VALUTAZIONE D'IMPATTO

AI SENSI DEL REGOLAMENTO EUROPEO N. 679/2016 E DEL COMBINATO DISPOSTO DI CUI AGLI ARTT. 4 E 13 DEL DLGS N. 24/2023 IN TEMA DI

WHISTLEBLOWING

E RISPETTO ALLE INFORMAZIONI DI CUI ALLA GESTIONE DEL CANALE DI SEGNALAZIONE

Informazioni sulla PIA

Il Regolamento Europeo n. 679/2016 (GDPR) costituisce una significativa svolta in tema di protezione e corretta circolazione dei dati personali, poiché la detta protezione è stata elevata a categoria di diritto fondamentale della persona. Tale diritto dovrà essere oggetto di un adeguato bilanciamento con altri interessi della persona, anch'essi a rilevanza primaria, perché, ad esempio, funzionali alla tutela di altri diritti ed interessi.

In taluni casi di trattamento è necessario precostituire un apparato documentale, idoneo a dimostrare di aver valutato i **prevedibili rischi** e le azioni necessarie per la protezione dei dati attraverso un **documento**, denominato «***valutazione d'impatto***» («*data protection impact assessment*»: DPIA ex art. 35 del GDPR), inteso dal Legislatore Europeo come strumento di valutazione indispensabile anche per rispettare il principio di **responsabilizzazione**.

Tale documento è perciò necessario al fine di poter comprovare di essersi attivati in relazione a quanto disposto dal comma 6 dell'art. 13 del **Dlgs n. 24/2023** che attua la direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio del 23/10/2019, recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato.

Il Decreto legislativo in questione prevede, in particolate, al proprio **art. 4**, rubricato "***Canali di segnalazione interna***", che:

- "*I soggetti del settore pubblico e i soggetti del **settore privato**, sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015, **attivano**, ai sensi del presente articolo, propri **canali di segnalazione**, **che garantiscano**, anche tramite il ricorso a strumenti di crittografia, **la riservatezza dell'identità della persona segnalante**, della **persona coinvolta** e della persona **comunque menzionata nella segnalazione**, nonché del **contenuto** della segnalazione e della relativa documentazione. I modelli di organizzazione e di gestione, di cui all'articolo 6, comma 1, lettera a), del decreto*

legislativo n. 231 del 2001, prevedono i ***canali di segnalazione*** *interna di cui al presente decreto;*

- La gestione del canale di segnalazione ***è affidata a una persona*** *o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero è affidata* ***a un soggetto esterno****, anch'esso* ***autonomo*** *e con personale specificamente formato.*

- Le segnalazioni sono effettuate ***in forma scritta****, anche con modalità informatiche,* ***oppure in forma orale****. Le segnalazioni interne in forma orale sono effettuate attraverso* ***linee telefoniche*** *o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante* ***un incontro diretto*** *fissato entro un termine ragionevole*".

- Il Dlgs n. 24/2023, al proprio **art. 5** ("***Gestione del canale di segnalazione interna***"), prevede altresì che "*la persona o l'ufficio interno* ***ovvero il soggetto esterno****, ai quali è affidata la* ***gestione del canale di segnalazione*** *interna svolgono le seguenti attività*:

(a) *rilasciano alla persona segnalante* ***avviso*** *di ricevimento della segnalazione entro* ***sette giorni*** *dalla data di ricezione;*

(b) *mantengono le interlocuzioni con la persona segnalante e possono richiedere a quest'ultima, se necessario,* ***integrazioni****;*

(c) *danno diligente* ***seguito*** *alle segnalazioni ricevute;*

(d) *forniscono* ***riscontro*** *alla segnalazione entro* ***tre mesi*** *dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione*;

(e) *mettono a disposizione* ***informazioni chiare sul canale****, sulle* ***procedure*** *e sui* ***presupposti*** *per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne. Le suddette informazioni sono esposte e rese facilmente visibili* ***nei luoghi di lavoro****, nonché accessibili alle persone che pur non frequentando i luoghi di lavoro intrattengono un rapporto giuridico in una delle forme di cui all'art. 3, commi 3 o 4.*

