


<p>Azienda Sanitaria Locale "Città di Torino" Regione Piemonte</p> 	<p>DPIA – Data Protection Impact Assessment</p>	<p>Pag. 1 di 18</p>
--	---	---------------------

DPIA (Data Protection Impact Assessment)

Servizio/Prodotto
"Whistleblowing"

Panoramica del trattamento.....	4
1. Quale è il trattamento in considerazione?.....	4
2. Quali sono le responsabilità connesse al trattamento?	4
3. Ci sono standard applicabili al trattamento?	4
Dati, processi e risorse di supporto.....	5
4. Quali sono i dati trattati e le operazioni di trattamento?.....	5
5. Qual è il ciclo di vita del trattamento dei dati?	5
6. Quali sono le risorse di supporto ai dati?	5
Proporzionalità e necessità.....	5
7. Gli scopi del trattamento sono specifici, espliciti e legittimi?	6
8. Quali sono le basi legali che rendono lecito il trattamento?.....	6
9. I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	6
10. I dati sono esatti e aggiornati?	6
11. Qual è il periodo di conservazione dei dati?	7
Misure a tutela dei diritti degli interessati.....	7
12. Come sono informati del trattamento gli interessati?	7
13. Ove applicabile: come si ottiene il consenso degli interessati?	7
14. Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati? ..	7
15. Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?	7
16. Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?	7
17. Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	8
18. In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?.....	8
Calcolo del rischio.....	9
19. Misure esistenti o pianificate	11
Accesso Illegittimo ai dati (Perdita di riservatezza per accesso non autorizzato o divulgazione non autorizzata)	14
20. Quali sono le fonti di rischio?.....	14
21. In caso di accesso illegittimo ai dati, quali potrebbero essere i principali impatti sugli interessati (rischio inerente da data breach)?	14
22. Quali sono le principali minacce che potrebbero concretizzare il rischio?	14
23. Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	14
24. Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate (rischio inerente Ri e residuo Rr da data breach)?.....	14

25. Come sono gestiti gli incidenti di sicurezza e le violazioni dei dati personali?	15
26. Quali sono le fonti di rischio?	15
27. In caso di modifiche indesiderate ai dati, quali potrebbero essere i principali impatti sugli interessati?	15
28. Quali sono le principali minacce che potrebbero concretizzare il rischio?	15
29. Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	15
30. Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate (rischio inerente Ri e residuo Rr da data breach)?	15
31. Come sono gestite le situazioni che comportano modifiche indesiderate dei dati personali?	16
32. Quali sono le fonti di rischio?	16
33. In caso di perdita dei dati, quali potrebbero essere i principali impatti sui diritti degli interessati?	16
34. Quali sono le principali minacce che potrebbero concretizzare il rischio?	16
35. Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	17
36. Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate (rischio inerente Ri e residuo Rr da data breach) ?	17
37. Come sono gestite le situazioni che comportano la perdita dei dati personali?	17
Ulteriori misure di miglioramento	17
Riferimenti del DPO	18

Panoramica del trattamento

1. *Quale è il trattamento in considerazione?*

L'istituto del whistleblowing, regolato dal recente D.Lgs. 10 marzo 2023, n. 24 e dalle "Linee guida dell'Autorità Nazionale Anticorruzione", approvate con Delibera n. 311 del 12 luglio 2023, è uno strumento diretto a facilitare la segnalazione di illeciti di cui il soggetto segnalante sia venuto a conoscenza nell'ambito del proprio contesto lavorativo, sia in ambito pubblico che privato.

I dati forniti dal soggetto segnalante vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e per l'adozione dei conseguenti provvedimenti.

L'acquisizione e la gestione delle segnalazioni dà luogo a trattamenti di dati personali anche appartenenti a particolari categorie di dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti ad interessati, ovvero alle persone fisiche (identificate o identificabili) che inoltrano la segnalazione o a quelle indicate come possibili responsabili delle condotte illecite o a quelle a vario titolo coinvolte nelle vicende segnalate (art. 4, par. 1, nn. 1 e 2 del Regolamento UE 2016/679).

A tale scopo l'ASL Città di Torino ha deciso di adottare un servizio di Whistleblowing Digitale, basato sul software GlobalLeaks, erogato in modalità Software as a Service (SaaS) e fornito dalla Whistleblowing Solutions Impresa Sociale S.r.l.

