COMUNE DI BUSSO
Provincia di Campobasso

86010 Via Alessandro Manzoni, 5 Tel. 0874 / 447133 CF 00172190704
e-mail: comune.busso@virgilio.it – pec: comune.bussocb@legalmail.it
sito web: www.comune.busso.cb.it

WHISTLEBLOWING – CANALE DI SEGNALAZIONE

Valutazione d'impatto delle attività di trattamento

redatta ai sensi del D.Lgs. 24/2023, Art. 13, comma 6

SOMMARIO

1. Introduzione 3
2. Glossario 3
3. Verifica preliminare di applicabilità della DPIA 5
4. Valutazione degli impatti sulla protezione dei dati personali 5
4.1. Informazioni generali 5
4.2. Contesto 5
4.2.1. Panoramica del trattamento 5
4.2.2. Dati, processi e risorse di supporto 7
4.3. Principi fondamentali 9
4.3.1. Finalità 9
4.3.2. Basi giuridiche 9
4.3.3. Misure a tutela degli interessati 10
4.4. Valutazione e modalità di gestione dei rischi dei soggetti interessati 12
4.4.1. Identificazione delle possibili minacce di violazione dei dati personali 12
4.4.2. Stima del livello di impatto sugli interessati 13
4.4.3. Stima della probabilità di accadimento delle minacce 13
4.4.4. Valutazione del livello di rischio e selezione delle relative misure tecniche e organizzative 15
4.5. Validazione della DPIA 19
4.5.1. Parere del Responsabile della protezione dei dati 19

1. INTRODUZIONE

L'istituto del Whistleblowing, disciplinato dal D.Lgs. 24/2023 (di seguito per brevità *Decreto*), prevede la realizzazione di un canale di segnalazione interna mediante il quale i soggetti qualificati possono segnalare condotte illecite poste in essere da una amministrazione.

Il Decreto stabilisce, tra i principi posti a protezione del segnalante ovvero whistleblower, la tutela della riservatezza della sua identità. Un principio al quale la normativa attribuisce particolare importanza sottraendo, infatti, la segnalazione e la documentazione a essa allegata sia al diritto di accesso agli atti amministrativi e, a maggior ragione, all'accesso civico generalizzato, che all'esercizio dei diritti previsti dagli articoli 15-22 del Regolamento (UE) 2016/679 del Parlamento Europeo (c.d. GDPR) da parte del soggetto segnalato.

Verso questo aspetto, pertanto, l'amministrazione pone particolare attenzione adottando, quindi, un sistema di gestione in cui esclusivamente i soggetti autorizzati, rappresentati dall'RPCT ed eventualmente dal personale dell'ufficio dell'RPCT, hanno pieno accesso ai contenuti della segnalazione.

Il Comune di Busso nell'ambito delle attività finalizzate alla realizzazione dei canali di segnalazione interna redige pertanto, già in fase di progettazione, il documento di valutazione d'impatto sulla protezione dei dati personali (c.d. DPIA) che saranno oggetto di trattamento.

La DPIA, nell'individuare e pianificare le misure necessarie per una corretta esecuzione delle attività di trattamento dei dati personali, rappresenta lo strumento al quale il Titolare del Trattamento e ogni eventuale soggetto che opera in qualità di Responsabile del Trattamento faranno riferimento per l'applicazione delle misure tecniche e organizzative necessarie.

La presente DPIA viene redatta ai sensi del D.Lgs. 24/2023, Art. 13, comma 6 e in considerazione:

- di quanto stabilito dall'Art 35 del GDPR;
- delle indicazioni espresse dal WP29/EDPB, attraverso le *"Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento <<possa presentare un rischio elevato>> ai fini del regolamento (UE) 2016/679"*;
- delle indicazioni espresse dall'Enisa, attraverso il *"Manuale sulla Sicurezza nel trattamento dei dati personali"*.

2. GLOSSARIO

I seguenti termini utilizzati nel presente documento assumono i seguenti significati:

Accountability	Principio espresso all'Art. 24 del GDPR che così recita *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento...."*
Categorie particolari di dati personali	Dati atti a rilevare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
Clausole contrattuali standard	Clausole contrattuali che consentono di trasferire dati personali verso Paesi terzi
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento

Dati personali relativi a condanne penali e reati	Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
Dati genetici	Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione
Dati biometrici	Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici
Dati relativi alla salute	Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Diffusione	La divulgazione di dati personali al pubblico o, comunque, ad un numero indeterminato di soggetti
DPIA (o PIA)	Data Protection Impact Assessment (o Privacy Impact Assessment), è la valutazione d'impatto sulla protezione dei dati da eseguire in funzione. Tale processo è volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo. Lo stesso può riguardare una singola operazione di trattamento dei dati, ma potrebbe riferirsi anche a trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi.
Interessato	La persona fisica cui si riferiscono i dati personali.
Liceità del trattamento	L'insieme delle condizioni poste dal GDPR agli Artt. 6 e 9 che legittimano un trattamento di dati personali.
Misure di sicurezza	Insieme degli accorgimenti tecnici e organizzativi utilizzati per garantire la protezione dei dati personali.
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
Pseudonimizzazione	Applicazione di tecniche finalizzate a garantire che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Responsabile del Trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Soggetti a maggiore tutela di anonimato	Persone sieropositive, donne che si sottopongono a un'interruzione volontaria di gravidanza, vittime di atti di violenza sessuale o di pedofilia, persone che fanno uso di sostanze stupefacenti, psicotrope e di alcool, donne che decidono di partorire in anonimato, nonché assistiti che si avvalgono dei servizi offerti dai consultori familiari.
Titolare del Trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati

	personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

3. VERIFICA PRELIMINARE DI APPLICABILITÀ DELLA DPIA

La valutazione degli impatti viene redatta ai sensi del D. Lgs. 24/2023, Art. 13, comma 6.