Rispetto a tali incombenti e, in particolare, relativamente alle lettere a), b), c), d) dell'anzidetto art. 5 del Decreto legislativo in parola, chi gestirà il canale di segnalazione dovrà, necessariamente, trattare una serie di informazioni contenenti dati personali.

o0o

Avuto riguardo al trattamento di dati personali conseguenti alla ridetta gestione, l'**art. 13** del Dlgs n. 24/2023 (rubricato "***Trattamento dei dati personali***") dispone, ancora più specificatamente per quanto qui rileva, quanto segue:

- "***Ogni trattamento*** *dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dal presente decreto,* ***deve essere effettuato a norma del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196*** *e del decreto legislativo 18 maggio 2018, n. 51. La comunicazione di dati personali da parte delle istituzioni, degli organi o degli organismi dell'Unione europea è effettuata in conformità del regolamento (UE) 2018/1725.*

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

*- I diritti di cui agli articoli **da 15 a 22 del regolamento (UE) 2016/679** possono essere **esercitati** **nei limiti** di quanto previsto **dall'articolo 2-undecies** del Dlgs 196/2003.*

o0o

Da annotare subito che l'**art. 2-undecies del Dlgs 196/2003** (rubricato: "***Limitazioni ai diritti dell'interessato***") prevede testualmente quanto segue che:

1. **I diritti di cui agli articoli da 15 a 22** del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:

a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;

b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;

c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché' alla tutela della loro stabilità;

e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;

f) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio;

f-bis) agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale.

2. Nei casi di cui al comma 1, lettera c), si applica quanto previsto dai regolamenti parlamentari ovvero dalla legge o dalle norme istitutive della Commissione d'inchiesta.

3. Nei casi di cui al comma 1, lettere a), b), d), **e)**, **f)** e f-bis) i diritti di cui al medesimo comma sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del Regolamento. L'esercizio **dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato**, a **meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata**, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere a), b), d), **e)**, **f)** e f-bis). **In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'articolo 160**. In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. Il titolare del trattamento informa l'interessato delle facoltà di cui al presente comma.

