Fondazione Onlus
Casa di Riposo Città di Sondrio
Via Don Guanella, 36 – 23100 Sondrio- Tel. 0342/541011 – Fax. 0342/541050

Procedura relativa alla notifica di violazione sui dati personali (Data Breach)

Autore	Fondazione Onlus Casa di Riposo Città di Sondrio		
Sintesi	La presente procedura stabilisce gli adempimenti da porre in essere nel caso di violazioni dei dati personali trattati da Fondazione Onlus Casa di Riposo Città di Sondrio conformemente alla normativa privacy vigente.		
Versione	1.0		
Stato	Definitivo		
Data di pubblicazione	24.02.2022		
Approvato con	Determinazione n.3 del 21.02.2022		
Data di approvazione	21.02.2022		
Contatti	privacy@rsasondrio.it		

SOMMARIO

1. PREMESSE

Fondazione Onlus Casa di Riposo Città di Sondrio, in qualità di Titolare del trattamento (di seguito anche "**Titolare del trattamento**"), è tenuta, ai sensi del Regolamento Europeo 2016/679 (di seguito anche "**GDPR**"), a mantenere sicuri i dati personali trattati dalla propria struttura e a reagire senza ingiustificato ritardo in caso di violazione dei dati personali (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).

È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici alla Fondazione, che permettano, altresì, di rispettare gli adempimenti previsti dalla normativa europea, nei tempi e modi ivi previsti (es. notificazione all'autorità garante e/o comunicazione agli interessati).

Le sanzioni previste dal GDPR per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, comportano l'applicazione in capo a Fondazione Onlus Casa di Riposo Città di Sondrio di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del fatturato di Gruppo annuo totale dell'esercizio precedente, accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.

2. SCOPO

Lo scopo di questa procedura è di fornire un flusso di gestione delle violazioni dei dati personali trattati da Fondazione Onlus Casa di Riposo Città di Sondrio. Questo documento integra le procedure in essere presso il Titolare del trattamento ai sensi del GDPR e gli ulteriori provvedimenti in materia di protezione dei dati personali.

3. COS'È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali è ogni *violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati* dal Titolare del trattamento.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni, quali, a titolo di esempio:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà (data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo (proprietario);
- virus o altri attacchi al sistema informatico o alla rete della Fondazione;
- violazione di misure di sicurezza fisica (i.e. forzatura di porte o finestre di stanze di sicurezza o archivi contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche della Fondazione;
- invio di e-mail contenenti dati personali e/o particolari ad erroneo destinatario.

Il WP29 (Gruppo di Lavoro Articolo 29), nel suo parere n. 3 del 2014, ha classificato le violazioni in base ai seguenti tre ben noti principi di sicurezza delle informazioni:

- ***Violazione della riservatezza***: in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- ***Violazione della disponibilità***: in caso di perdita non autorizzata o accidentale o in caso di distruzione di dati personali;
- ***Violazione dell'integrità***: in caso di alterazione non autorizzata o accidentale dei dati personali.

Per meglio contestualizzare il riconoscimento di un Data Breach, si veda il paragrafo 8 della presente procedura.

4. AMBITO DI APPLICAZIONE E DESTINATARI

Questa procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura): i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nello svolgimento delle proprie attività per conto del Titolare del trattamento (di seguito, genericamente denominati "DESTINATARI").

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei soggetti inadempienti, secondo le normative vigenti in materia.

5. A QUALI TIPI DI DATI SI RIFERISCE QUESTA PROCEDURA

Questa procedura si riferisce ai ***dati personali*** (ivi incluse le categorie particolari di dati personali e i dati relativi a condanne penali o reati) trattati da e per conto del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo (i.e. sistemi informatici).

Per «***dato personale***» si intende "*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*".

Per «**dati particolari**» si intende "*dati personali che rivelino 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*"

6. GESTIONE DELLA COMUNICAZIONE INTERNA DI DATA BREACH

DESTINATARI della presente procedura sono i dipendenti/collaboratori di Fondazione Onlus Casa di Riposo Città di Sondrio nonché tutti i soggetti esterni alla struttura del Titolare che trattano dati per conto dello stesso.
Nel caso in cui uno dei destinatari si accorga o venga a conoscenza di un incidente che potenzialmente possa rientrare nei casi di Data Breach, dovrà immediatamente informare il Team Privacy (Fiori,Tachimiri, Bordoni, Damiani) mediante la compilazione dell'**Allegato A** alla presente procedura **"Modulo di comunicazione interna di Data Breach"** da inviare a mezzo mail all'indirizzo privacy@rsasondrio.it