La piattaforma informativa di segnalazione è basata su un software libero e open source di cui Whistleblowing Solution è autore e coordinatore di progetto. Oltre a GlobalLeaks, utilizzato in via principale per l'implementazione del servizio di pubblicazione e documentazione e supporto del progetto vengono utilizzate altre tecnologie a codice aperto di pubblico dominio e, limitatamente, alcune tecnologie proprietarie necessarie per finalità di gestione infrastrutturale e backup professionale.

2. *Quali sono le responsabilità connesse al trattamento?*

Titolare del trattamento dei dati personali è l'Azienda Sanitaria Locale "Città di Torino", con sede legale in Torino, Via San Secondo n. 29.

Il Titolare, per la gestione del sistema whistleblowing e per l'esecuzione di operazioni informatizzate di trattamento di dati ai fini della erogazione del servizio, ha designato Responsabile del trattamento dei dati la Whistleblowing Solutions Impresa Sociale S.r.l., P.I. IT09495830961, con sede legale in Milano, via Duca degli Abruzzi 13/A, (d'ora in poi "Whistleblowing Solutions") che, a sua volta, ha designato due sub-responsabili del trattamento:

- Seeweb s.r.l., P.I. 02043220603, con sede legale in Frosinone, C.so Lazio 9/a per la gestione dell'infrastruttura (IaaS);
- Transparency International Italia, CF 97186250151, con sede in **Milano**, Piazzale Carlo Maciachini 11 20159 Milano.

3. *Ci sono standard applicabili al trattamento?*

Il Responsabile del trattamento applica i seguenti standard:

- ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobalLeaks"

- ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud
- ISO27018 per la protezione dei dati personali nei servizi Public Cloud
- Qualifica AGID
- Certificazione CSA Sta

Dati, processi e risorse di supporto

4. Quali sono i dati trattati e le operazioni di trattamento?

Dati personali (art. 4, n. 1, Regolamento UE 2016/679) relativi alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS.

Dati di registrazione (art. 4, n. 1, Regolamento UE 2016/679) ovvero dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione).

Particolari Categorie di dati (art. 9, Regolamento UE 2016/679) eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati.

Dati relativi a condanne penali e reati (art. 10, Regolamento UE 2016/679) eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

5. Qual è il ciclo di vita del trattamento dei dati?

Il trattamento dei dati mediante piattaforma web si può riassumere nelle seguenti macro fasi:

- 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.

6. Quali sono le risorse di supporto ai dati?

Le risorse impiegate per il trattamento in esame comprendono:

- Software di whistleblowing professionale GlobaLeaks
- Infrastruttura IaaS e SaaS privata basata su tecnologie:
 - - VMWARE (virtualizzazione)
 - - Debian Linux LTS (sistema operativo)
 - - VEEAM (backup)
 - - OPNSENSE (firewall)
 - - OPENVPN (vpn)

Proporzionalità e necessità

7. Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati forniti dal segnalante, al fine di rappresentare le presunte condotte illecite delle quali sia venuto a conoscenza in ragione del proprio rapporto di servizio con l'Ente, vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.

Gli scopi perseguiti con il trattamento dei dati, attraverso il sistema denominato "Wistleblowing", risultano, pertanto, specifici, espliciti e leciti, ai sensi dell'art. 5, par. 1, lett. a) del Regolamento UE 679/2016.

8. Quali sono le basi legali che rendono lecito il trattamento?

I trattamenti di dati personali sono necessari per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c), art. 9, par. 2, lett. b) ed art. 10 del Regolamento UE 2016/679, in relazione all'art. 54-bis del D.Lgs. n. 165/2001, nonché per l'esecuzione di un compito di interesse pubblico contemplato dall'ordinamento (art. 6, par. 1, lett. e) ed art. 9, par. 2, lett. g) del Regolamento UE 2016/679).

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

La raccolta dei dati viene effettuata nel rispetto del *principio di minimizzazione dei dati*, di cui all'art. 5, par. 1, lett. c) del Regolamento UE 679/2016, ovvero si svolge in maniera tale da ridurre la gravità dei rischi limitando la raccolta di dati personali al minimo necessario per la specifica finalità. 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 PI).

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 e sono messi a punto da Transparency International Italia in conformità alla normativa vigente in materia.

