

# Data Privacy Impact Assessment (DPIA)

## Adempimenti Whistleblowing

### Tobanelli S.P.A.

#### ELENCO DELLE REVISIONI

REV.	DATA	NATURA DELLE MODIFICHE	APPROVAZIONE
00	15/12/2023	Prima Emissione	Titolare del trattamento

## 1. Premessa

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito anche "GDPR"), la DPIA corrisponde alla valutazione d'impatto del trattamento del dato sulla protezione dei dati personali, qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ciò considerata la natura, il contesto e le finalità del trattamento.

Il GDPR introduce dunque una valutazione di stampo preliminare, che consente al Titolare del trattamento di prendere visione del rischio prima ancora di procedere al trattamento e di attivarsi perché tale rischio possa essere, se non annullato, quantomeno fortemente ridotto.

I principi fondamentali della DPIA risultano pertanto:

- i diritti e le libertà fondamentali dell'interessato, punto cardine dell'intero impianto del GDPR;
- la gestione dei rischi per la privacy, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio.

Una DPIA poggia su due pilastri:

1. i principi e i diritti fondamentali, i quali sono "non negoziabili", stabiliti dalla legge e che devono essere rispettati e non possono essere soggetti ad alcuna variazione, indipendentemente dalla natura, gravità e probabilità dei rischi;
2. la gestione dei rischi per la privacy dei soggetti interessati, che determina i controlli tecnici e organizzativi opportuni a tutela dei dati personali.

La Metodologia di analisi dei rischi adottata nella conduzione delle attività di Data Privacy Impact Assessment è la metodologia di analisi CNIL del Garante Francese.

## 2. Contesto

### 2.1. Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni ai sensi del D.lgs. n. 24/2023.

La gestione delle segnalazioni viene effettuata attraverso canale esterno (piattaforma web-based adottata dalla Società), di cui vengono riportate le principali caratteristiche.

### 2.2 Responsabilità connesse al trattamento

<b>Ruolo</b>	<b>Nominativo</b>
Titolare del trattamento	Tobanelli S.p.A.
Responsabile del trattamento	Resolve Consulting S.r.l.
Incaricati al trattamento	Cristina Ruffoni Gianangelo Monchieri Simone Guidetti

## 2.3 Standard applicabili al trattamento

Al trattamento in materia di segnalazioni e normativa whistleblowing si applicano le seguenti normative e standard.

Regolamento UE n. 2016/679 (c.d. GDPR)
D.lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D.lgs. n. 101/2018
Direttiva UE 1937/2019
D.lgs. n. 24/2023

## 2.4 Dati, processi e risorse di supporto

Di seguito si riportano le tipologie di dati personali che sono oggetto di trattamento a seguito di una segnalazione fatta ai sensi del D.lgs. n. 24/2023

Categoria di dato personale	Categoria di interessato
Dati personali comuni e di contatto	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto. Fornitori che effettuano una segnalazione o vengono segnalati.
Dati personali particolari (es. dati relativi alla salute, dati relativi all'appartenenza sindacale)	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto. Fornitori che effettuano una segnalazione o vengono segnalati.
Dati giudiziari (es. condanne penali)	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto. Fornitori che effettuano una segnalazione o vengono segnalati.

### Ciclo di vita del trattamento dei dati (descrizione funzionale)

- 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

## 2.5. Risorse a supporto dei dati

Piattaforma Teseo.

## 3. Principi Fondamentali

<b>Gli scopi del trattamento sono specifici, espliciti e legittimi?</b>	Il trattamento è finalizzato esclusivamente alla gestione della segnalazione e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing.
<b>Quali sono le basi giuridiche che rendono lecito il trattamento?</b>	Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge a cui è tenuto il titolare (Art. 6.1. lett. c) GDPR).

<b>I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?</b>	I dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'articolo 12 del D.lgs. n. 24/2023. Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (art. 5.1. lett. c) GDPR).
<b>I dati sono esatti e aggiornati?</b>	Il trattamento dei dati personali relativi alle segnalazioni sono costantemente aggiornati in quanto i soggetti incaricati di ricevere e gestire le segnalazioni ne verificano preliminarmente la corrispondenza a verità.
<b>Qual è il periodo di conservazione dei dati?</b>	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, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 14/2023.

### 3.1. Misure a tutela dei diritti degli interessati

<b>Come sono informati del trattamento gli interessati?</b>	Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR. L'informativa viene resa disponibile secondo le seguenti modalità: <ul style="list-style-type: none"> <li>- Processo comunicazione aziendale sull'esistenza del canale di segnalazione interno (canale informatico);</li> <li>- Pubblicazione sito internet – sezione dedicata al Whistleblowing</li> <li>- In apertura della piattaforma</li> </ul>
<b>Ove applicabile: come si ottiene il consenso degli interessati?</b>	Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati al trattamento non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (Art. 6.1. lett. c) del GDPR). Nel caso invece ricorra l'ipotesi di comunicazione dei dati personali a soggetti diversi da quelli espressamente autorizzati dal Titolare, il segnalante dovrà prestare il suo consenso specifico alla segnalazione tramite piattaforma ai sensi degli artt. 6.1. lett. a) e 7 del GDPR.
<b>Come fanno gli interessati a esercitare i loro diritti previsti dagli artt. 15 ss. GDPR?</b>	Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR attraverso l'indirizzo di posta elettronica dedicato <a href="mailto:privacy@tobanellispa.it">privacy@tobanellispa.it</a> , nei limiti di cui all'articolo 2-undecies del Codice Privacy.
<b>Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?</b>	Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili del trattamento ai sensi dell'art. 28 GDPR, attraverso contratti o altri atti giuridici
<b>In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?</b>	Per questa tipologia di trattamento non è previsto un trasferimento di dati personali fuori dall'Unione Europea.