Infatti, in caso di evento che comporti una sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che questa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

Per facilitare i DESTINATARI, intesi come *dipendenti/collaboratori* che hanno accesso alla rete aziendale, Fondazione Onlus Casa di Riposo Città di Sondrio ha reso disponibile, nella cartella "modulistica" , sotto la voce "Privacy – Data Breach", un modello e-mail già pre-configurato nel testo (corrispondente al citato Allegato A), con l'indirizzo del destinatario della comunicazione (privacy@rsasondrio.it).

Per facilitare i DESTINATARI, intesi come *dipendenti* che non hanno accesso alla rete aziendale, Fondazione Onlus Casa di Riposo Città di Sondrio ha reso disponibile un modello e-mail già pre-configurato nel testo (corrispondente al citato Allegato A), con l'indirizzo del destinatario della comunicazione (privacy@rsasondrio.it) inviato via mail tramite la piattaforma interna del gestionale CBA.

Per facilitare i DESTINATARI, intesi come *fornitori esterni nominati responsabili del trattamento ai sensi dell'art. 28 GDPR*, Fondazione Onlus Casa di Riposo Città di Sondrio invierà la procedura e l'Allegato A) sopra citato tramite e-mail.

La casella privacy@rsasondrio.it è stata identificata come canale per l'invio delle comunicazioni. La stessa verrà gestita, letta e consultata dai componenti del team privacy:

- Fiori Carlo, Direttore sanitario
- Tachimiri Simona, Direttore
- Bordoni Alessandra, impiegata
- Damiani Simona, impiegata

7. GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Nella gestione della notizia della violazione di dati personali pervenuta, il Team Privacy dovrà seguire i seguenti cinque step:

Step 1: Identificazione e indagine preliminare.

Step 2: Contenimento, recovery e risk assessment.

Step 3: Eventuale notifica all'Autorità Garante.

Step 4: Eventuale comunicazione agli interessati.

Step 5: Documentazione della violazione.

Step 1: Identificazione e indagine preliminare

L'**Allegato A** permetterà al Team Privacy di condurre una valutazione inziale della notizia dell'incidente occorso, per stabilire se sia effettivamente accaduto un Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, con il passaggio al risk assessment (step 2), e il coinvolgimento del DPO.

Infatti, mentre tutte le violazioni di dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni di dati personali (es. un incidente che porta alla indisponibilità dei dati personali per un certo periodo di tempo è una violazione della sicurezza, che dovrà essere documentata attraverso l'inserimento nell'**Allegato D - Registro delle violazioni**, mentre la perdita di un file contenente solo dati tecnici si configura esclusivamente come incidente di sicurezza).

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato A:

- La data di scoperta della violazione (tempestività);
- Il soggetto che è venuto a conoscenza della violazione;
- Breve descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- Le categorie, il numero approssimativo di interessati coinvolti nella violazione e di registrazioni di dati personali in questione;
- Breve descrizione di eventuali azioni già poste in essere.

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che un Data Breach è avvenuto, il Team Privacy e il DPO dovranno stabilire:

- Se esistono azioni/misure tecniche o organizzative che possano limitare i danni potenzialmente causati dalla violazione (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambiamento dei codici di accesso delle entrate; ecc.);
- Una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- L' attivazione delle misure identificate;
- L'effettivo rischio per i diritti e le libertà delle persone fisiche, con eventuale notifica della violazione all'Autorità Garante per la Protezione dei dati personali;
- Se la violazione presenti un *elevato* rischio per i diritti e le libertà delle persone fisiche, con conseguente comunicazione della violazione agli interessati;
- Per determinare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Team Privacy e il DPO valuteranno la gravità della violazione mediante:
  - esame dei dati contenuti nell'Allegato A;
  - compilazione dell'**Allegato B - Modulo di valutazione del Rischio del Data Breach**, tenendo in debita considerazione i principi e le indicazioni di cui all'art. 33 GDPR e adottando una delle metodologie suggerite da ENISA[1].

I criteri **di Valutazione della gravità della violazione** sono riassunti nell'**Allegato C**.

Step 3: Eventuale notifica all'Autorità Garante competente

Ove la risultanza della valutazione della gravità della violazione effettuata sulla base della procedura di cui allo step 2 desse un punteggio ***NON TRASCURABILE***, Fondazione Onlus Casa di Riposo Città di Sondrio dovrà provvedere ad effettuare la notifica all'Autorità Garante competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza.