4. VALUTAZIONE DEGLI IMPATTI SULLA PROTEZIONE DEI DATI PERSONALI

4.1. Informazioni generali

Titolare per il trattamento: Comune di Busso

Responsabile della protezione dei dati personali: Dott. Ing. Maurizio Giacci

Denominazione del trattamento: Whistleblowing - Canale di segnalazione interna

Frequenza di aggiornamento prevista: 1 anno

4.2. Contesto

4.2.1. Panoramica del trattamento

Descrizione del trattamento

L'istituto del Whistleblowing prevede la possibilità da parte di soggetti qualificati a tal scopo (soggetti segnalanti o whistleblowers) di segnalare condotte illecite poste in essere da una amministrazione.

Con l'intervento del Decreto la platea dei soggetti segnalanti è ridefinita come di seguito riassunto:

- i dipendenti delle amministrazioni pubbliche e degli enti pubblici economici;
- i lavoratori autonomi, i titolari di un rapporto di collaborazione, i liberi professionisti, i consulenti e i volontari e i tirocinanti (retribuiti e non retribuiti) che prestano la propria attività presso soggetti del settore pubblico;
- i lavoratori e collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica.

Il Decreto stabilisce, tra i principi posti a protezione del segnalante, la tutela della riservatezza della sua identità. Un principio al quale la normativa attribuisce particolare importanza sottraendo, infatti, la segnalazione e la documentazione a essa allegata sia al diritto di accesso agli atti amministrativi e, a maggior ragione, all'accesso civico generalizzato, che all'esercizio dei diritti previsti dagli articoli 15-22 del GDPR da parte del soggetto segnalato. Verso questo aspetto, pertanto, l'amministrazione deve porre particolare attenzione adottando, quindi, un sistema di gestione in cui esclusivamente i soggetti legittimati, ossia l'RPCT e l'eventuale personale dell'ufficio dell'RPCT, possano avere pieno accesso ai contenuti della segnalazione e quindi svolgere il corrispondente trattamento di dati personali.

Il Decreto, altresì, prevede che l'RPCT possa stabilire una comunicazione diretta con il segnalante, qualora per lo svolgimento dell'istruttoria sia necessario richiedere chiarimenti, documenti o informazioni ulteriori.

Pertanto, nell'implementare il sistema di gestione delle segnalazioni (c.d. *canale di segnalazione interna*) bisogna tener presente anche di tale necessità e porre particolare attenzione affinché tale comunicazione diretta avvenga nel rispetto del principio di riservatezza dell'identità del segnalante.

Il canale di segnalazione interna che l'amministrazione deve adottare, deve garantire l'inoltro di segnalazioni sia in forma scritta, anche con modalità informatiche, oppure in forma orale. Quest'ultime attraverso linee telefoniche o sistemi di messaggistica vocale.

I canali di segnalazione interna, sia telefonico che telematico, devono avere caratteristiche funzionali tali da tutelare la riservatezza dell'identità del segnalante e quindi osservare almeno i seguenti requisiti minimi:

a) garantire l'accesso, al contenuto della segnalazione e della documentazione ad essa allegata, ai soli soggetti autorizzati e previsti nell'iter procedurale;
b) prevedere la modifica periodica e obbligatoria delle credenziali di accesso ai canali;
c) garantire la non tracciabilità del segnalante, indirizzo IP o numero telefonico, in modo tale che nessun soggetto terzo, inclusa la ditta fornitrice della soluzione, possa prenderne visione. Di tali identificativi non deve esserci traccia nemmeno nei file di tracciamento (c.d. file di log) dei dispositivi tecnologici coinvolti (firewall, proxy, centralini, etc.);
d) disaccoppiare i dati del segnalante rispetto alle informazioni relative alla segnalazione e rendere intellegibili, anche alla ditta fornitrice della soluzione, i contenuti di quest'ultima sia se essa avvenga in modalità telematica che attraverso strumento telefonici, mediante l'adozione di un sistema di crittografia;
e) rendere disponibile agli istruttori ovvero il personale dell'ufficio di RPCT il solo contenuto della segnalazione e solo dopo esplicita assegnazione da parte dell'RPCT;
f) prevedere l'accesso sicuro e protetto ai canali mediante l'adozione di sistemi di autenticazione e autorizzazione opportuni e in particolare assicurare che alla numerazione telefonica dedicata alla richiesta di appuntamento per un incontro diretto possa rispondere esclusivamente l'RPCT e alla casella vocale, dedicata alla registrazione della segnalazione, possa accedere esclusivamente dall'RPCT;
g) tracciare l'attività degli operatori del sistema in specifici file di log che devono essere adeguatamente protetti da accessi non autorizzati e non devono riportare alcuna informazione che possa ricondurre all'identità o all'attività del segnalante;
h) consentire, nel corso dell'istruttoria e solo relativamente al canale telematico, lo scambio di messaggi o documenti con il segnalante mediante meccanismi interni alla piattaforma che tutelino l'identità del segnalante. È esclusa l'adozione della posta elettronica individuale quale mezzo di comunicazione con il segnalante;
i) qualora la piattaforma per l'acquisizione e gestione delle segnalazioni invii messaggi (variazione dello stato di avanzamento dell'istruttoria, riscontro del segnalante a una richiesta di integrazione, riscontro del segnalante a una richiesta di consenso a rivelare la propria identità nell'ambito di un procedimento disciplinare, ecc.) sulla casella di posta elettronica individuale assegnata all'RPCT e/o all'istruttore, tali messaggi non devono contenere riferimenti all'identità del segnalante o all'oggetto della segnalazione.