#### 4. Misure esistenti

<b>Crittografia</b>	Implementata secondo le policies GlobaLeaks <a href="https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html">https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html</a>
<b>Controllo degli accessi logici</b>	Log accessi da parte dei soggetti destinatari delle segnalazioni. Log ricezione delle segnalazioni (di cui non viene tenuta traccia). I riceventi accedono tramite apposito account personale. Credenziali di accesso vengono generate dell'utente e devono essere generate credenziali di accesso (minimo dieci caratteri, di cui 7 caratteri diversi e almeno 3 con diversi caratteri, maiuscole, minuscola, numeri, simbolo).
<b>Tracciabilità</b>	Log di audit che identificano le attività che avvengono sulla piattaforma Log Utenti Log Segnalazioni Log Attività pianificate
<b>Archiviazione</b>	Datacenter situato in Italia di Aruba con elevati standard di sicurezza Data Center Rating 4 (Former Tier 4) <a href="https://www.datacenter.it/data-center-aruba/italia-bergamo-dc-it3.aspx">https://www.datacenter.it/data-center-aruba/italia-bergamo-dc-it3.aspx</a>
<b>Gestione delle vulnerabilità tecniche</b>	<a href="https://www.datacenter.it/data-center-aruba/italia-bergamo-dc-it3.aspx">https://www.datacenter.it/data-center-aruba/italia-bergamo-dc-it3.aspx</a>
<b>Backup</b>	La macchina virtuale è ridondata (in caso di danno fisico a un disco o a una macchina, ne esiste una sua copia che subentra automaticamente)
<b>Manutenzione</b>	In caso di manutenzione viene spenta la macchina che viene archiviata, attivato uno snapshot per poi procedere alla manutenzione (backup che poi può essere ripristinato).
<b>Sicurezza dei canali informatici</b>	Piattaforma accessibile tramite protocollo https oppure tramite connettività onion routing browser (Tor).
<b>Sicurezza dell'hardware</b>	<a href="https://www.datacenter.it/data-center-aruba/italia-bergamo-dc-it3.aspx">https://www.datacenter.it/data-center-aruba/italia-bergamo-dc-it3.aspx</a>
<b>Lotta contro il malware</b>	Accessibile solo e esclusivamente tramite https.
<b>Politica di tutela della privacy</b>	La società adotta un Modello Organizzativo sulla protezione dei dati personali.
<b>Gestione dei rischi</b>	L'analisi dei rischi viene condotta secondo metodologia CNIL.
<b>Gestire gli incidenti di sicurezza e le violazioni dei dati personali</b>	Gli incidenti di sicurezza e le violazioni dei dati personali vengono gestiti secondo la "Procedura Data Breach" adottata dalla Società in conformità a quanto prescritto dagli artt. 33-34 del GDPR.
<b>Vigilanza sulla protezione dei dati</b>	Vigilanza svolta da DPO/Comitato Privacy/funzioni incaricate dal Titolare del trattamento (a secondo di quanto definito nell'organigramma privacy aziendale).

## 5. Rischi

Matrice R = P x G					
	Probabilità	1 - Trascurabile	2 – Limitata	3 – Importante	4 – Massima
Gravità	1 - Trascurabile	1	2	3	4
	2 – Limitata	2	4	6	8
	3 – Importante	3	6	9	12
	4 – Massima	4	8	12	16

### In riferimento alla procedura “Valutazione del Rischio\_Trattamenti ad Alto rischio”

Come indicato dal considerando 76, l'azienda si è dotata di un sistema di calcolo del rischio basato su **parametri oggettivi**, al fine di stabilire se esiste un rischio o un rischio elevato per il trattamento specifico. L'Oggettivazione del rischio pertanto passa attraverso un modello di creazione della probabilità e della Gravità in grado di rispecchiare il contesto in cui l'organizzazione opera. Sono state identificate griglie oggettive di calcolo delle Probabilità e Gravità con riguardo ai diritti e libertà dell'interessato.

Gravità	Significato	Descrizione generica degli impatti (diretti e indiretti)
4	Massima	I soggetti interessati possono incontrare conseguenze irreversibili.
3	Importante	I soggetti interessati possono incontrare conseguenze significative, e difficoltà nella loro risoluzione, ma comunque superabili.
2	Limitata	I soggetti interessati possono incontrare inconvenienti superabili.
1	Trascurabile	Gli interessati non saranno coinvolti o potrebbero incontrare alcuni lievi inconvenienti senz'altro superabili.