Nel rispetto del principio di privacy by design, tutti i dispositivi utilizzati, come l'applicativo GlobaLeaks, i log di sistema e i firewall, sono configurati per non registrare alcun tipo di log lesivo dall'anonimato del segnalante quali, ad esempio, indirizzi IP, User Agents e altri Metadata.

L'applicativo GlobaLeaks prevede la possibilità di navigazione tramite Tor Browser per consentire l'accesso in anonimato, con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

10. I dati sono esatti e aggiornati?

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.

11. Qual è il periodo di conservazione dei dati?

I dati sono conservati, di default, per 12 mesi dalla data di segnalazione, prorogabili, da parte del Titolare del trattamento, per singole segnalazioni, per ulteriori 12 mesi. E' prevista la cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere effettuata più volte dal Titolare del trattamento. In ogni caso il periodo di conservazione delle segnalazioni e della relativa documentazione non può superare i cinque anni a decorrere dalla data di comunicazione dell'esito finale della procedura di segnalazione.

Decorsi 15 giorni dalla disattivazione del servizio fornito Whistleblowing Solutions è prevista la Cancellazione dei dati dalla piattaforma, a condizione che non siano presenti sulla piattaforma delle segnalazioni aperte.

Misure a tutela dei diritti degli interessati

12. Come sono informati del trattamento gli interessati?

Gli interessati vengono messi a conoscenza del trattamento mediante apposita informativa ai sensi degli articoli 13 e 14 del Regolamento UE 2016/679, pubblicata sul sito web del Titolare del trattamento nella sezione "Amministrazione Trasparente".

L'informativa è resa in forma concisa, trasparente, intellegibile e facilmente accessibile con un linguaggio chiaro e semplice e contiene in modo trasparente informazioni in merito al trattamento dei dati effettuato.

13. Ove applicabile: come si ottiene il consenso degli interessati?

Non occorre il consenso degli interessati al trattamento dei dati.

Solo quando la contestazione è fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante è indispensabile per la difesa dell'incolpato, la segnalazione, per essere utilizzabile ai fini del procedimento disciplinare, necessita del consenso del segnalante alla rivelazione della propria identità; infatti il Regolamento UE 2016/679 richiede la prestazione del consenso nei seguenti casi: per la rivelazione dell'identità del segnalante a persone diverse da quelle competenti a ricevere o dare seguito alle segnalazioni (art. 12, comma 2, del D.Lgs. n. 24/2023); per la rivelazione dell'identità del segnalante, qualora nell'ambito di procedimento disciplinare, sia indispensabile la sua conoscenza per la difesa dell'incolpato (art. 12, comma 5, del D.Lgs. n. 24/2023).

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

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

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

In forza dell'art. 2-undecies del D.Lgs. 196/2003 (Codice Privacy) i diritti di cui agli artt. da 15 a 22 del Regolamento UE 2016/679 (diritto di accesso dell'interessato, diritto di rettifica, diritto alla cancellazione o all'oblio, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione al trattamento) non possono essere esercitati con richiesta al Titolare del trattamento o con reclamo ai sensi dell'art. 77 del Regolamento qualora, con riferimento all'istituto

del whistleblowing, dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona segnalante.

Inoltre, ai sensi dell'art. 20, paragrafo 3 del Regolamento UE 679/2016, il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Si precisa, tuttavia, che al soggetto segnalato, presunto autore dell'illecito, non è preclusa in termini assoluti la possibilità di esercitare tali diritti. Infatti, l'art. 2-undecies del Codice Privacy stabilisce al suo comma 3, in relazione a specifiche limitazioni ai diritti dell'interessato dallo stesso previste al comma 1, che i diritti in questione possono essere esercitati per il tramite del Garante per la Protezione dei Dati Personali con le modalità dell'art. 160 del Codice medesimo. In tal caso il Garante informa l'interessato di avere eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale.

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

Gli obblighi contrattuali con le seguenti società:

- Whistleblowing Solutions in qualità di Responsabile del trattamento
- Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions
- Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions.

sono definiti nei contratti stipulati con il Titolare del trattamento.

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

I Dati Personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea e non vengono trasferiti verso paesi terzi.

