A.P.S.P. "SUOR AGNESE"
TITOLARE DEL TRATTAMENTO

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI ART. 35 REG UE 16/679

Rev. dd. 16/04/2024

LA PRESENTE VALUTAZIONE DI IMPATTO CONCERNE I TRATTAMENTI EFFETTUATI DA PARTE DI A.P.S.P. "SUOR AGNESE", TITOLARE DEL TRATTAMENTO, NELL'AMBITO DELLA GESTIONE DELLE SEGNALAZIONI DI CONDOTTE ILLECITE (C.D. WHISTLEBLOWING).

L'Unione Europea, con la Direttiva 2019/1937, ha rinnovato la normativa riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, al fine di creare uno standard minimo per la protezione dei diritti dei whistleblowers in tutti gli Stati Membri.

L'Italia ha attuato la Direttiva Europea con il D.lgs. 10 marzo 2023 n. 24 e con l'adozione della presente DPIA, il Titolare del trattamento ha inteso conformarsi alle suddette prescrizioni normative.

Si richiama integralmente la policy aziendale di Whistleblowing adottata dal Titolare in data 21/03/2024

PREMESSA

La valutazione d'impatto sulla protezione dei dati (di seguito "DPIA) è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all'impiego di nuove tecnologie, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone.

L'art. 13 comma 6 del citato Decreto stabilisce l'obbligatorietà della redazione della presente DPIA.

Il processo di DPIA è ritenuto uno degli aspetti di maggiore rilevanza nel nuovo quadro normativo definito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), in quanto esprime chiaramente la responsabilizzazione (c.d. accountability) del Titolare nei confronti dei trattamenti dallo stesso effettuati. Il Titolare del trattamento, infatti, è tenuto non solo a garantire l'osservanza delle disposizioni regolamentari, quanto anche a dimostrare adeguatamente in che modo egli garantisca tale osservanza.

In generale, la disciplina vigente stabilisce che la procedura di gestione delle segnalazioni deve garantire le protezioni accordate al segnalante dalla legge informando e rendendo nel contempo consapevoli i potenziali segnalanti delle condizioni di operatività delle protezioni previste a loro tutela.

METODOLOGIA UTILIZZATA NELLA REDAZIONE DELLA DPIA

La presente DPIA fa propri alcuni elementi elencati dal Considerando 90 GDPR e mira a gestire i rischi esistenti per i diritti e le libertà delle persone fisiche interessate del trattamento in questione attraverso i processi di seguito indicati:

- definizione del contesto tenendo conto della natura, dell'ambito e delle finalità del trattamento;
- valutando i rischi considerando la loro probabilità e gravità;

- gestendo i rischi assicurando la protezione dei dati personali.

La metodologia applicata osserva il seguente modello operativo:

DESCRIZIONE DEL TRATTAMENTO IN OGGETTO

AMBITO DEL TRATTAMENTO

La ricezione e la gestione delle segnalazioni interne determinano in capo al Titolare il trattamento dei dati seguenti dati personali riferiti alle persone a vario titolo coinvolte nei fatti segnalati (segnalante, segnalato, facilitatore, eventuali altri terzi), c.d. interessati:

- dati personali di natura comune;
- dati personali rientranti nelle categorie particolari eventualmente contenuti nella segnalazione e negli atti e nei documenti a essa allegati;
- informazioni riferite a condanne penali e reati, eventualmente contenuti nella segnalazione e negli atti e nei documenti a essa allegati.

CATEGORIE DI INTERESSATI

Persone fisiche a vario titolo coinvolte nei fatti segnalati (segnalante, segnalato, facilitatore, eventuali altri terzi).