Finalità

I dati personali sono trattati al fine di assicurare:

- la corretta e completa gestione del procedimento di Whistleblowing in conformità alla vigente normativa in materia;
- lo svolgimento delle necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti;

- la tutela in giudizio di un diritto del Titolare del trattamento;
- la risposta a una richiesta dell'Autorità giudiziaria o ad essa assimilata.

Descrizione del contesto ed eventuali problematiche

I canali di segnalazione interna, sia telefonico che telematico, devono avere caratteristiche funzionali tali da tutelare la riservatezza dell'identità del segnalante e quindi osservare i requisiti minimi precedentemente elencati e qui nuovamente riaffermati:

a) garantire l'accesso, al contenuto della segnalazione e della documentazione ad essa allegata, ai soli soggetti autorizzati e previsti nell'iter procedurale;
b) prevedere la modifica periodica e obbligatoria delle credenziali di accesso ai canali;
c) garantire la non tracciabilità del segnalante, indirizzo IP o numero telefonico, in modo tale che nessun soggetto terzo, inclusa la ditta fornitrice della soluzione, possa prenderne visione. Di tali identificativi non deve esserci traccia nemmeno nei file di tracciamento (c.d. file di log) dei dispositivi tecnologici coinvolti (firewall, proxy, centralini, etc.);
d) disaccoppiare i dati del segnalante rispetto alle informazioni contenute nella segnalazione e rendere intellegibili, anche alla ditta fornitrice della soluzione, i contenuti di quest'ultima sia se essa avvenga in modalità telematica che attraverso strumento telefonici, mediante l'adozione di un sistema di crittografia;
e) rendere disponibile agli istruttori ovvero il personale dell'ufficio di RPCT il solo contenuto della segnalazione e solo dopo esplicita assegnazione da parte dell'RPCT;
f) prevedere l'accesso sicuro e protetto ai canali mediante l'adozione di sistemi di autenticazione e autorizzazione opportuni e in particolare assicurare che alla numerazione telefonica dedicata alla richiesta di appuntamento per un incontro diretto possa rispondere esclusivamente l'RPCT e alla casella vocale, dedicata alla registrazione della segnalazione, possa accedere esclusivamente dall'RPCT;
g) tracciare l'attività degli operatori del sistema in specifici file di log che devono essere adeguatamente protetti da accessi non autorizzati e non devono riportare alcuna informazione che possa ricondurre all'identità o all'attività del segnalante;
h) consentire, nel corso dell'istruttoria e solo relativamente al canale telematico, lo scambio di messaggi o documenti con il segnalante mediante meccanismi interni alla piattaforma che tutelino l'identità del segnalante. È esclusa l'adozione della posta elettronica individuale quale mezzo di comunicazione con il segnalante;
i) qualora la piattaforma per l'acquisizione e gestione delle segnalazioni invii messaggi (variazione dello stato di avanzamento dell'istruttoria, riscontro del segnalante a una richiesta di integrazione, riscontro del segnalante a una richiesta di consenso a rivelare la propria identità nell'ambito di un procedimento disciplinare, ecc.) sulla casella di posta elettronica individuale assegnata all'RPCT e/o all'istruttore, tali messaggi non devono contenere riferimenti all'identità del segnalante o all'oggetto della segnalazione.

Normativa di settore

- D. Lgs. 24/2023;
- Delibera ANAC 469/2021 recante "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)".

4.2.2. Dati, processi e risorse di supporto

Descrizione dei dati

I dati che saranno oggetto di trattamento riguardano dati personali identificativi sia del soggetto segnalante che dei soggetti coinvolti nella condotta illecita segnalata. Non è possibile escludere la presenza di dati di tipo particolare all'interno del corpo della segnalazione, che potrebbe ad esempio riportare informazioni sullo stato di salute di un soggetto identificabile.