Pertanto, il Team Privacy e il DPO determineranno l'Autorità di Controllo competente sulla base delle informative e/o della valutazione d'impatto sulla protezione dei dati già in essere presso Fondazione Onlus Casa di Riposo Città di Sondrio in relazione ai dati oggetto di violazione (in mancanza di tale documentazione che abbia preventivamente individuato l'Autorità Garante competente, la stessa sarà da individuare in quella dello Stato in cui è ubicato lo stabilimento principale o lo stabilimento unico del titolare del trattamento, anche per i trattamenti transfrontalieri eventualmente effettuati).

Una volta determinata l'Autorità di Controllo competente, il Team Privacy e il DPO individueranno la corretta modulistica da utilizzare per effettuare la notificazione e vi provvederanno (di seguito il link relativo al modulo di notifica messo a disposizione dal garante italiano https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=1.2).

Step 4: Eventuale comunicazione agli interessati

Ove la risultanza della valutazione della gravità della violazione effettuata sulla base della procedura di cui allo step 2 dia un punteggio ***ALTO***, Fondazione Onlus Casa di Riposo Città di Sondrio dovrà comunicare l'avvenuta violazione agli interessati coinvolti, senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Team Privacy e il DPO dovranno fare attenzione almeno ai seguenti aspetti:

- comunicare il nome e i dati di contatto del responsabile della protezione dei dati (DPO) o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, il Team Privacy e il DPO dovranno, caso per caso, privilegiare sempre modalità di comunicazione diretta con i soggetti interessati (quali e-mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e

[1] European Network and Information Security Agency (ENISA), "Recommendations for a methodology of the assessment of severity of personal data breaches", Dicembre 2013. https://www.enisa.europa.eu/publications/dbn-severity/at_download/fullReport

trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato dai DESTINATARI attraverso l'Allegato A, Fondazione Onlus Casa di Riposo Città di Sondrio sarà tenuta a documentarlo.

Tale documentazione sarà affidata al Team Privacy che vi provvederà mediante la tenuta dell'**Allegato D - Registro dei Data Breach**, con compilazione delle informazioni ivi riportate: (i) n. violazione; (ii) data violazione; (iii) natura della violazione; (iv) categoria di interessati; (v) categoria di dati personali coinvolti; (vi) numero approssimativo di registrazioni dei dati personali; (vii) conseguenze della violazione; (viii) contromisure adottate; (ix) gravità della violazione; (x) se sia stata effettuata notifica all'Autorità Garante Privacy; (xi) se sia stata effettuata comunicazione agli interessati.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

8. ESEMPI DI DATA BREACH

Per meglio contestualizzare il riconoscimento dei Data Breach, di seguito vengono proposti, a titolo esemplificativo ma non esaustivo, alcuni casi basati su quelli proposti dal Gruppo di lavoro dei Garanti Europei, ai sensi dell'ex art. 29 della Direttiva Europea 95/46:

Tipologia *Data Breach*	**Esempio**	**Necessita Notifica la Garante Privacy?**	**Necessita Notifica agli interessati?**	**Note**
Violazione della disponibilità	Furto o smarrimento di Chiavetta USB o Notebook o Tablet o Smartphone o Hard Disk su cui sono memorizzati dati non cifrati o cifrati con algoritmi non allo stato dell'arte	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Violazione della disponibilità	Furto o smarrimento di Chiavetta USB o Notebook o Tablet o Smartphone o Hard Disk su cui sono memorizzati dati cifrati con algoritmi allo stato dell'arte	NO	NO	Non deve essere notificato, ma va inserito nel registro dei Data Breach
Violazione della riservatezza	Una applicazione informatica subisce un attacco informatico a fronte del quale gli attaccanti hanno avuto accesso a dati personali e c'è il ragionevole sospetto che li abbiano consultati e/o sottratti (esempi di applicativi: Gestione Documentale, Gestione carriera studenti, Gestione del personale *Ugov Risorse Umane*, Gestione Diritto allo studio, Gestione prestito bibliotecario, Servizio di Posta Elettronica *Office 365*, etc.)	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Violazione della disponibilità	Temporanea non disponibilità di un server, un applicativo o della connettività di rete (ad esempio per mancanza energia elettrica, guasto degli apparati)	NO	NO	Non deve essere notificato, ma va inserito nel registro dei Data Breach
Violazione della riservatezza/ *Violazione della*	Una postazione di lavoro, o un server vengono compromessi da un Ransomware e conseguentemente i dati vengono cifrati, non esiste un BackUp dei dati e/o c'è una ragionevole evidenza	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli	