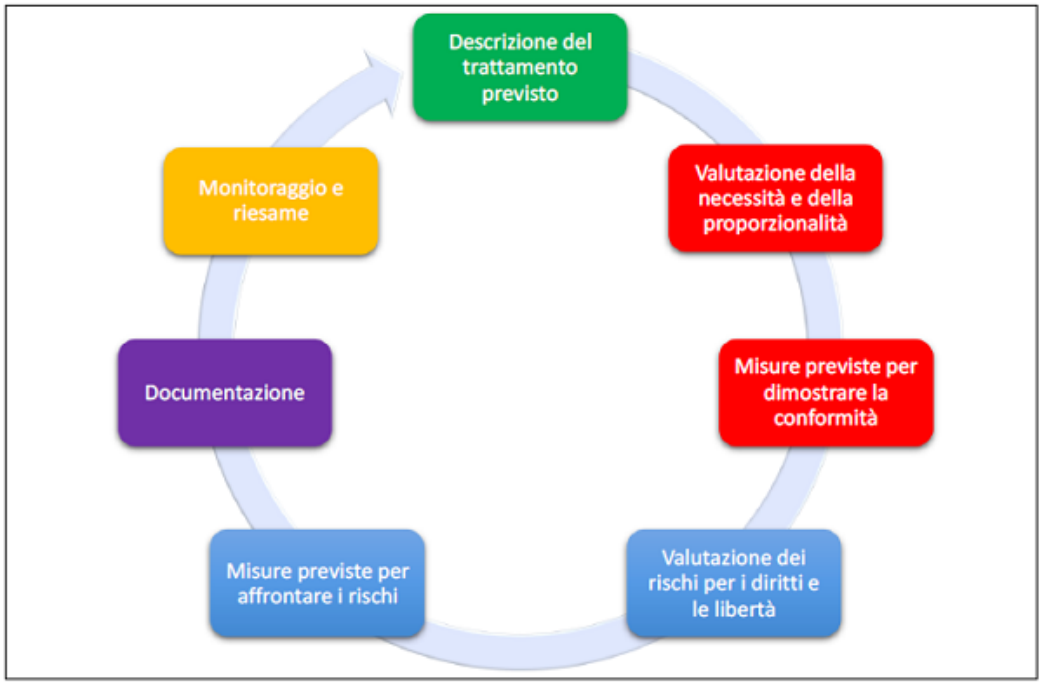
o0o

*- I trattamenti di dati personali relativi al ricevimento e **alla gestione delle segnalazioni sono effettuati dai soggetti di cui all'articolo 4**, in qualità di **titolari del trattamento**, nel rispetto dei principi di cui agli articoli 5 e 25 del regolamento (UE) 2016/679 o agli articoli 3 e 16 del decreto legislativo n. 51 del 2018, **fornendo idonee informazioni** alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679 o dell'articolo 11 del citato decreto legislativo n. 51 del 2018, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.*

- I soggetti del settore pubblico e i soggetti del settore privato che condividono risorse per il ricevimento e la gestione delle segnalazioni, ai sensi dell'articolo 4, comma 4, determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali, ai sensi dell'articolo 26 del regolamento (UE) 2016/679 o dell'articolo 23 del decreto legislativo n. 51 del 2018.

- (comma 6) *I soggetti di cui all'articolo 4 **definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato** agli specifici rischi derivanti dai trattamenti effettuati, sulla base di **una valutazione d'impatto sulla protezione dei dati**, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018*".

I passaggi di cui allo svolgimento della D.P.I.A., nel prosieguo esposti in separati paragrafi, possono così sintetizzarsi.



Schematizzato sopra il contenuto del documento si debbono evidenziare pure le modalità redazionali unitamente ad altre considerazioni in ordine alla sua natura.

In generale, ai sensi dell'art. 35, Reg. U.E. 679/2016, «*le valutazioni di impatto mirano a svolgere un'analisi sistematica*» del trattamento dei dati personali. Quanto detto presuppone che la valutazione sia calata in un determinato contesto che, nel caso in oggetto, è riferito alla gestione del canale di segnalazione interna da parte di soggetto esterno ai sensi dell'art. 4 del Dlgs n. 24/2023 (segnatamente da parte di Lorenzo Tamos).

Rispetto al citato contesto la valutazione d'impatto in esame è da considerasi unitaria, poiché le tipologie di trattamento riferibili a tale compito, ancorché plurime nel loro possibile realizzarsi, presentano **caratteristiche omogenee** (se non *standard*) in termini di natura, finalità di trattamento, ambito, contesto, e tipologie di rischi.

Il documento sarà oggetto da parte di Lorenzo Tamos di monitoraggio nel corso dell'intero ciclo di vita del trattamento, al fine di garantire l'individuazione di ulteriori soluzioni che potranno agevolare e sempre più migliorare l'osservanza degli obblighi previsti e delle misure di sicurezza necessarie, oltre agli indispensabili adeguamenti in caso di nuovi interventi normativi.

CONTATTI		
Responsabile della gestione del canale di segnalazione	Avv. Lorenzo Tamos	n. di tel. 0270006392 n. di fax 0276113344 *email* lorenzo.tamos@avvocatinteam.com pec lorenzo.tamos@milano.pecavvocati.it cell. 339 6438001

IL TRATTAMENTO

1. Quale è il trattamento in considerazione?

Il trattamento in questione è esclusivamente quello di cui al già menzionato Dlgs n. 24/2023 che prevede, in particolate al proprio **art. 4**, rubricato "***Canali di segnalazione interna***", quanto segue in relazione ai flussi di dati personali che il soggetto esterno gestore del canale interno di segnalazione verrà a potenzialmente trattare:

"*1. I soggetti del settore pubblico e i soggetti del **settore privato**, **sentite le rappresentanze o le organizzazioni sindacali** di cui all'articolo 51 del decreto legislativo n. 81 del 2015, **attivano**, ai sensi del presente articolo, propri **canali di segnalazione**, **che garantiscano**, anche tramite il ricorso a strumenti di crittografia, **la riservatezza dell'identità della persona segnalante**, della **persona coinvolta** e della persona **comunque menzionata nella segnalazione**, nonché del **contenuto** della segnalazione e della relativa documentazione. I modelli di organizzazione e di gestione, di cui all'articolo 6, comma 1, lettera a), del decreto legislativo n. 231 del 2001, prevedono i canali di segnalazione interna di cui al presente decreto.*

*2. La gestione del canale di segnalazione **è affidata a una persona** o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero è affidata **a un soggetto esterno**, anch'esso **autonomo** e con personale specificamente formato.*

*3. Le segnalazioni sono effettuate **in forma scritta**, anche con modalità informatiche, **oppure in forma orale**. Le segnalazioni interne in forma orale sono effettuate attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole*".