Descrizione delle fasi/operazioni di trattamento

Canale di segnalazione telematico

1. Il segnalante accede alla piattaforma web accessibile dal sito istituzionale del Comune di Busso
2. Il segnalante sceglie se trasmettere la segnalazione in forma anonima o altrimenti
   a. Se il segnalante non sceglie di trasmettere la segnalazione in forma anonima inserisce i suoi dati identificativi
3. Il segnalante inserisce le informazioni riguardanti la presunta condotta illecita e chiude il processo di segnalazione
4. La piattaforma comunica all'RPCT, sulla casella di email dedicata, la presenza di una segnalazione e nel contempo restituisce al segnalante il codice univoco di segnalazione con la quale quest'ultimo potrà successivamente visualizzare lo stato del procedimento
5. L'RPCT nel ricevere la comunicazione di cui al precedente punto accede, con le sue credenziali, alla piattaforma web per visualizzare la segnalazione. Successivamente da inizio alle necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti

L'RPCT al compimento delle diverse fasi aggiornerà lo stato dell'attività istruttoria che il segnalante potrà conoscere accedendo alla piattaforma web e utilizzando il codice univoco di segnalazione.

L'RPCT visualizza in prima istanza solo il corpo della segnalazione. Solo attraverso una richiesta esplicita al sistema potrà avere accesso ai dati identificativi del segnalante. Il sistema di segnalazione registra la richiesta effettuata dall'RPCT.

Canale di segnalazione telefonico

1. Il segnalante compone il numero telefonico dedicato e posto a disposizione del Comune di Busso
2. Viene attivato un sistema IVR (Interactive Voice Response) che consente al segnalante attraverso i menù vocali se richiedere un appuntamento telefonico o procedere alla registrazione di una segnalazione
3. Se il segnalante sceglie di richiedere un appuntamento telefonico:
   a. La chiamata viene dirottata verso il numero interno assegnato all'RPCT che pertanto fissa l'appuntamento telefonico
4. Se il segnalante sceglie di procedere nella segnalazione:
   a. La chiamata viene dirottata verso una casella vocale al fine di procedere nella registrazione
   b. Al termine della registrazione il sistema telefonico comunica all'RPCT, sulla casella di email dedicata, la presenza di una segnalazione
   c. L'RPCT accede alla casella vocale e successivamente da inizio alle necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti

Descrizione delle risorse di supporto

Canale di segnalazione telematico

Il canale di segnalazione telematico è fornito dalla ditta Whistleblowing Solutions Impresa Sociale S.r.l. (https://www.whistleblowing.it/) in modalità SaaS e tramite un intermediario in modalità IaaS.

L'architettura di sistema è principalmente composta da due firewall perimetrali, raccolti in cluster, da due server fisici dedicati, raccolti in cluster, e da una storage area network ridondata.

Seguono i software utilizzati per la realizzazione della piattaforma:

- GlobaLeaks,
- Debian/Linux, sistema operativo
- Postfix, mail server
- Bind9, dns server
- OPNSense, firewall
- OpenVPN, sistema di virtual private network
- VMware, software di virtualizzazione;
- Veeam, software di backup;
- Plesk, software per realizzazione siti web di facciata del progetto.

La rete utilizza un firewall perimetrale e la tecnologia VLAN per isolare e raggruppare i sistemi in ordine alla funzionalità svolta e limitare l'esposizione degli stessi in caso di attacco.

La comunicazione con la piattaforma utilizza il protocollo sicuro *https*.

4.3. Principi fondamentali

4.3.1. Finalità

I dati personali sono trattati al fine di assicurare:

a) la corretta e completa gestione del procedimento di Whistleblowing in conformità alla vigente normativa in materia;
b) lo svolgimento delle necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti;
c) la tutela in giudizio di un diritto del Titolare del trattamento;
d) la risposta a una richiesta dell'Autorità giudiziaria o ad essa assimilata.

4.3.2. Basi giuridiche

Il trattamento dei dati avviene senza uno specifico consenso poiché necessario:

- per adempiere un obbligo legale al quale è soggetto il titolare del trattamento [GDPR, Art. 6, comma 1, lett c];
- per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri [GDPR, Art. 9, comma 2, lett g].

Principio di minimizzazione dei dati

I dati sono raccolti nel rispetto di quanto indicato dalla normativa vigente e si limitano ad un set di dati strettamente necessario al raggiungimento delle finalità.

A tal proposito, si precisa, che qualora la segnalazione contenga dati manifestatamente non utili al trattamento della segnalazione questi non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

Principio di limitazione della conservazione

Come stabilito dal D. Lgs. 24/2023, i dati forniti verranno conservati per il tempo strettamente necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

4.3.3. Misure a tutela degli interessati

Informazioni agli interessati

Agli interessati viene fornita specifica informativa che sarà resa telefonicamente, qualora il segnalante utilizzi il canale di comunicazione telefonico, o prima di procedere alla compilazione delle schede, qualora il segnalante utilizzi il canale di comunicazione telematico.

Consenso dell'interessato

Il trattamento dei dati avviene senza uno specifico consenso poiché necessario:

- per adempiere un obbligo legale al quale è soggetto il titolare del trattamento [GDPR, Art. 6, comma 1, lett c];
- per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri [GDPR, Art. 9, comma 2, lett g].