Calcolo del rischio

Il presente paragrafo punta a stimare i rischi per i diritti delle persone fisiche derivanti dal trattamento dei dati personali oggetto della presente DPIA. In particolare, è possibile distinguere tre scenari di rischio:

- “Violazione della riservatezza”, in caso di divulgazione dei dati personali o accessi agli stessi non autorizzati o accidentali;
- “Violazione dell’integrità”, in caso di modifica non autorizzata o accidentale dei dati personali;
- “Violazione della disponibilità”, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Per identificare le misure organizzative e tecniche idonee a prevenire e/o contenere i rischi in un livello accettabile, il rischio deve essere stimato considerando la sua gravità e la probabilità che esso si configuri.

La gravità rappresenta la rilevanza o la portata del rischio, la quale dipende dalla natura del potenziale impatto sugli interessati.

La valutazione della gravità del rischio è effettuata utilizzando la seguente scala:

Livello di gravità del rischio	Descrizione
Trascurabile	Gli individui possono andare incontro a disagi minori che supereranno senza alcun problema (es. sentimento della violazione della privacy senza un danno oggettivo, perdita di tempo nel recuperare i dati, etc.)
Limitata	Gli individui possono andare incontro a disagi significativi che saranno in grado di superare nonostante alcune difficoltà (es. accesso negato a servizi aziendali, stress e disturbi fisici di lieve entità, etc.)
Importante	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (es. sentimento di vulnerabilità o di violazione dei diritti fondamentali, peggioramento della salute, etc.)
Massima	Gli individui possono subire conseguenze significative, o addirittura irreversibili che non sono in grado di superare (es. disagi psicologici a lungo termine o permanenti, morte, etc.)

La probabilità esprime la possibilità che il rischio si realizzi. Per stimare la probabilità che un rischio si verifichi è utilizzata la seguente scala:

Livello di probabilità del rischio	Descrizione
Trascurabile	Non sembra possibile che le fonti di rischio identificate si materializzino in una violazione dei dati personali sfruttando possibili vulnerabilità esistenti nei dispositivi di supporto.
Limitata	Sembra difficile che le fonti di rischio identificate si materializzino in una violazione dei dati sfruttando possibili vulnerabilità esistenti nei dispositivi di supporto.
Importante	Sembra possibile che le fonti di rischio identificate si materializzino in una violazione dei dati sfruttando possibili vulnerabilità esistenti nei dispositivi di supporto.
Massima	Sembra estremamente prevedibile che le fonti di rischio identificate si materializzino in una violazione dei dati sfruttando possibili vulnerabilità esistenti nei dispositivi di supporto.

Il rischio inerente o impatto potenziale è pertanto il risultato di:

- Rischio inerente (impatto potenziale) = **Probabilità * Gravità**

Il rischio residuo, una volta applicate le misure di sicurezza, corrisponde a:

- Rischio residuo = Probabilità * Gravità / Contromisure

Una volta determinati probabilità e gravità per ogni scenario di rischio, e le contromisure già predisposte, è possibile individuare un valore di rischio inerente e residuo, espresso secondo la seguente matrice:

Gravità massima				
Gravità importante				
Gravità limitata				
Gravità minima				
	Probabilità trascurabile	Probabilità limitata	Probabilità importante	Probabilità massima

Il risultato corrisponde a una scala di valori corrispondenti a un livello di rischio basso, medio o alto:

Colore	Livello rischio	Descrizione
	Basso	Rischio accettabile, si può procedere all'implementazione del trattamento
	Medio	Rischio accettabile e trattamento implementabile. Tuttavia, si rende necessaria l'esecuzione di una serie di misure di miglioramento
	Alto	Rischio non accettabile. Rivedere le modalità di trattamento e le relative misure di controllo. Nel caso non sia possibile intervenire sul trattamento, decidere se procedere o meno nell'implementazione e se procedere alla consultazione dell'Autorità Garante per la Protezione dei dati personali.

19. Misure esistenti o pianificate

Misura applicata	Descrizione
Crittografia	<p>L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.</p> <p>Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLabs rating A+.</p> <p>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.</p> <p>Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento</p> <p>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.</p> <p>Protocollo crittografico https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html</p>
Controllo degli accessi logici	<p>L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.</p> <p>Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.</p> <p>Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.</p> <p>Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.</p>

Tracciabilità	<p>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.</p> <p>I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.</p> <p>I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati</p>
Archiviazione	<p>L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM.</p> <p>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.</p>
Vulnerabilità	<p>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.</p> <p>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.</p> <p>Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.htm.</p>
Backup	I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery
Manutenzione	<p>E' prevista manutenzione periodica correttiva, evolutiva e con finalità di migloria continua in materia di sicurezza.</p> <p>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.</p> <p>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.</p>
Sicurezza dei canali informatici	<p>Tutte le connessioni sono protette tramite protocollo TLS 1.2+</p> <p>Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.</p>

Sicurezza dell'hardware	I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24. I datacenter del fornitore IaaS sono certificati ISO27001..
Gestione degli incidenti di sicurezza e violazione 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.