Sempre il Dlgs n. 24/2023, al proprio **art. 5** ("***Gestione del canale di segnalazione interna***"), prevede altresì che "*la persona o l'ufficio interno **ovvero il soggetto esterno**, ai quali è affidata la **gestione del canale di segnalazione** interna svolgono le seguenti attività*:

> ***(a)** rilasciano alla persona segnalante **avviso** di ricevimento della segnalazione entro **sette giorni** dalla data di ricezione;*
>
> ***(b)** mantengono le interlocuzioni con la persona segnalante e possono richiedere a quest'ultima, se necessario, integrazioni;*
>
> ***(c)** danno diligente **seguito** alle segnalazioni ricevute;*
>
> ***(d)** forniscono **riscontro** alla segnalazione entro **tre mesi** dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione*;
>
> ***(e)** mettono a disposizione **informazioni chiare sul canale**, sulle **procedure** e sui **presupposti** per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne. Le suddette informazioni sono esposte e rese facilmente visibili **nei luoghi di lavoro**, nonché accessibili alle persone che pur non frequentando i luoghi di lavoro intrattengono un rapporto giuridico in una delle forme di cui all'art. 3, commi 3 o 4.*

*Se dotati di un proprio **sito internet**, i soggetti del settore pubblico e del settore privato pubblicano le informazioni di cui alla presente lettera anche in una sezione dedicata del suddetto sito*".

2. Quali sono le responsabilità connesse al trattamento?

Le responsabilità civili ed amministrative connesse al trattamento in oggetto sono, anzitutto, quelle previste dal Dlgs n. 24/20203 e, correlativamente, dal Regolamento UE 2016/679, nonché dal Dlgs n. 196/2003 ossia, in particolare, quelle di cui agli artt. 82 e 83 del GDPR, ovvero quelle di cui agli artt. da 75 a 97 e da 166 a 172 del detto Decreto.

Le responsabilità connesse al trattamento di dati personali possono così riassumersi: responsabilità civile; responsabilità amministrativa; responsabilità civile ed amministrativa del gestore del canale, autonoma o in via solidale con il titolare del trattamento; responsabilità civile e disciplinare di un designato/autorizzato al trattamento; responsabilità civile di un collaboratore interno/esterno; responsabilità penale degli autori del reato ed eventuale (correlabili rispetto al trattamento e protezione dei dati) responsabilità dell'Ente ex Dlgs n. 231/2001.

3. Ci sono standard applicabili al trattamento?

Allo stato, non vi sono standard specifici applicabili al trattamento di cui al Dlgs n. 24/2023. Lorenzo Tamos monitora la redazione e pubblicazione delle linee guida ovvero dei codici di condotta, ovvero ancora delle misure di garanzia adeguando il relativo trattamento alle migliori prassi e procedure di trattamento atte a proteggere i dati personali.

Valutazione: Accettabile

Quali sono i dati trattati?

Le categorie di dati personali trattamenti sono così sinteticamente tratteggiate:

- dati "generici" (nome, cognome, eventuale indirizzo *email*; riferimenti anagrafici). Al proposito i soggetti interessati possono essere i seguenti: soci-lavoratori; amministratori; soci-lavoratori coordinatori dei servizi; collaboratori volontari e non; fornitori; professionisti esterni; legali rappresentanti/amministratori di *partners* economici; lavoratori di partners economici; utenti; potenziali utenti; familiari degli utenti; amministratori di sostegno; assistenti sociali; personale di enti pubblici o pubbliche amministrazioni; persone decedute ovvero gli eredi/soggetti legittimati;
- dati particolari, ai sensi dell'art. 9, Reg. UE n. 679/2016 inerenti alla gestione del rapporto lavorativo ed associativo, ovvero dati relativi alla salute (o altre tipologie di dati particolari);
- categoria di dati giudiziari o di reato ex art. 10 del GDPR.