Diritto di accesso

Esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Diritto alla portabilità

Esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Diritto di rettifica

Il diritto di rettifica può essere esercitato solamente dal segnalante mediante il canale di segnalazione telematico o mediante incontro con l'RPCT. Gli altri soggetti interessati possono esercitarlo nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196

Diritto alla cancellazione

Esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Diritto di limitazione

Esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Diritto di opposizione

Esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196

Responsabile del trattamento esterno

Il Comune di Busso si avvale di soggetti terzi al fine di garantire la continuità operativa dei canali di comunicazione. Con quest'ultimi sono stabiliti contratti di fornitura di servizi di tipo IaaS e SaaS che prevedono la manutenzione correttiva ed evolutiva.

Detti fornitori operano inevitabilmente un trattamento di dati personali per conto del Comune di Busso (leggasi anche Titolare del Trattamento) e pertanto, ai sensi dell'articolo 4 comma 8 del GDPR, si configura per essi il ruolo di Responsabile del Trattamento.

Di conseguenza, il Comune di Busso, nell'affidare tali servizi, ricorre a soggetti che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

Inoltre, ai sensi dell'Art. 28, comma 3 del GDPR, i trattamenti svolti dai Responsabili del Trattamento sopra indicati è disciplinato da un contratto che li vincola al Titolare del Trattamento e che stipula la materia disciplinata, la durata, la natura e la finalità del trattamento, nonché il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del Trattamento.

Il contratto prevede, in particolare, che il Responsabile del Trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32 del GDPR;
d) rispetti le condizioni di cui ai commi 2 e 4 dell'Art. 28 del GDPR qualora ricorri a un altro responsabile del trattamento;
e) assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR
g) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato

Con riferimento al canale di **comunicazione telematico**, rappresentano Responsabili del Trattamento:

- la Whistleblowing Solutions, per la fornitura e la gestione del sistema di whistleblowing
- la Seeweb, come Sub-Responsabile del trattamento, nominato dalla Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS);
- la Transaparency International Italia, come Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing

Trasferimento dei dati

I dati raccolti non saranno soggetti a trasferimento verso paesi extra UE.

4.4. Valutazione e modalità di gestione dei rischi dei soggetti interessati

4.4.1. Identificazione delle possibili minacce di violazione dei dati personali

1. DISTRUZIONE non autorizzata di dati personali di lunga durata o irreversibile

☒	Eliminazione logica non autorizzata di dati personali (es. cancellazione dei dati)	
☒	Eliminazione fisica di supporti contenenti dati personali (es. danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei)	
☐	Eliminazione logica o del supporto fisico dell'unica copia elettronica di dati personali, il cui ripristino da documenti cartacei è possibile, ma richiede un tale impiego di tempo da poter generare effetti sull'Interessato	Non esiste una copia elettronica unica. I dati sono posizionati in un sistema cloud qualificato AGiD

2. INDISPONIBILITÀ di mezzi e strumenti temporanea o irreversibile

☒	Indisponibilità dei sistemi e dei servizi informatici mediante i quali le informazioni sono accessibili (es. in caso di attacco informatico)	
☒	Indisponibilità dei mezzi e degli strumenti necessari per ottenere l'accesso alle informazioni (es. perdita di una chiave di decifratura o di un token hardware per accedere a dati in backup o altri archivi)	
☐	Indisponibilità degli strumenti atti a identificare l'informazione all'interno di grandi archivi cartacei o elettronici	
☒	Degrado prestazionale dei servizi informatici, che determina l'impossibilità di perfezionare operazioni di trattamento	
☒	Modifiche tecnologiche che rendono impossibile la decodifica di dati rappresentati secondo particolari formati di memorizzazione	

3. PERDITA dei supporti di memorizzazione di dati personali

☒	Privazione o sottrazione di supporti fisici di memorizzazione dei dati	Le postazioni di lavoro con le quali si procede all'inserimento dei dati potrebbero contenere copie di dati personali
☒	Smarrimento di supporti fisici di memorizzazione dei dati	Le postazioni di lavoro con le quali si procede all'inserimento dei dati potrebbero contenere copie di dati personali

4. ALTERAZIONE non autorizzata di dati personali

☐	Comunicazione di informazioni erronee a soggetti esterni o al pubblico determinata da alterazioni non autorizzate di dati personali	
☒	Errori nel trattamento o trattamento non conforme, determinati da alterazioni non autorizzate di dati personali	
☒	Decisioni errate con effetti sull'Interessato, determinate da alterazioni non autorizzate di dati personali	

5. DIVULGAZIONE non autorizzata di dati personali (non già pubblici)

☒	Comunicazione non autorizzata od impropria di dati personali, non corrispondenti a informazioni di pubblico dominio, verso terze parti,	

anche se note o non identificabili

☒ Diffusione non autorizzata od impropria di dati personali, non corrispondenti a informazioni di pubblico dominio

6. ACCESSO non autorizzato a dati personali

☒ Accesso effettivo a dati personali (anche in sola visualizzazione) da parte di soggetti non autorizzati al momento della violazione

4.4.2. Stima del livello di impatto sugli interessati

Perdita della disponibilità dei dati personali

La perdita di disponibilità dei dati contenuti nei dispositivi di memorizzazione posti a disposizione dei canali di comunicazione può essere conseguenza del concretizzarsi delle minacce di DISTRUZIONE, INDISPONIBILITÀ E PERDITA di cui ai punti 1, 2 e 3 del precedente paragrafo. L'evento potrebbe comportare l'interruzione dell'attività istruttoria avviata a seguito di una segnalazione che potrebbe essere intrapresa nuovamente dal whistleblower attraverso l'invio di una nuova segnalazione.

