezza applicate.

Valutazione: Accettabile

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

2° LIVELLO – INFRASTRUTTURA I.T. DEL CLOUD SERVICE PROVIDER	
Service Provider	Microsoft Azure.
Tipologia di servizio cloud	Public Cloud
Certificazioni del cloud service provider	Consulta la documentazione di conformità di Microsoft Azure.
Localizzazione dei data center utilizzati	West Europe (Netherlands)
Livelli di sicurezza adottati dal service provider	Operazioni eseguite da Microsoft per proteggere l'infrastruttura di Azure.

Ridondanza dei dati del service provider	Archiviazione con ridondanza di zona (Zone Redundancy Storage, ZRS): replica i dati archiviati in Azure in modalità sincrona su tre aree disponibili interne all'area primaria (primary region).

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

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

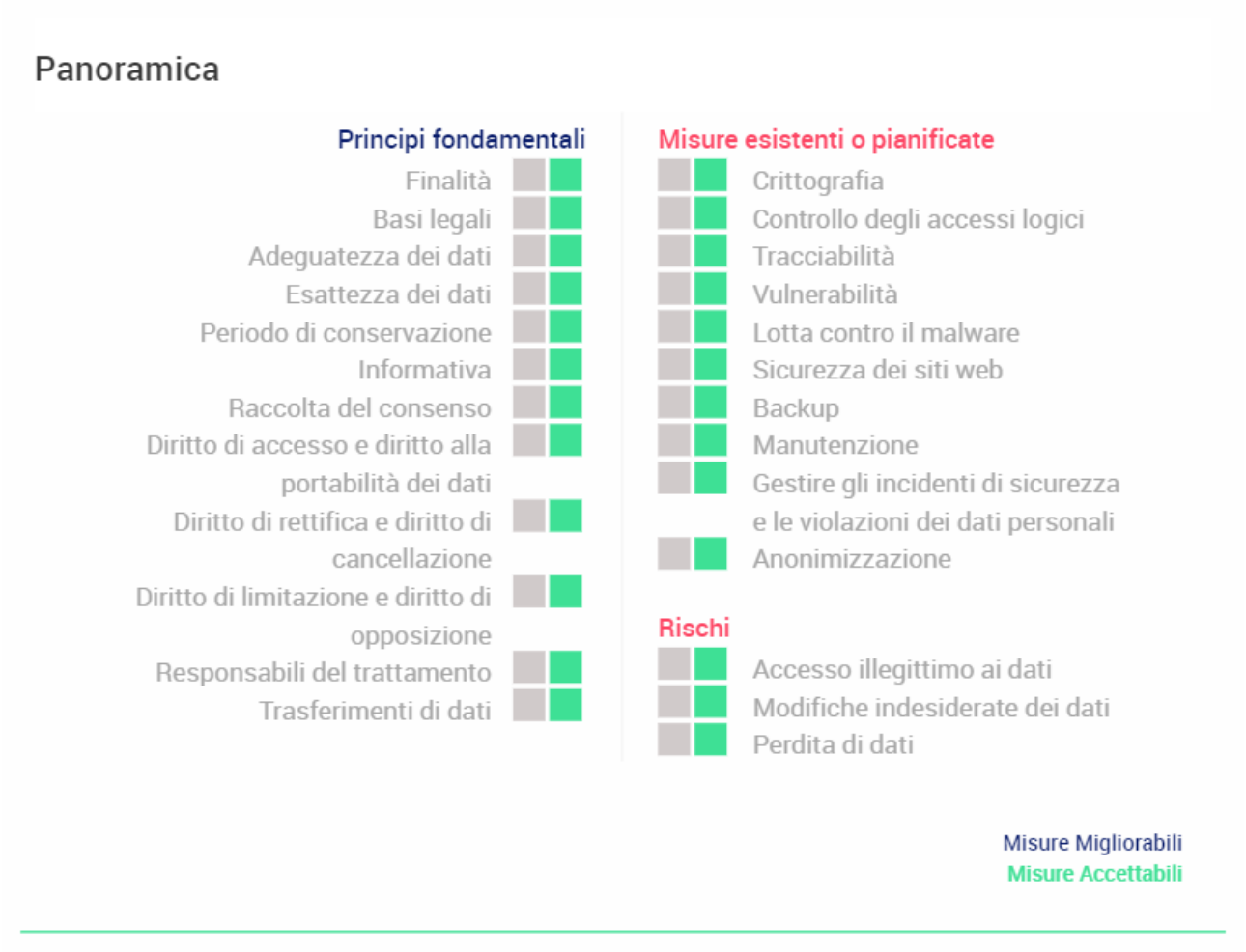
4° LIVELLO – COMPONENTI SOFTWARE	
Sistema operativo	Antivirus Microsoft Forefront
Server virtuale	L'accesso ai server virtuali avviene mediante una VPN ed utilizzando un profilo utente dimensionato strettamente in base alle necessità di monitoraggio e manutenzione.