Le persone che potrebbero accedere ai dati personali sono, a seconda dei casi, i responsabili del trattamento appositamente nominati con atto scritto, nonché le persone designate (cioè autorizzate) al trattamento dei dati personali.

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

Il ciclo di vita del trattamento dei dati è stabilito dagli adempimenti di cui al Dlgs n. 24/2023 e, in particolare, in base agli adempimenti di cui agli artt. 4 e 5 del medesimo Decreto, tenuto conto che l'art. 14 del ridetto Dlgs n. 24/2023 impone che, le segnalazioni, interne ed esterne, e la relativa documentazione da cui possono emergere dati personali, siano 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, nel rispetto degli obblighi di riservatezza.

Quali sono le risorse di supporto ai dati?

I dati trattati sono ospitati/trattati su risorse tecniche e strutturali: sistemi operativi locali; server (e/o/su) host dedicato; rete interna dedicata; faldoni riposti in scaffali in ambienti protetti e soggetti a misure di sicurezza fisica.

Precisamente (ma impregiudicato quanto meglio evidenziato nella sezione «*misure esistenti*» del presente documento), i dati personali raccolti ed archiviati elettronicamente, sono conservati su memorie protette e ridondanti, implementate con tecnologia apposita e protetti da antivirus.

Valutazione: Accettabile

PRINCIPI FONDAMENTALI

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento sono specifiche, esplicite e legittime. Le stesse sono individuate in modo chiaro dalla legge e sono connesse allo scopo legittimo che si deve perseguire nel rispetto degli altri obblighi correlati che derivano dallo svolgimento del proprio compito.

Le finalità, inoltre, sono esplicite in quanto previste dalla legge ed illustrate nei c.d. Registri del trattamento (art. 30 Reg. UE n. 679/2016), nonché nelle informative fornite, consegnate e anche pubblicamente diffuse mediante affissioni (ex artt. 12 e ss. Reg. UE n. 679/2016).

Trattasi quindi di scopi legittimi perseguiti nel rispetto del principio di liceità ed in osservanza ad un obbligo legale.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Ai sensi dell'art. 6, del Reg. UE n. 679/2016, le basi giuridiche dei trattamenti, in generale, sono le seguenti che, nel caso, in considerazione del servizio erogati, sono: i) obbligo legale; ii) contratto; iii) esecuzione di un compito di interesse pubblico; iv) il consenso (residualmente ove espresso dall'interessato in base al Dlgs n. 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)?

Si. I dati raccolti sono adeguati, pertinenti, limitati a quanto è necessario compiere rispetto alle finalità perseguite, ossia adeguati in base agli adempimenti previsti dal Dlgs. 24/2023. Invero, non sussiste alcun interesse e/o utilità, nemmeno ipotetica, a raccogliere dati oltre quelli strettamente necessari e previsti dalla legge per attuare le finalità di erogazione dei servizi di gestione del canale di segnalazione.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

Si. I dati trattati sono esatti ed aggiornati poiché, di fondo, è necessario che lo siano sin dall'origine per eseguire correttamente il servizio di gestione del canale di segnalazione. Nell'ambito delle informative fornite, che di per loro indicano quali dati personali indicare, è oltretutto espressamente indicata e facilitata la facoltà degli interessati di rettificare, integrare e/o cancellare i dati non corretti e/o obsoleti, ovvero le indicazioni per esercitare i diritti agli stessi spettanti.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Il periodo di conservazione dei dati è essenzialmente basato sui relativi obblighi di legge di cui, in primis, all'art. 14 del Dlgs 24/2023 che dispone come le segnalazioni, interne ed esterne, e la relativa documentazione da cui possono emergere dati personali 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, nel rispetto degli obblighi di riservatezza.

Valutazione: Accettabile

Piano d'azione / misure correttive:

Ulteriori azioni di monitoraggio al fine di individuare casi peculiari rispetto al periodo di conservazione massimo, ovvero nel caso in cui, per motivi inerenti alla difesa in giudizio di diritti la conservazione debba essere prolungata.