LIVELLO DI IMPATTO: BASSO

Perdita dell'integrità dei dati personali

La perdita di integrità dei dati contenuti nei dispositivi di memorizzazione posti a disposizione dei canali di comunicazione può essere conseguenza del concretizzarsi delle minacce di ALTERAZIONE di cui al punto 4 del precedente paragrafo. L'evento potrebbe comportare lo svolgimento di una istruttoria non corretta in quanto viziata da informazioni erronee. Gli individui potrebbero andare incontro a conseguenze significative.

LIVELLO DI IMPATTO: ALTO

Perdita della riservatezza dei dati personali

La perdita di riservatezza può essere conseguenza del concretizzarsi della minaccia di PERDITA dei supporti di memorizzazione di dati personali e ACCESSO non autorizzato di cui ai punti 3 e 6 del precedente paragrafo. Gli eventi potrebbero esporre gli interessati a conseguenze significative.

LIVELLO DI IMPATTO: ALTO

STIMA DEL LIVELLO GENERALE DI IMPATTO

LIVELLO DI IMPATTO: ALTO

4.4.3. Stima della probabilità di accadimento delle minacce

1. AREA DI RISCHIO TECNICO - MINACCE CORRELATE A RISORSE DI RETE E TECNICHE SIA HARDWARE CHE SOFTWARE)

☒	Il sistema che opera il trattamento dei dati personali è esposto sulla rete Internet	Il sistema è quindi esposto ad attacchi esterni che possono concretizzarsi con attacchi di Denial of Service, di tipo Man-in-the-Middle o tentativi di SQL injection
☒	L'accesso al sistema è garantito anche tramite Internet	Aumenta pertanto la probabilità di subire attacchi esterni, che potrebbero comportare la perdita di riservatezza e integrità. *Si evidenzia la necessità di applicare forme di autenticazione forti per l'accesso degli amministratori.*
☐	Il sistema di trattamento dei dati personali è	

	interconnesso con un altro sistema o servizio IT esterno	
☐	Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati	I canali di comunicazione sono ospitati su infrastruttura cloud qualificata AGiD
☐	Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi	I canali di comunicazione sono ospitati su infrastruttura cloud qualificata AGiD

2. AREA DI RISCHIO ORGANIZZATIVO, PROCESSI/PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

☐	I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti	Sono stabilite procedure finalizzate a organizzare utenti e autorizzazione sulla base di un organigramma dei ruoli.
☐	L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito	L'uso delle risorse viene stabilito nelle procedure di cui alla voce sopra. Saranno specificate le limitazioni d'uso al fine di evitare utilizzi impropri.
☒	I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali	Lo smart working viene eseguito con dispositivi personali dei dipendenti.
☐	I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione	Nelle procedure di cui alla voce sopra verrà fatto specifico richiamo sul divieto di trattare dati personali al di fuori dei locali dell'organizzazione
☐	Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro	Sono adottati adeguati meccanismi di registrazione e monitoraggio delle attività svolte dagli utenti

3. AREA DI RISCHIO OPERATIVO - MINACCE CORRELATE A PARTI E PERSONE COINVOLTE NELLE OPERAZIONI DI TRATTAMENTO

☐	Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti	L'accesso è ristretto al solo RPCT o eventualmente ai dipendenti dell'ufficio dell'RPCT.
☒	Qualche parte dell'operazione di trattamento dei dati è eseguita da un responsabile del trattamento	
☐	Gli obblighi delle parti/persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti	Gli obblighi e i ruoli svolti sono specificati nelle lettere di designazione.
☒	Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni	
☒	Le persone/parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e/o distruggere in modo sicuro i dati personali?	

4. AREA DI RISCHIO STATISTICO - MINACCE CORRELATE AL SETTORE DI OPERATIVITÀ E SCALA DEL TRATTAMENTO

☒	Il settore di operatività in cui si inserisce il trattamento è esposto ad attacchi informatici	
☐	La struttura organizzativa ha subito attacchi informatici o altri tipi di violazioni della sicurezza	

negli ultimi due anni

- ☐ Sono state ricevuto notifiche e/o segnalazioni riguardo alla sicurezza del sistema informatico nell'ultimo anno
- ☐ Un'operazione del trattamento riguarda un grande volume di individui e / o dati personali
- ☐ Esistono best practice di sicurezza specifiche, per il settore di attività in cui si inserisce il trattamento, che non sono state adeguatamente seguite

SOMMARIO - PROBABILITÀ DI ACCADIMENTO DELLE MINACCE

AREA DI RISCHIO	PROBABILITÀ DI ACCADIMENTO DELLE MINACCE
Area di rischio tecnico	MEDIA
Area di rischio organizzativo	BASSA
Area di rischio operativo	MEDIA
Area di rischio statistico	BASSA
STIMA DELLA PROBABILITÀ GENERALE DI ACCADIMENTO	MEDIA

4.4.4. Valutazione del livello di rischio e selezione delle relative misure tecniche e organizzative

Si riporta di seguito il ***"livello di rischio inerente"*** (LRI) calcolato per il trattamento in esame:

Livello di rischio inerente = Alto

Sono pertanto elencate le misure di sicurezza da adottare e/o consolidare per la gestione del rischio.