CATEGORIE DI DATI TRATTATI

Il trattamento in questione concerne:

a) dati personali comuni di cui all'art. 4, punto 1, del GDPR, tra i quali, ad esempio, i dati anagrafici (nome, cognome, data e luogo di nascita), i dati di contatto (numero telefonico fisso e/o mobile, indirizzo postale/e-mail), il ruolo/mansione lavorativa;

b) dati personali "particolari" di cui all'art. 9 del GDPR, tra i quali, ad esempio, le informazioni relative a condizioni di salute, opinioni politiche, convinzioni religiose o filosofiche, orientamento sessuale o appartenenza sindacale;

c) dati personali "giudiziari" di cui all'art. 10 del GDPR, relativi a condanne penali e reati, o a connesse misure di sicurezza.

FINALITA' DEL TRATTAMENTO

Adempimento degli obblighi di legge (art. 54-bis d.lgs. 165/2001).

OPERAZIONI ESEGUITE SUI DATI TRATTATI

Il trattamento sopra descritto svolto dal Titolare 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 dei trattamento del Titolare (art. 30 GDPR) e nell'informativa whistleblowing.

Si richiama integralmente la policy aziendale di Whistleblowing.

MODALITÀ DEL TRATTAMENTO

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

CRITERI DI DATA RETENTION

Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione. I

dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

BASI GIURIDICHE DEL TRATTAMENTO

La base giuridica del trattamento dei dati personali è costituita dall'adempimento ad un obbligo legale a cui è soggetto il Titolare del trattamento.
Nei casi contemplati dalla medesima disciplina potrà essere richiesto uno specifico e libero consenso al soggetto segnalante – ai sensi dell'art. 6, par. 1, lett. a) del GDPR – e, segnatamente, laddove si ravveda la necessità di svelarne l'identità.
Il trattamento di dati personali "particolari", eventualmente inclusi nelle segnalazioni, si fonda sull'assolvimento di obblighi e sull'esercizio di diritti specifici del Titolare del trattamento e dell'interessato in materia di diritto del lavoro, ai sensi dell'art. 9, par. 2, lett. b) del GDPR.
Quanto alla finalità di accertare, esercitare o difendere un diritto in sede giudiziaria, la relativa base giuridica del trattamento di dati personali è costituita dal legittimo interesse del Titolare in tal senso, di cui all'art. 6, par. 1, lett. f), del GDPR; per la medesima finalità, i trattamenti di dati personali di natura "particolare", se presenti, si fondano sull'art. 9, par. 2, lett. f) del GDPR.

DESTINATARI

Sussistendone gli estremi, i dati personali potranno essere trasmessi all'Autorità Giudiziaria, Corte dei Conti, Anac e/o Organi di Polizia che ne facciano richiesta nel contesto di indagini giudiziarie.
I dati personali raccolti sono trattati da parte di soggetti autorizzati sulla base di specifiche istruzioni fornite in ordine a finalità e modalità del trattamento medesimo.
In nessun caso i dati personali saranno oggetto di diffusione.

SOGGETTI AUTORIZZATI AL TRATTAMENTO

Il Titolare ha individuato quale gestore della segnalazione (di seguito anche il "gestore" o "ricevente") nonché incaricato al relativo trattamento il RPCT, nella persona del Direttore – Dott.ssa Armanda Denicolò.
Nell'ambito della gestione del canale di segnalazione interna, il gestore della segnalazione è stato istruito sul dovere di operare nel rispetto della policy aziendale di Whistleblowing.
Il Gestore è stato altresì informato sul dovere di attenersi al segreto e alla riservatezza in merito non solo all'adempimento dei propri compiti, ed ai dati personali di cui viene in contatto, ma in generale su tutte le informazioni aziendali di cui viene a conoscenza in esecuzione od in occasione dell'incarico conferito. Tali obblighi permangono anche dopo la cessazione dell'incarico, senza limiti di tempo.

Qualora il Gestore versi in situazione di conflitto di interessi dovrà astenersi dal gestire la segnalazione ed attenersi alle indicazioni previste nella policy whistleblowing.
Nella gestione delle segnalazioni whistleblowing e nella fase istruttoria deve inoltre attenersi alle norme dettate dal Regolamento (UE) 2016/679, dal decreto legislativo 30 giugno 2003 n. 196 e a quanto prescritto dall'art. 13 del d.lgs. 24/2023.