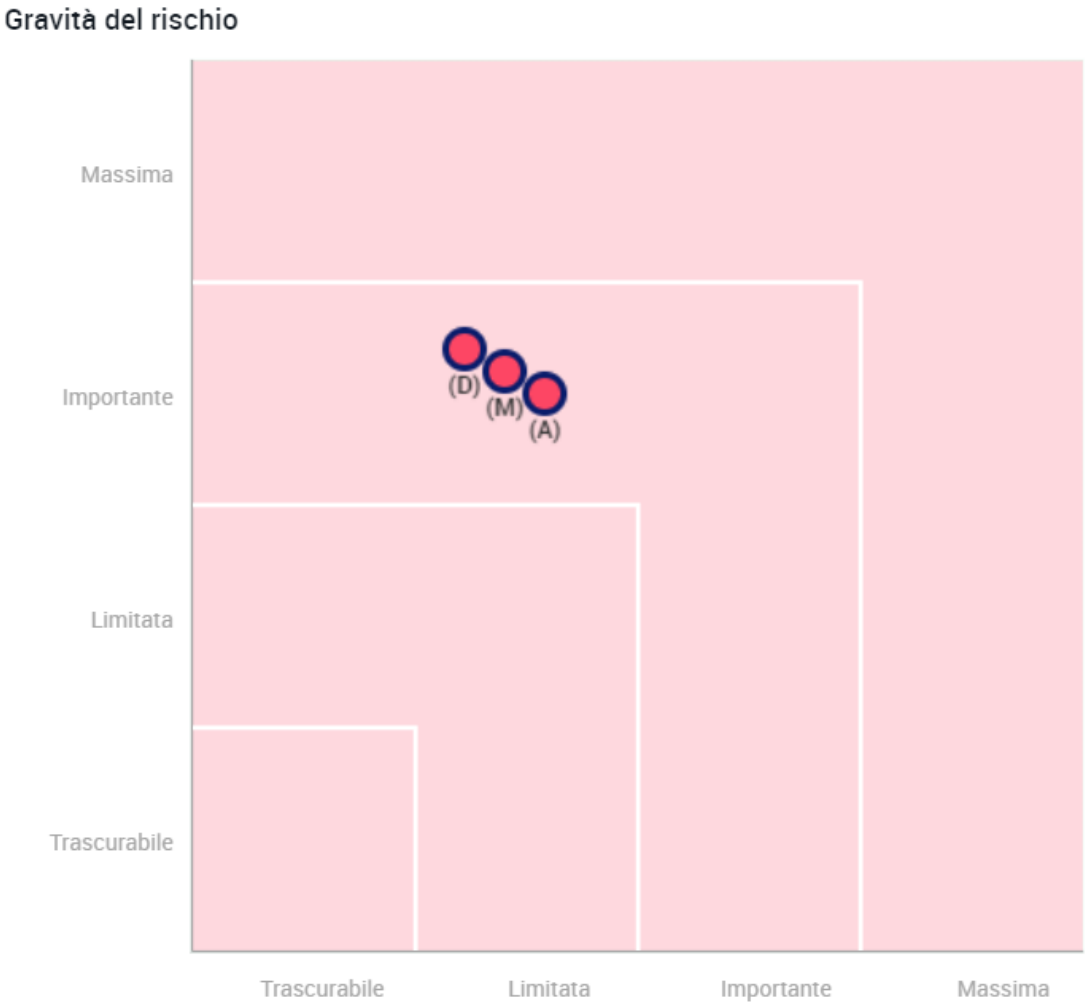
5° LIVELLO – CODICE APPLICATIVO	
Sicurezza informatica del produttore	Nell'ambito del processo di qualificazione del Cloud Marketplace ACN, il produttore ha validato i propri livelli di gestione della riservatezza e della sicurezza dei dati della soluzione Whistleblowing presso lo STAR Registry (Security,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