MISURE DA ADOTTARE			
CATEGORIA	**DESCRIZIONE**	**ATTUATO (SI/NO)**	**NOTE**
Gestione delle segnalazioni telematiche e telefoniche			
Ruoli e responsabilità	Definizione dei ruoli e delle responsabilità relative al trattamento dei dati personali che sono assegnati in conformità con le politiche di sicurezza.	SI	I ruoli e le responsabilità sono definiti in conformità con quanto stabilito dal D. lgs. 24/2023
	Revoca dei diritti, delle responsabilità e dei profili di autorizzazione, nonché riconsegna di materiali e mezzi del trattamento, in caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo.	SI	La sostituzione dell'RPCT prevede la modifica delle credenziali di accesso al canale telematico, al canale telefonico e alla casella di mail dedicata
Politica di controllo degli accessi	Assegnazione delle autorizzazioni di accesso al sistema in base al principio della stretta pertinenza e necessità	SI	Alle figure che operano sui canali di comunicazione (RPCT e eventuali dipendenti dell'ufficio dell'RPCT) sono assegnati profili operativi che limitano l'accesso ai dati di stratta pertinenza

MISURE DA ADOTTARE			
CATEGORIA	**DESCRIZIONE**	**ATTUATO (SI/NO)**	**NOTE**
Responsabili del trattamento	Formalizzazione delle attività svolte dai responsabili del trattamento attraverso un contratto.	SI	Con i fornitori del canale telematico e telefonico viene stipulato un contratto come stabilito dall'Art. 28 del GDPR
Obblighi di confidenzialità imposti al personale	Assegnazione di ruoli e responsabilità ad ogni soggetto designato al trattamento.	SI	L'RPCT e gli eventuali dipendenti dell'ufficio di RPCT siglano per accettazione e presa visione una lettera di incarico a persona autorizzata al trattamento dei dati personali.
Controllo degli accessi e autenticazione	L'accesso ai dispositivi sotto il controllo del titolare del trattamento è soggetto ad autenticazione.	Si	Bisogna verificare che l'accesso alla postazione di lavoro, assegnata all'RPCT e ad ogni eventuale dipendente dell'ufficio dell'RPCT, non sia libero ossia sia necessario inserire username e password
Sicurezza delle Postazioni di lavoro	Utilizzo di applicazioni anti-virus con firme di rilevamento automaticamente aggiornate almeno su base settimanale.	Si	Bisogna verificare che l'accesso alla postazione di lavoro, assegnata all'RPCT e ad ogni eventuale dipendente dell'ufficio dell'RPCT, abbia installato un antivirus che si aggiorni almeno settimanalmente
	L'utilizzo ordinario delle postazioni avviene con utenti privi di privilegi di amministrazione, ossia privilegi che permettono l'installazione o la disinstallazione, non autorizzata, di applicazioni software.	SI	Bisogna verificare che l'accesso alla postazione di lavoro, assegnata all'RPCT e ad ogni eventuale dipendente dell'ufficio dell'RPCT, non avvenga come utente 'administrator'
	Il sistema attiva il *timeout* di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	Si	Bisogna verificare che la postazione di lavoro, assegnata all'RPCT e ad ogni eventuale dipendente dell'ufficio dell'RPCT, attivi automaticamente il blocco dell'elaboratore allo scadere di un periodo di inattività
	Installazione automatica degli aggiornamenti critici di sicurezza.	Si	Bisogna verificare che la postazione di lavoro, assegnata all'RPCT e ad ogni eventuale dipendente dell'ufficio dell'RPCT, faccia automaticamente gli aggiornamenti di windows
	Non è autorizzato, in via ordinaria, il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).	SI	La lettera di incarico a persona autorizzata al trattamento dei dati personali riporta tale divieto
Cancellazione/Eliminazione dei dati	I supporti di memorizzazione utilizzati per il trattamento di dati sono soggetti a sovrascrittura basata sul software (wiping) prima della loro eliminazione o riutilizzo. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), si procede alla distruzione		Previsione contenuta nella lettera di incarico a persona autorizzata al trattamento dei dati personali