TUTELA DEL SEGNALANTE

Uno dei principali cardini della disciplina del whistleblowing è rappresentato dalle tutele riconosciute al segnalante per le segnalazioni effettuate nel rispetto della disciplina. Il legislatore pone l'obbligo di garantire la riservatezza della sua identità e di ogni altra informazione, inclu-

sa l'eventuale documentazione allegata, dalla quale possa direttamente o indirettamente risalire all'identità del whistleblower. La riservatezza deve essere garantita per ogni modalità di segnalazione, quindi, anche quando avvenga in forma orale (linee telefoniche, messaggistica vocale, incontro diretto) e/o scritta (tramite posta ordinaria o piattaforma digitale). In particolare, il Decreto si preoccupa di proteggere il segnalante con:

- l'obbligo di riservatezza della sua identità;
- il divieto di atti ritorsivi nei suoi confronti;
- la limitazione della sua responsabilità per la rilevazione o diffusione di alcune tipologie di informazioni protette.

Tali misure di protezione si applicano non solo al soggetto segnalante ma anche ad altri soggetti che potrebbero essere destinatari di ritorsioni, in ragione del ruolo assunto o della particolare vicinanza o rapporto con il segnalante.

Nell'ambito del procedimento disciplinare attivato dal Titolare contro il presunto autore della condotta segnalata, 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 invece la contestazione sia fondata, in tutto o in parte, sulla segnalazione e l'identità del segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare o della persona comunque coinvolta nella segnalazione, quest'ultima sarà utilizzabile ai fini del procedimento disciplinare solo previo consenso espresso della persona segnalante alla rivelazione della propria identità. In tali casi, è dato preventivo avviso alla persona segnalante mediante comunicazione scritta delle ragioni che rendono necessaria la rivelazione dei dati riservati.

Qualora il soggetto segnalante neghi il proprio consenso, la segnalazione non potrà essere utilizzata nel procedimento disciplinare che, quindi, non potrà essere avviato o proseguito in assenza di elementi ulteriori sui quali fondare la contestazione. Resta ferma in ogni caso, sussistendone i presupposti, la facoltà per il Titolare di procedere con la denuncia all'Autorità giudiziaria.

Il Decreto vieta ogni forma di ritorsione nei confronti del segnalante, intesa come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, che si verifichi nel contesto lavorativo e che determini – in via diretta o indiretta – un danno ingiusto ai soggetti tutelati. Gli atti ritorsivi adottati in violazione di tale divieto sono nulli.

Si evidenzia che esistono dei casi in cui il segnalante perde la protezione:

- qualora sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di diffamazione o di calunnia o nel caso in cui tali reati siano commessi con la denuncia all'autorità giudiziaria o contabile;
- in caso di responsabilità civile per lo stesso titolo per dolo o colpa grave. In entrambe le ipotesi alla persona segnalante o denunciante verrà irrogata una sanzione disciplinare.

Di fronte a una segnalazione anonima, la tutela è assicurata qualora la persona segnalante sia stata successivamente identificata o la sua identità si sia palesata soltanto in un secondo momento.

OSSERVANZA DEI PRINCIPI STABILITI DALL'ART. 5 DEL GDPR

1) **TRASPARENZA DEL TRATTAMENTO**: Il Titolare ha predisposto e rende disponibile ai possibili interessati un'idonea informativa sul trattamento dei dati personali (art. 13, co. 4 del Decreto), recante, tra le altre, le informazioni su:

- il titolare del trattamento e i relativi dati di contatto;
- le categorie dei dati trattati e le finalità del trattamento;
- le basi giuridiche del trattamento;
- la natura del conferimento;
- le modalità del trattamento e il periodo di conservazione dei dati personali;
- l'ambito di comunicazione e trasferimento dei dati personali;
- i diritti dell'interessato.