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Come sono informati del trattamento gli interessati?

Gli interessati sono informati in ordine agli elementi principali del trattamento mediante spiegazioni scritte semplificate, al fine di renderli consapevoli e edotti sulle principali caratteristiche dello stesso. Vi sono delle informative per il trattamento dei dati personali, utilizzate appositamente per informare gli interessati rispetto al trattamento da segnalazione ai sensi del Dlgs. 24/2023.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

In base al Dlgs 24/2023 il rilascio del consenso da parte dell'interessato segnalante è previsto e delimitato ad alcune ipotesi di cui alla gestione delle segnalazioni. In ogni caso, le modalità di ottenimento del consenso, ove prevedibile e legittimo, sono le seguenti: rilascio all'interessato di adeguata informativa per il trattamento dei dati personali; redazione dell'informativa anche nel rispetto del criterio di c.d. granularità del consenso; descrizione delle caratteristiche del trattamento e delle finalità per cui può essere espresso; ulteriore spiegazione orale preventiva anche o solo su richiesta dell'Interessato o del soggetto legittimato.

Inoltre, tramite la documentazione resa pubblica presso le sedi operative, gli interessati sono resi edotti circa la possibilità di esercitare il diritto di revoca del consenso eventualmente prestato e circa le conseguenze della revoca anche sul trattamento pregresso.

Valutazione: Accettabile

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

Presso la sede amministrativa e legale, il sito web e le sedi operative, sono rese disponibile ai soggetti interessati le informazioni per consentire agli stessi di esercitare agevolmente i propri diritti di cui agli artt. 15 e seguenti del Reg. UE n. 679/2016. Inoltre, la pubblicazione dei dati di contatto agevola gli interessati ad esercitare tutti i propri diritti ove esercitabili *ex lege*.

Valutazione: accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?
Si rinvia a quanto sopra esposto.

Valutazione: Accettabile

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

Si rinvia a quanto sopra esposto.

Valutazione: Accettabile

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

Ove la norma si renda applicabile, si.

Valutazione: accettabile

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

Non si trattano dati personali al di fuori dell'Unione Europea.

Valutazione: Accettabile

RISCHI
MISURE ESISTENTI O PIANIFICATE

A) Controllo degli accessi logici

Sono effettuati periodicamente *test* di resistenza rispetto agli archivi informatici.

Valutazione: Accettabile

B) Archiviazione

Tutti i dati personali raccolti ed archiviati elettronicamente, sono conservati su memorie ridondanti, implementate attraverso tecnologia apposita, al fine di assicurare l'integrità dei dati stessi, e la possibilità di un loro recupero anche in caso di un guasto ad un *hard disk*.

Valutazione: Accettabile

C) Lotta contro il malware

I "PC Client" e il server di riferimento sono protetti da Software *Antivrus* e *Antispyware*. Gli Antivirus sono sempre aggiornati.

Valutazione: Accettabile

D) Vulnerabilità

I programmi informatici sono regolarmente aggiornati. Anche per quanto riguarda i Sistemi Operativi gli aggiornamenti vengono eseguiti regolarmente.

Valutazione: Accettabile

E) Backup

Per tutti i dati personali (e misti con quelli non personali) archiviati in dispositivi elettronici è prevista una procedura che contempla un *backup* completo e una serie di *backup* incrementali.

Valutazione: Accettabile

F) Gestione postazioni

Relativamente all'accesso fisico ai personal computer locali, va osservato che i p.c. sono utilizzati soltanto per l'accesso al terminal *server*, con un account nominale, tramite autenticazione attraverso username e password su Dominio.

I dati a cui è consentito l'accesso vengono raggiunti tramite *desktop* remoto. In caso di inutilizzo, viene disabilitato l'*account* e sono resi invalidi i dati di convalida all'accesso. Esistono istruzioni affinché chi abbandona anche solo momentaneamente la postazione di lavoro, ha l'obbligo di rendere la stazione inaccessibile.

Valutazione: accettabile

G) Controllo degli accessi fisici

Gli uffici sono dotati di porta blindata, misure antiintrusione alle finestre ed allarme interno a sensore di movimento. La stanze ove si trovano i fascicoli cartacei sono presidiate negli orari di servizio e, di norma, chiudibili a chiave fuori servizio.