disponibilità	che i dati personali possono essere stati esfiltrati dal dispositivo		interessati	
Violazione della riservatezza/ Violazione della disponibilità	Una postazione di lavoro, o un server vengono compromessi da un Ransomware e conseguentemente i dati vengono cifrati, esiste un BackUp dei dati per cui possono essere ripristinati in tempi ragionevoli e c'è una ragionevole evidenza che i dati personali non sono stati sottratti dal dispositivo	NO	NO	Non deve essere notificato, ma va inserito nel registro dei Data Breach
Violazione della riservatezza	Un titolare di credenziali di accesso a sistemi informatici che trattano dati personali segnala una perdita di confidenzialità delle proprie credenziali (ad esempio per aver dato seguito ad un messaggio di Phishing), da una veloce investigazione risulta che le credenziali siano state usate per accedere a dati personali con attività non riconducibili all'utente autorizzato	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Violazione della riservatezza	A seguito di un attacco informatico sono state trafugate le credenziali di utenze con privilegi di accesso a dati personali, tali credenziali erano memorizzati sul server in modalità non cifrata o cifrate con algoritmi non allo stato dell'arte o con meccanismi di cifratura non reversibile (hash) non allo stato dell'arte.	SI	SI	
Violazione della riservatezza	A seguiti di un errore di programmazione e configurazione di un sistema informatico o di una applicazione informatica, sono stati resi accessibili dati personali a soggetti non Autorizzati al trattamento o diversi dagli Interessati, inoltre da una rapida investigazione risulta che sono stati fatti accessi in violazione di quanto sopra	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Violazione della riservatezza	Comunicazione di dati personali ad errato destinatario (ad esempio per invio ad indirizzo email errato)	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Violazione della riservatezza	Invio a mailing list di uno o più messaggi con gli indirizzi email dei destinatari in chiaro nel campo 'A' o nel campo 'CC'	SI se l'evento coinvolge un largo numero di individui	Dipende dallo scopo e dalla finalità della mailing list	

Da compilare a cura dei Destinatari (interni e esterni) e da inviare al Team Privacy di **Fondazione Onlus Casa di Riposo Città di Sondrio** al seguente indirizzo privacy@rsasondrio.it come da paragrafo 6 della presente procedura.

Comunicazione di Data Breach	Note
Data scoperta incidente **Modalità con cui è venuto a conoscenza della violazione:**	
Data dell'incidente:	☐ Il _____ ☐ Dal _____ e ancora in corso ☐ Dal _____ al _____ ☐ la data dell'incidente non è ad oggi nota – da determinare
Nome cognome e dati di contatto (indirizzo e-mail, numero telefonico) della persona che compila il presente modulo.	
Luogo dell'incidente (ad esempio: se in Italia o all'estero e specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Breve descrizione dell'incidente: **Con precisazione della modalità di esposizione al rischio: lettura (presumibilmente i dati non sono stati copiati), copia (ma i dati sono ancora presenti sui sistemi del titolare), alterazione (i dati sono presenti sui sistemi ma sono stati alterati), cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione), altro.** **Causa dell'incidente: azione intenzionale interna/esterna; azione accidentale interna/esterna; sconosciuta; altro.**	
Breve descrizione: **- della/e banca/che dati oggetto dell'incidente** **- della tipologia di dati coinvolti (es. dati personali comuni; categorie particolari di dati, tra cui origine razziale o etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale; dati relativi a condanne penali e reati)**	
Breve descrizione: **- Categorie di interessati (es. lavoratori; clienti; fornitori; utenti sito web)** **- Numero approssimativo di interessati coinvolti nell'incidente (se si è a conoscenza del numero esatto si prega di indicarlo)** **- Numero approssimativo di registrazioni dei dati personali coinvolti**	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta dell'incidente	
Responsabile del settore di appartenenza/Referente interno:	
Data:	

ALLEGATO B – MODULO DI VALUTAZIONE DEL RISCHIO DEL DATA BREACH

Da compilare a cura del Team Privacy, con il supporto del DPO.