2) **LIMITAZIONE DELLE FINALITÀ**: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità, prevedendo che le segnalazioni non possano essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse;

3) **MINIMIZZAZIONE DEI DATI**: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. I dati manifestamente non utili alla trattazione di una specifica segnalazione non verranno raccolti o, in caso di raccolta accidentale, verranno prontamente cancellati.

4) **LIMITAZIONE DELLA CONSERVAZIONE**: le segnalazioni e la relativa documentazione sono conservate per il tempo necessario alla trattazione della segnalazione e, comunque, non oltre 5 anni dalla comunicazione dell'esito finale della procedura;

5) **INTEGRITÀ E RISERVATEZZA:** i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali).
Il Gestore della segnalazione provvede all'archiviazione delle segnalazioni giunte per posta ordinaria attraverso idonei strumenti che consentano di garantire la riservatezza (es. all'interno di archivi protetti da misure di sicurezza).
La segnalazione effettuata oralmente, previo consenso della persona segnalante, viene documentata a cura del Gestore della segnalazione mediante verbale, che sarà sottoscritto sia dal gestore che dal segnalante e di cui verrà a quest'ultimo fornita copia.
Nel caso di incontro diretto con il segnalante, si redigerà dell'incontro apposito verbale che sarà sottoscritto sia dal Gestore che dal segnalante e di cui verrà a quest'ultimo fornita copia.

Il Titolare, in adempimento alle previsioni di legge e nell'ottica di garantire correttezza e trasparenza nella conduzione della propria attività, ha predisposto un sistema informatico di "Whistleblowing", a disposizione di chiunque voglia segnalare situazioni rilevanti ai fini di legge (Decreto legislativo n. 24 del 10 marzo 2023).

VALUTAZIONE DELLE POTENZIALI CONSEGUENZE DERIVANTI DALLA MANCATA ADOZIONE DI ADEGUATE MISURE DI SICUREZZA

Il trattamento oggetto di questa valutazione di impatto potrebbe essere soggetto ai seguenti rischi per i diritti e le libertà degli interessati sopra individuati:

RISCHI INCOMBENTI SUL TRATTAMENTO	CONSEGUENZE	IMPATTO (gravità delle conseguenze)	MISURE DI SICUREZZA ADOTTATE DAL TITOLARE	PROBABILITA' DEL RISCHIO
perdita della riservatezza	invasione della privacy dell'interessato; disturbi psicologici per l'interessato (diffamazione, lesione reputazionale); potenziali tentativi o atti di ritorsione o discriminazione; rischio di ostacoli alle indagini sulla violazione segnalata; potenziale pregiudizio economico per l'interessato.	Alto	i processi di whistleblowing sono definiti tramite la procedura aziendale di Whistleblowing; i soggetti coinvolti nel trattamento sono stati autorizzati e applicano elevati standard professionali; il gestore delle segnalazioni (RPCT) è stato scelto in base alla posizione funzionali di neutralità e indipendenza rispetto al contenuto delle segnalazioni pervenute; i documenti sono soggetti a conservazione in archivi con serrature e/o presidiati; i soggetti coinvolti garantiscono la sicurezza delle chiavi di accesso ai locali dove sono conservati gli archivi in modo tale da ovviare ad ipotesi di accesso non autorizzato ad essi da parte di terzi; nel caso in cui la segnalazione venisse formulata mediante posta ordinaria, al momento della ricezione, la persona individuata a gestire le segnalazioni deve garantire la riservatezza dell'identità del segnalante e del contenuto delle buste e procedere all'archiviazione della segnalazione attraverso idonei strumenti che permettano di garantire la riservatezza (ad esempio all'interno di archivi protetti da misure di sicurezza); nel caso di utilizzo di una linea telefonica registrata o di un altro sistema di messaggistica registrato, il soggetto gestore della segnalazione conserva, previo consenso del segnalante alla registrazione, la segnalazione all'interno di un dispositivo idoneo alla conservazione e all'ascolto; nel caso di utilizzo di linee telefoniche non registrate, al momento della ricezione della segnalazione, il soggetto gestore della segnalazione deve documentarla mediante resoconto dettagliato del massaggio e il contenuto dev'essere controfirmato dal segnalante, previa verifica ed eventuale rettifica. Del resoconto sottoscritto deve essere fornita copia al segnalante; nel caso in cui la segnalazione avesse luogo mediante incontro diretto, l'incontro deve svolgersi in un luogo adatto a garantire la riservatezza del segnalante; il fornitore della piattaforma digitale adottata per il ricevimento delle segnalazioni è stato nominato responsabile del trattamento; il fornitore dichiara che la piattaforma è dotata di adeguate misure di sicurezza e protezione (elencate in calce); nei confronti del fornitore si prevede un'attività di controllo mediante audit periodici.	Basso
perdita dell'integrità	Potenziale pregiudizio per l'interessato che dovrebbe nuovamente ricostruire la dinamica di eventuali fatti illeciti segnalati.	Basso	i soggetti coinvolti nel trattamento sono stati autorizzati e applicano elevati standard professionali; gli archivi sono protetti; il fornitore della piattaforma digitale adottata per il ricevimento delle segnalazioni è stato nominato responsabile del trattamento;	Basso