Accesso Illegittimo ai dati (Perdita di riservatezza per accesso non autorizzato o divulgazione non autorizzata)

20. Quali sono le fonti di rischio?

- R1) errori umani senza dolo nei procedimenti amministrativi utilizzando il software
- R2) errori umani con dolo nei procedimenti amministrativi utilizzando il software
- R3) attacchi informatici che minano la continuità operativa
- R4) attacchi informatici che mirano al trasferimento dei dati personali
- R5) errori senza dolo da parte degli amministratori di sistema
- R6) errori con dolo da parte degli amministratori di sistema

21. In caso di accesso illegittimo ai dati, quali potrebbero essere i principali impatti sugli interessati (rischio inerente da data breach)?

- I1) danni economici per gli interessati
- I2) discriminazione sociale ed economica per gli interessati
- I3) alterazione del procedimento amministrativo

Impatti che si possono valutare LIMITATI, ovvero, inconvenienti significativi, ma superabili nonostante alcune difficoltà.

22. Quali sono le principali minacce che potrebbero concretizzare il rischio?

- M1) operatività umana
- M2) attacchi informatici

23. Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Tutte le misure tecniche e organizzative messe in atto contribuiscono a mitigare il rischio. In particolare: Crittografia, Controllo degli accessi logici, Gestione delle Vulnerabilità, Lotta contro il malware, Sicurezza dei canali informatici, Sicurezza hardware.

24. Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate (rischio inerente R_i e residuo R_r da data breach)?

Gravità massima		R_i		
Gravità importante				
Gravità limitata		R_r		
Gravità minima				
	Probabilità trascurabile	Probabilità limitata	Probabilità importante	Probabilità massima

Si ritiene che le misure applicate siano atte ad abbassare la gravità dell'impatto e che la probabilità del rischio stimato sia LIMITATA

25. Come sono gestiti gli incidenti di sicurezza e le violazioni dei dati personali?

Il Responsabile della Struttura aziendale coinvolta nella violazione, e dei dati personali della stessa, che viene a conoscenza di violazioni di sicurezza o di incidenti informatici, ne dà immediata comunicazione al Titolare del trattamento (e per conoscenza al RPD, al Comitato Privacy e alla S.C. Tecnologie), al fine di consentire le valutazioni e gli adempimenti prescritti dalla legge.

Modifiche indesiderate dei dati (perdita di integrità per alterazione)

26. Quali sono le fonti di rischio?

- R1) errori umani senza dolo nei procedimenti amministrativi utilizzando il software
- R2) errori umani con dolo nei procedimenti amministrativi utilizzando il software
- R3) attacchi informatici che minano la continuità operativa
- R4) attacchi informatici che mirano al trasferimento dei dati personali
- R5) errori senza dolo da parte degli amministratori di sistema
- R6) errori con dolo da parte degli amministratori di sistema

27. In caso di modifiche indesiderate ai dati, quali potrebbero essere i principali impatti sugli interessati?

- I1) danni economici per gli interessati
- I2) discriminazione sociale ed economica per gli interessati
- I3) alterazione del procedimento amministrativo

Impatti che si possono valutare LIMITATI, ovvero inconvenienti significativi ma superabili nonostante alcune difficoltà.

28. Quali sono le principali minacce che potrebbero concretizzare il rischio?

- M1) operatività umana
- M2) attacchi informatici

29. Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Tutte le misure tecniche e organizzative messe in atto contribuiscono a mitigare il rischio. In particolare: Crittografia, Controllo degli accessi logici, Gestione delle Vulnerabilità, Lotta contro il malware, Sicurezza dei canali informatici, Sicurezza hardware

30. Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate (rischio inerente Ri e residuo Rr da data breach)?