Assessment soglia di rischio	NOTE
Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente (es. computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro) **loro ubicazione**	
Se laptop/mobile device è stato perso/rubato: quando è stata l'ultima volta in cui il laptop/mobile device è stato sincronizzato con il sistema IT centrale?	
Quali sono le potenziali conseguenze della violazione dei dati per gli interessati? **Selezionare una o più categorie, se applicabile.**	a) In caso di perdita di confidenzialità: ☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento ☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati ☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito ☐ Altro. *Si prega di specificare*: Clicca qui per inserire il testo b) In caso di perdita di integrità: ☐ I dati sono stati modificati e resi inconsistenti ☐ I dati sono stati modificati mantenendo la consistenza ☐ Altro. *Si prega di specificare*: Clicca qui per inserire il testo c) In caso di perdita di disponibilità: ☐ Mancato accesso a servizi ☐ Malfunzionamento e difficoltà nell'utilizzo di servizi ☐ Altro. *Si prega di specificare*: Clicca qui per inserire il testo Ulteriori considerazioni sulle possibili conseguenze:

Indicare i potenziali effetti negativi per gli interessati:	☐ Perdita del controllo dei dati personali ☐ Limitazione dei diritti Discriminazione Furto o usurpazione d'identità ☐ Frodi ☐ Perdite finanziarie ☐ Decifratura non autorizzata della pseudonimizzazione ☐ Pregiudizio alla reputazione ☐ Perdita di riservatezza dei dati personali protetti da segreto professionale ☐ Conoscenza da parte di terzi non autorizzati ☐ Qualsiasi altro danno economico o sociale significativo. *Si prega di specificare:* Clicca qui per inserire il testo
Indicare eventuali ulteriori soggetti coinvolti nei trattamenti (contitolare, responsabile ex art. 28 GDPR, rappresentante del titolare non stabilito nell'UE)	
Quali misure tecniche e organizzative erano state adottate per la protezione dei dati oggetto di violazione? (i.e. la pseudonimizzazione e la cifratura dei dati personali)	
La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo? **(membri UE, Islanda, il Liechtenstein e Norvegia)**	☐ SI (indicare quali): Clicca qui per inserire il test ☐ NO
La violazione coinvolge interessati di Paesi non appartenenti allo Spazio Economico Europeo?	☐ SI (indicare quali): Clicca qui per inserire il testo ☐ NO
Stima della gravità della violazione e indicazione delle motivazioni:	☐ Trascurabile ☐ Basso ☐ Medio ☐ Alto MOTIVAZIONI: Clicca qui per inserire il testo
Il Titolare del trattamento ha aderito ad un codice di condotta approvato ai sensi dell'art. 40 Regolamento (UE) o un meccanismo di certificazione di cui all'art. 42 Regolamento (UE)?	
Misure tecniche e organizzative adottate (o di cui si propone l'adozione) <u>per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati</u>	
Misure tecniche e organizzative adottate (o di cui si propone l'adozione) <u>per prevenire simili violazioni future</u>	
Notificazione del Data Breach all'Autorità Garante	Si/NO Se sì, notificato in data: Dettagli (indicare anche, se del caso, se deve essere notificata anche ad altre autorità di controllo o a organismi di vigilanza o di controllo):

Comunicazione del Data Breach agli interessati **(allegare testo in caso di invio della comunicazione)**	NO perché: ☐ a) il titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche Spiegare le motivazioni: Clicca qui per inserire il testo ☐ b) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi Descrivere le misure applicate: Clicca qui per inserire il testo ☐ c) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati Descrivere le misure adottate: Clicca qui per inserire il testo ☐ d) detta comunicazione richiederebbe sforzi sproporzionati. Descrivere la modalità (comunicazione pubblica o misura simile) tramite la quale gli interessati sono stati informati: Clicca qui per inserire il testo ☐ Sì, comunicato in data: Numero di interessati cui è stata comunicata la violazione: Clicca qui per inserire il testo Canale utilizzato per la comunicazione agli interessati: ☐ SMS ☐ Posta cartacea ☐ Posta elettronica ☐ Altro (specificare): Clicca qui per inserire il testo
E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?	☐ SI (indicare quali): Clicca qui per inserire il testo ☐ NO
Generalità dei soggetti compilatori del presente modulo:	
Data di compilazione del presente modulo:	

Il Team Privacy deve prontamente valutare il livello di gravità di una violazione di dati personali rispetto ai diritti e alle libertà dei soggetti interessati. Una delle metodologie suggerite per effettuare tale valutazione è quella proposta da ENISA.
La metodologia definisce dei criteri quantitativi che servono al Titolare per arrivare a una valutazione complessiva dell'impatto della violazione di dati personali.
In particolare, il Titolare applicherà la metodologia in base alle informazioni in suo possesso, raccolte durante le prime fasi di investigazione di un incidente.
Potrebbe essere necessario effettuare più valutazioni in tempi diversi, in base alle informazioni raccolte anche durante le fasi successive. La metodologia potrebbe non coprire tutti i possibili specifici casi; tutti dovranno essere trattati con particolare cura ed attenzione.