Valutazione: Accettabile

H) Sicurezza dei siti web

Al sito web sono applicate le misure di sicurezza necessarie. I trattamenti tramite sito web sono circoscritti al minimo.

Valutazione: Accettabile

I) Gestione del personale

Le iniziative di sensibilizzazione del personale (composto da professionisti che già conoscono bene la materia e vincolati da obblighi deontologici e di riservtezza) in materia di protezione dei dati personali, intraprese ed attuate, sono sinteticamente le seguenti: diffusione di materiale sintetico informativo-formativo in detta materia; pubblicazione in loco di protocolli adottati ex Reg. UE n. 679/2019; convegnistica periodica; eventi formativi.

Valutazione: Accettabile

L) Vigilanza sulla protezione dei dati

Sono svolte verifiche periodiche sullo stato dei trattamenti dei dati personali, coinvolgendo, all'occorrenza, i seguenti soggetti: legale rappresentante; IT-Manager/Responsabile esterno; eventuali consulenti esterni.

Valutazione: Accettabile

M) Gestione dei terzi che accedono ai dati

Rispetto ai (pochissimi) terzi autorizzati ad accedere ai dati si verifica la necessità, o meno, di adottare, ove possibile, apposito atto giuridico funzionale all'applicazione dei principi in tema di protezione dei dati personali. Gli accessi di terzi (ove avvenissero) avvengono solo sotto il controllo diretto e di presenza da parte del gestore del canale di segnalazione.

Valutazione: Accettabile.

N) Sicurezza dei documenti cartacei

I documenti cartacei sono ridotti allo stretto necessario ed indispensabile anche perché non sussiste ragione e/o interesse ad un tipo di raccolta e conservazione più vasta.

Le politiche di trattamento dei dati cartacei sono in tal senso sintetizzabili: raccolta (per quanto possibile) limitata; duplicazione limitata; accesso da parte delle sole persone che li devono usare per attuare le finalità aziendali; conservati in luoghi resi accessibili solo da parte delle persone autorizzate; i luoghi di conservazione dei documenti non prevedono (di norma) la presenza isolata di persone e, dunque, è remota la possibilità che una singola persona possa essere agevolata nell'estrarre e/o accedere a dati senza essere vista da altre persone; conservati in luoghi sicuri e, in ogni caso, in stabile, di fatto, allarmato e blindato; conservati per i periodi prestabiliti.

Valutazione: Accettabile

P) Tracciabilità

Esiste una politica di tracciabilità degli eventi gestita da apposito IT (esterno nominato responsabile). Esiste, altresì, un apposito registro dei sinistri. Esistono apposite istruzioni ed informazioni sui modi corretti di utilizzo dei metodi di tracciabilità degli eventi e sui protocolli da osservare.

Valutazione: Accettabile

Q) Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Esiste la conoscenza diretta e l'amplia pratica professionale del gestore del canale a gestire i possibili sinistri. Esiste, altresì, un apposito protocollo funzionale a gestire, in ottemperanza agli artt. 33, 34, del Reg. UE n. 679/2016 gli eventuali incidenti.

Valutazione: Accettabile

ACCESSO ILLEGITTIMO AI DATI

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

Danno per la reputazione, difficoltà di esercitare diritti, servizi o opportunità, discriminazione, perdita di controllo dei dati personali, altri svantaggi economici o sociali, furto d'identità.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Pirati informatici, personale non autorizzato, virus informatici.

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne, Fonti non umane.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Gestione diretta del canale e delle segnalazioni, postazione presidiata, Vigilanza sulla protezione dei dati, Gestione dei terzi che accedono ai dati, Controllo degli accessi fisici.

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

Limitato - potenziale

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

Limitata. Ciò detto, in considerazione delle misure preventive adottate e considerato il livello formativo-informativo del gestore del servizio di segnalazione.

Valutazione: Accettabile

Modifiche indesiderate dei dati

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

Difficoltà di esercitare i diritti previsti dalla normativa ex Dlgs 24/2023.