Gravità massima		Ri		
Gravità importante				
Gravità limitata		Rr		
Gravità minima				
	Probabilità trascurabile	Probabilità limitata	Probabilità importante	Probabilità massima

Si ritiene che le misure applicate, se monitorate e verificate, siano atte ad abbassare la gravità dell'impatto e che la probabilità del rischio stimato sia LIMITATA

31. Come sono gestite le situazioni che comportano modifiche indesiderate dei dati personali?

Il Responsabile della Struttura aziendale coinvolta nella violazione, e dei dati personali della stessa, che viene a conoscenza di violazioni di sicurezza o di incidenti informatici, ne dà immediata comunicazione al Titolare del trattamento (e per conoscenza al RPD, al Comitato Privacy e alla S.C. Tecnologie), al fine di consentirgli le valutazioni e gli adempimenti prescritti dalla legge.

Perdita di dati (perdita di disponibilità temporanea o irreversibile)

32. Quali sono le fonti di rischio?

- R1) errori umani senza dolo nei procedimenti amministrativi utilizzando il software
- R2) errori umani con dolo nei procedimenti amministrativi utilizzando il software
- R3) attacchi informatici che minano la continuità operativa
- R4) attacchi informatici che mirano al trasferimento dei dati personali
- R5) errori senza dolo da parte degli amministratori di sistema
- R6) errori con dolo da parte degli amministratori di sistema

33. In caso di perdita dei dati, quali potrebbero essere i principali impatti sui diritti degli interessati?

- I1) danni economici per gli interessati
- I2) discriminazione sociale ed economica per gli interessati
- I3) alterazione del procedimento amministrativo

Impatti che si possono valutare LIMITATI, ovvero, inconvenienti significativi, ma superabili nonostante alcune difficoltà.

34. Quali sono le principali minacce che potrebbero concretizzare il rischio?

- M1) operatività umana

M2) attacchi informatici

35. Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Tutte le misure tecniche e organizzative messe in atto contribuiscono a mitigare il rischio. In particolare: Crittografia, Controllo degli accessi logici, Gestione delle Vulnerabilità, Lotta contro il malware, Sicurezza dei canali informatici, Sicurezza hardware.

36. Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate (rischio inerente R_i e residuo R_r da data breach) ?

Gravità massima		R_i		
Gravità importante				
Gravità limitata		R_r		
Gravità minima				
	Probabilità trascurabile	Probabilità limitata	Probabilità importante	Probabilità massima

Si ritiene che le misure applicate, se monitorate e verificate, siano atte ad abbassare la gravità dell'impatto e che la probabilità del rischio stimato sia LIMITATA

37. Come sono gestite le situazioni che comportano la perdita dei dati personali?

Il Responsabile della Struttura aziendale coinvolta nella violazione, e dei dati personali della stessa, che viene a conoscenza di violazioni di sicurezza o di incidenti informatici, ne dà immediata comunicazione al Titolare del trattamento (e per conoscenza al RPD, al Comitato Privacy e alla S.C. Tecnologie), al fine di consentirgli le valutazioni e gli adempimenti prescritti dalla legge.

Ulteriori misure di miglioramento

Il presente documento sintetizza una serie di metodologie standard conformi con la normativa vigente in ambito nazionale ed internazionale in materia di trattamento sicuro dell'informazione, privacy e whistleblowing.

A queste si aggiungono ulteriori misure al passo con la ricerca e la tecnica in ambito di sicurezza informatica descritte nelle seguenti pagine web:

- THREAT MODEL <https://docs.globaleaks.org/en/main/security/ThreatModel.html>
- APPLICATION SECURITY <https://docs.globaleaks.org/en/main/security/ApplicationSecurity.html>

Parere del DPO

L'avv. Stefano Comellini, quale Responsabile della Protezione dei Dati dell'ASL Città di Torino, esaminata la suesesa valutazione d'impatto del servizio/prodotto "Whistleblowing", tenuto conto delle misure tecniche e organizzative predisposte per garantire un corretto trattamento dei dati personali, ritiene che i rischi per i diritti e le libertà delle persone fisiche per i previsti trattamenti dei dati personali siano Limitati.

Pertanto, non sussistendo un rischio elevato (come inteso dall'art. 35 del Regolamento UE 2016/679) non risulta necessario procedere alla Consultazione preventiva dell'Autorità di Controllo (prevista dall'art. 36 del medesimo Regolamento).

Riferimenti del DPO

Avv. Stefano Comellini: E-mail: comellini@comellini.it PEC: comellini@ordineavvocatibopec.it