MISURE DA ADOTTARE			
CATEGORIA	**DESCRIZIONE**	**ATTUATO (SI/NO)**	**NOTE**
	fisica.		
	La carta utilizzata per memorizzare i dati personali viene distrutta attraverso processi di triturazione		Previsione contenuta nella lettera di incarico a persona autorizzata al trattamento dei dati personali
Canale di segnalazione telematico			
Politica di controllo degli accessi	Assegnazione delle autorizzazioni di accesso al sistema in base al principio della stretta pertinenza e necessità	SI	Alle figure che operano sui canali di comunicazione (RPCT e eventuali dipendenti dell'ufficio dell'RPCT) sono assegnati profili operativi che limitano l'accesso ai soli dati di stretta pertinenza
Gestione risorse/asset	Controllo annuale e aggiornamento, se richiesto, delle risorse IT e del loro corretto funzionamento	SI	Viene operato dal fornitore dei servizi IaaS e SaaS
Business continuity	Adozioni di soluzioni finalizzate a garantire un adeguato livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali	SI	L'architettura di sistema è composta da due da due server fisici dedicati, raccolti in cluster, e da una storage area network ridondata
Controllo degli accessi e autenticazione	Implementazione di un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema.	SI	
	Assegnazione di account personali e non comuni (condivisi tra più utenti)	SI	L'RPCT e gli eventuali dipendenti dell'ufficio dell'RPCT accedono con credenziali proprie
	Adozione di un meccanismo di autenticazione basato almeno sulla coppia username/password.	SI	
	Modifica periodica delle credenziali di accesso	SI	
	Le password degli utenti vengono memorizzate in formato "*hash*".	SI	
Generazione di file di log e monitoraggio	Generazione di file di log che tracciano le attività degli operatori	SI	
	Non tracciabilità del segnalante, indirizzo IP o numero telefonico, in tutti i dispositivi tecnologici coinvolti (firewall, proxy, centralino, etc.)	SI	

MISURE DA ADOTTARE			
CATEGORIA	**DESCRIZIONE**	**ATTUATO (SI/NO)**	**NOTE**
	I file di log sono contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Sincronizzazione dell'orologio mediante il protocollo NTP con server autoritativi.	SI	
	Tracciamento delle azioni degli amministratori di sistema e degli operatori di sistema	SI	
Sicurezza di Server e Database	I server ove risiedono database e applicazioni sono configurati per essere operativi con un account diverso da quello di amministrazione e dotato di privilegi strettamente necessari per il corretto funzionamento.	SI	
	I server dove risiedono database e applicazioni trattano solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità.	SI	
	Disaccoppiamento dei dati del segnalante rispetto alle informazioni contenute nella segnalazione	SI	
	I contenuti della segnalazione sono resi intellegibili ai soggetti non autorizzati mediante sistemi di crittografia	SI	
	I contenuti della segnalazione sono resi accessibili agli istruttori ovvero il personale dell'ufficio di RPCT solo dopo esplicita assegnazione da parte dell'RPCT	SI	
Sicurezza della Rete e delle Infrastrutture di comunicazione	Utilizzo di protocolli crittografici (TLS / SSL) nelle comunicazioni tramite Internet.	SI	La comunicazione con la piattaforma utilizza il protocollo sicuro https
	Lo scambio di messaggi o documenti tra il segnalante e l'RPCT avviene mediante meccanismi interni alla piattaforma. È esclusa l'adozione della posta elettronica individuale quale mezzo di comunicazione con il segnalante	SI	
	Il traffico da e verso il sistema IT è monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.	SI	La rete utilizza un firewall perimetrale e la tecnologia VLAN per isolare e raggruppare i sistemi in ordine alla funzionalità svolta e limitare l'esposizione degli stessi in caso di attacco.

MISURE DA ADOTTARE			
CATEGORIA	**DESCRIZIONE**	**ATTUATO (SI/NO)**	**NOTE**
Backups	Adozione di procedure di backup e ripristino dei dati	SI	
	Protezione fisica e ambientale dei backup	SI	
	Monitoraggio dell'esecuzione dei backup	SI	
	Esecuzione regolare di backup completi	SI	
	Conservazione in modo sicure delle copie del backup	SI	

La piena applicazione delle sopra elencate misure di sicurezza comporta una diminuzione della probabilità generale di accadimento definibile come "*LIEVE*".

Di conseguenza il "*livello di rischio residuo*" calcolato per il trattamento in esame è:

Livello di rischio residuo = Medio

4.5. Validazione della DPIA

4.5.1. Parere del Responsabile della protezione dei dati

Il sottoscritto Dott. Ing. Maurizio GIACCI nominato, ai sensi dell'Art. 37 del GDPR, dal Comune di Busso come Responsabile della protezione dei dati (c.d. DPO),

- presso atto dei contenuti della presente valutazione degli impatti sul trattamento dei dati personali e in particolare:
  a. della stima del livello generale di impatto sulla protezione dei dati personali, valutata come "*Alta*";
  b. della stima della probabilità generale di accadimento, valutata come "*Media*";
  c. del livello di rischio inerente, calcolato sui valori di cui ai precedenti punti *a)* e *b)*, valutato come "*Alto*";
- in considerazione delle misure di sicurezza che il Titolare del Trattamento adotta per il trattamento dei dati personali in questione e che determinerebbero un livello di rischio residuo pari al valore "*Medio*";

esprime il proprio parere favorevole all'opportunità e necessità di procedere al trattamento dei dati personali oggetto della presente DPIA.

Il DPO
(*Dott. Ing. Maurizio Giacci*)