Probabilità	Significato	Criterio di scelta
4	Massima	Il verificarsi del danno dipende da condizioni direttamente connesse alla situazione; Il verificarsi del danno non provocherebbe alcuna reazione di stupore; Eventi simili sono già accaduti in azienda o in aziende dello stesso tipo
3	Importante	Il verificarsi del danno dipende da condizioni non direttamente connesse alla situazione ma possibili; Il verificarsi del danno provocherebbe reazioni di moderato stupore; Eventi simili sono stati già riscontrati
2	Limitata	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili si sono verificati molto raramente

1	Trascurabile	<p>Il verificarsi del danno è subordinato a un concatenamento di eventi indipendenti tra loro;</p> <p>Il verificarsi del danno è creduto impossibile dagli addetti;</p> <p>Non è mai accaduto nulla di simile</p>
---	--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#### Valutazione % delle Misure Esistenti

Rating	Descrizione
1-25%	Non adeguate
26-50%	Minime
51-75%	Adeguate

#### Rating rischio residuo (Rr)

Rischio Alto	6,1-16
Rischio Medio	3,1-6
Rischio Basso	1-3

Elementi per la valutazione:

- a. **Ri** è il valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione
- b. L'azienda valuta come Rischio Accettabile (**Ra**) = 3
- c. Se il rischio inerente **Ri** a seguito delle valutazioni oggettive, dovesse risultare superiore ad **Ra**, l'azienda interverrà con mitigazioni opportune tali che ad **Rr < Ra**

## 5.1 Analisi dei rischi

### 5.1.1. Accesso illegittimo – Perdita della riservatezza

<b>GRAVITÀ (G)</b>	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative, Ritorsioni.				
<b>PROBABILITÀ (P)</b>	Il verificarsi del danno dipende da condizioni imprevedute Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili si sono verificati molto raramente				
<b>FONTI DI RISCHIO</b>	<p>Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale)</p> <p>Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker)</p> <p>Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)</p>				
<b>MISURE</b>	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento				
<b>CALCOLO DEL RISCHIO INERENTE</b>	G	P	Ri	Mitigazione % abbattimento rischio	Rr
	3	2	6	70%	1,8

### 5.1.2. Modifiche indesiderate – Perdita dell'integrità

<b>GRAVITÀ (G)</b>	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio; Diffusione indesiderata dei propri dati; Consultazione dei propri da parte di personale non autorizzato; Ricatto economico; Problematiche di natura giuslavoristica e contrattuale; Mobbing; Discriminazioni lavorative.				
<b>PROBABILITÀ (P)</b>	Il verificarsi del danno dipende da condizioni impreviste. Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti. Eventi simili si sono verificati molto raramente.				
<b>FONTI DI RISCHIO</b>	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici).				
<b>MISURE</b>	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento.				
<b>CALCOLO DEL RISCHIO INERENTE</b>	<b>G</b>	<b>P</b>	<b>Ri</b>	<b>Mitigazione % abbattimento rischio</b>	<b>Rr</b>
	3	2	6	70%	1,8

### 5.1.3. Perdita del dato – Perdita della disponibilità

<b>GRAVITÀ (G)</b>	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio; Diffusione indesiderata dei propri dati; Consultazione dei propri da parte di personale non autorizzato; Ricatto economico; Problematiche di natura giuslavoristica e contrattuale; Mobbing; Discriminazioni lavorative.				
<b>PROBABILITÀ (P)</b>	Il verificarsi del danno dipende da condizioni impreviste. Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti. Eventi simili si sono verificati molto raramente.				
<b>FONTI DI RISCHIO</b>	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici).				
<b>MISURE</b>	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento.				
<b>CALCOLO DEL RISCHIO INERENTE</b>	<b>G</b>	<b>P</b>	<b>Ri</b>	<b>Mitigazione % abbattimento rischio</b>	<b>Rr</b>
	3	2	6	70%	1,8

## 6. Parere delle parti interessate

Non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento rappresentano l'adempimento di obblighi di legge. Ai fini dell'attivazione del canale di segnalazione interna, gli enti devono sentire le rappresentanze o le organizzazioni sindacali.

## 7. Parere DPO (se nominato)

Esempio: il DPO esprime il proprio parere favorevole alla DPIA effettuata con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conformi al dettato normativo.

## 8. Conclusioni

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emergono "rischi inerenti (Ri)" con impatto sui diritti e libertà degli interessati con stima a valore Medio. Nell'ottica di mitigazione di tali rischi, si evince che, con l'implementazione delle misure tecnico/organizzative pianificate ad integrazione di quelle già messe in atto, il valore di rischio residuo rientra nei parametri accettabili uguali o minori rispetto al Rischio accettato (Ra) dall'organizzazione aventi stima a *valore Basso*, valore ritenuto accettabile dall'organizzazione in relazione ai parametri oggettivi considerati.

Si ritiene pertanto che il trattamento in oggetto presenta un grado di rischio sui diritti e libertà dell'interessato rientrante nei parametri accettabili e di conseguenza *non è richiesta una consultazione preventiva all'Autorità Garante*.