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

Rischi

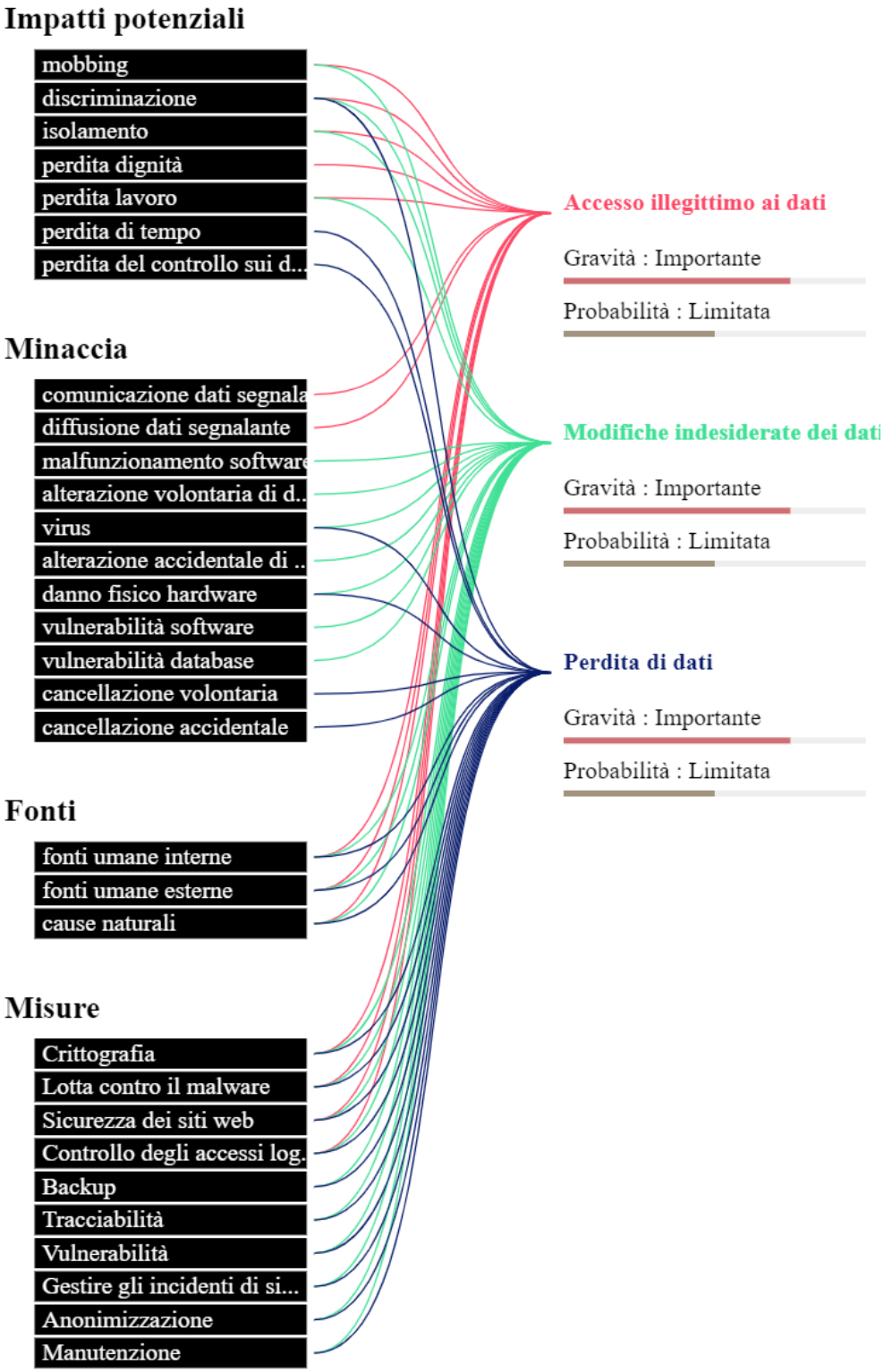
Panoramica dei rischi





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

04/08/21


Impatti potenziali
mobbing
discriminazione
isolamento
perdita dignità
perdita lavoro
perdita di tempo
perdita del controllo sui d...
Minaccia
comunicazione dati segnala
diffusione dati segnalante
malfunzionamento software
alterazione volontaria di d...
virus
alterazione accidentale di ...
danno fisico hardware
vulnerabilità software
vulnerabilità database
cancellazione volontaria
cancellazione accidentale
Fonti
fonti umane interne
fonti umane esterne
cause naturali
Misure
Crittografia
Lotta contro il malware
Sicurezza dei siti web
Controllo degli accessi log...
Backup
Tracciabilità
Vulnerabilità
Gestire gli incidenti di si...
Anonimizzazione
Manutenzione
Accesso illegittimo ai dati
Gravità : Importante
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Importante
Probabilità : Limitata
Perdita di dati
Gravità : Importante
Probabilità : Limitata

DPO/RPD

Dati di contatto del DPO: rpd@aslfg.it

Parere del DPO/RPD

Le misure tecniche ed organizzative presenti consentono un trattamento dei dati personali conforme ai requisiti del Regolamento UE 2016/679. Le misure di garanzia offerte dal Responsabile del trattamento e suoi sub-Responsabili consentono di ottenere un rischio residuo molto basso che dovrà comunque essere riesaminato almeno annualmente.

Responsabile della validazione della DPIA: Direttore Generale

Avendo letto integralmente la valutazione d'impatto sulla protezione dei dati (DPIA) relativa al trattamento di dati connessi alla gestione delle segnalazioni di illeciti (whistleblowing) ai sensi del d.lgs 24/2023

- Dichiaro che la descrizione del contesto corrisponde alla realtà;
- Dichiaro di essere consapevole dei rischi residui esistenti, in funzione delle misure attualmente implementate;
- Mi impegno a disporre il riesame periodico dell'analisi dei rischi e l'implementazione delle eventuali misure correttive proposte, sentito il DPO.

Data ……

Firma del Titolare del trattamento (Direttore G
……

Firmato digitalmente da:
NIGRI ANTONIO GIUSEPPE
Firmato il 03/08/2023 14:01
Seriale Certificato: 465338
Valido dal 25/05/2021 al 25/05/2024
InfoCamere Qualified Electronic Signature CA