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

Pirati informatici, Virus informatici

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne, Fonti non umane

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

Vigilanza diretta e personale sulla protezione dei dati, Sicurezza dei documenti cartacei, antivirus, ambienti protetti.

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

Limitato in ragione delle attività svolte e della conoscenza della materia.

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

Limitata.

La presenza di controlli interni, unitamente all'esistenza di procedure utile alla protezione dei dati personali consente di marginalizzare il rischio di verificazione dell'illecito.

Valutazione: Accettabile

Perdita di dati

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

Difficoltà di esercitare diritti, servizi o opportunità, perdita di controllo dei dati personali, altri svantaggi economici, sociali o associativi

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

Pirati informatici, Virus informatici

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne, Fonti non umane

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

Archiviazione, Backup, Lotta contro il malware, Controllo degli accessi logici, Gestione postazioni, Gestione dei terzi che accedono ai dati, Controllo degli accessi fisici, Vigilanza diretta sulla protezione dei dati, Sicurezza dei documenti cartacei, Tracciabilità, Modalità di gestione degli incidenti di sicurezza e delle violazioni dei dati personali.

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

La gravità del rischio è stata stimata come "limitata/ridotta".

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

Limitata.

La presenza di controlli interni, unitamente all'esistenza di procedure utili alla protezione dei dati personali consente di marginalizzare il rischio di verificazione dell'illecito.

Valutazione: Accettabile

Sintetico Piano d'azione e prime Conclusioni

Piano d'azione / misure correttive:

- Ulteriori e periodiche azioni di monitoraggio al fine di individuare casi peculiari di periodi di conservazione dei dati personali sulla base dell'esperienza che verrà ad accumularsi;
- Responsabile dell'implementazione: IT-Manager; L.T.

Diritto di accesso e diritto alla portabilità dei dati
Piano d'azione / misure correttive:

- Da ri-valutare all'occorrenza.
- Responsabile dell'implementazione: **L.T.**

Responsabili del trattamento
Piano d'azione / misure correttive:

- Occorre monitorare periodicamente (ovvero con frequenza) il sopraggiungere di nuove fattispecie di reato.
- Valutare all'occorrenza l'integrazione degli atti di nomina.
- Responsabile dell'implementazione**: L.T.**

Misure esistenti o pianificate

Backup
Piano d'azione / misure correttive:

- Confrontarsi costantemente con IT-Manager
- Data prevista di implementazione: 20/03/2025
- Responsabile dell'implementazione: **L.T.**

Gestione postazioni

Piano d'azione / misure correttive:

- Le azioni formative-informative devono essere periodicamente attuate.
- Data prevista di implementazione**:** 20/03/2025
- Responsabile dell'implementazione**: L.T.**

Sicurezza dei siti *web*
Piano d'azione / misure correttive

- Data prevista di implementazione: 20/03/2025
- Responsabile dell'implementazione: **L.T. -** IT-Manager

Sicurezza dei documenti cartacei

- Piano d'azione / misure correttive: nessuna
- Data prevista di implementazione: 20/03/2025
- Responsabile dell'implementazione**: L.T.**

Tracciabilità

- **Piano d'azione / misure correttive**:
  Da verificare periodicamente con l'IT-Manager
- **Data prevista di implementazione:** 20/03/2025
- **Responsabile dell'implementazione:** IT-Manager/L.T.

Inoltre, ancora più precisamente occorre periodicamente:

1. monitorare lo stato dei trattamenti di dati personali;
2. monitorare l'aggiornamento, il miglioramento e l'implementazione degli atti di nomina;
3. accertare l'attualità degli incarichi conferiti per la protezione e la corretta circolazione dei dati personali;
4. sondare ulteriori modalità con cui – ad es. tramite "questionari" – consentire meglio agli interessati di fornire il proprio "apporto" ai fini dell'implementazione del documento;
5. monitorare la correttezza e l'efficacia delle informative per il trattamento dei dati personali, anche in attuazione del principio di cui agli artt. 12ss, Reg. UE n. 679/2016;
6. verificare la concreta applicazione del principio di minimizzazione dei dati personali;
7. monitorare la necessità (e/o anche solo l'opportunità) di aggiornare il presente documento di valutazione d'impatto.