RISCHI INCOMBENTI SUL TRATTAMENTO	CONSEGUENZE	IMPATTO (gravità delle conseguenze)	MISURE DI SICUREZZA ADOTTATE DAL TITOLARE	PROBABILITA' DEL RISCHIO
			il fornitore dichiara che la piattaforma è dotata di adeguate misure di sicurezza e protezione (elencate in calce); nei confronti del fornitore si prevede un'attività di controllo mediante audit periodici.	
perdita della disponibilità	Danno al processo di gestione della segnalazione, o al processo di tutela dei soggetti tutelati dalla normativa whistleblowing.	Basso	i soggetti coinvolti nel trattamento sono stati autorizzati e applicano elevati standard professionali; gli archivi sono protetti; il fornitore della piattaforma digitale adottata per il ricevimento delle segnalazioni è stato nominato responsabile del trattamento; il fornitore dichiara che la piattaforma è dotata di adeguate misure di sicurezza e protezione (elencate in calce); nei confronti del fornitore si prevede un'attività di controllo mediante audit periodici.	Basso

Relativamente ai rischi derivanti dal trattamento svolto mediante la sopra richiamata piattaforma digitale si segnala che la società fornitrice, Whistleblowing Solutions I.S. S.r.l., affidataria della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento è stata designata quale responsabile del trattamento.

Il predetto fornitore dichiara che la piattaforma è dotata dei seguenti requisiti di sicurezza:

CRITTOGRAFIA

L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.

Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2 con SSLLabs rating A. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento. Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption FDE a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto. Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

CONTROLLO DEGLI ACCESSI LOGICI

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238. Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

TRACCIABILITÀ

L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

ARCHIVIAZIONE

L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

GESTIONE DELLE VULNERABILITÀ TECNICHE

L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review. A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente. Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html

BACKUP

I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.

MANUTENZIONE

E' prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza. Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti. Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

SICUREZZA DEI CANALI INFORMATICI

Tutte le connessioni sono protette tramite protocollo TLS 1.2. Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.

SICUREZZA DELL'HARDWARE

I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 724 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 724. I datacenter del fornitore IaaS sono certificati ISO27001.

GESTIRE GLI INCIDENTI DI SICUREZZA E LE VIOLAZIONI DEI DATI PERSONALI

Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati

personali.

LOTTA CONTRO IL MALWARE

Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

Il Titolare reputa che, a fronte delle misure di gestione del rischio applicate al trattamento in questione, i rischi per i diritti e le libertà fondamentali degli interessati siano entro un livello 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.