I principali parametri da tenere in considerazione durante la valutazione dell'impatto di una violazione di dati personali sono i seguenti:

- il **Contesto del trattamento dei dati** (Data Processing Context - **DPC**): tiene conto della natura dei dati oggetto della violazione, insieme ad altri fattori relativi al contesto generale del trattamento dei dati.
- la **Facilità di Identificazione** (Ease of Identification - **EI**): stima di quanto sia facile identificare i soggetti interessati a partire dai dati oggetto della violazione.
- le **Circostanze della violazione** (Circumstances of breach - **CB**): prende in considerazione le circostanze specifiche della violazione, relative alla sua tipologia, contemplando la perdita di sicurezza dei dati e gli eventuali scopi malevoli connessi.

Il DPC rappresenta la parte fondamentale della metodologia e valuta la criticità di un certo insieme di dati in uno specifico contesto di trattamento. Per calcolare tale parametro è necessario individuare le tipologie di dati personali oggetto della violazione, classificandole in almeno una delle seguenti quattro categorie:

Semplici: a titolo esemplificativo possono essere dati anagrafici, dati di contatto, dati relativi ai titoli di studio e alla formazione, informazioni relative alla vita famigliare, alle esperienze professionali **(1 punto)**.
Comportamentali: dati relativi alle preferenze e abitudini personali, dati di geolocalizzazione o dati di traffico **(2 punti)**.
Finanziari: qualunque tipo di dato finanziario (ad esempio: reddito, transazioni finanziarie, estratti conto, investimenti, carte di credito, ricevute, etc.), inclusi informazioni finanziarie relative alla previdenza sociale **(3 punti)**.
Particolari: qualunque tipo di dato particolare (ad esempio, salute, affiliazione politica, vita sessuale, etc.) **(4 punti)**.

Il DPC può aumentare di punteggio in base alla possibilità di derivare ulteriori informazioni dal dato violato.

Dopo aver classificato il dato e assegnato un punteggio, è necessario incrementarlo o diminuirlo in base al valore di fattori contestuali al trattamento dei dati. I fattori aggravanti sono: la quantità dei dati, le speciali caratteristiche del Titolare o dei soggetti interessati. I fattori attenuanti sono: la non validità o inaccuratezza dei dati, la disponibilità pubblica dei dati prima della violazione e la natura dei dati.

L'**EI** è un fattore correttivo di DPC. La criticità complessiva del trattamento può essere ridotta in base al valore di EI: minore è la facilità di identificazione e minore sarà il valore associato alla criticità complessiva. Ai fini della presente metodologia vengono definiti quattro livelli di EI, con un incremento lineare nel punteggio:

- Trascurabile **(0,25 punti)**.
- Limitato **(0,50 punti)**.
- Significativo **(0,75 punti)**.
- Massimo **(1 punti)**.

Il punteggio più basso è assegnato quando la possibilità di identificare gli interessati è trascurabile, mentre il punteggio più alto è selezionato quando l'identificazione è possibile direttamente dai dati violati, senza che siano necessarie particolari ricerche o elaborazioni per scoprire l'identità dei soggetti interessati. Durante la definizione del valore di EI devono essere tenuti in considerazione tutti i mezzi che ragionevolmente è probabile possano essere utilizzati da qualunque persona per identificare i soggetti interessati, tra cui, ad esempio, informazioni disponibili pubblicamente, detenute o ottenute in qualunque modo, incluse quelle reperibili tramite Internet, come anche incrociando dati presenti in altre fonti cui possono avere accesso il Titolare o terze parti.

La moltiplicazione dei valori di EI e DPC fornisce il valore iniziale della gravità (**Severity – SE**) della violazione.

Il valore di **CB** definisce specifiche circostanze della violazione che possono essere o non essere presenti. Nello specifico, i fattori da prendere in considerazione sono:

- **Perdita di confidenzialità**: avviene quando hanno avuto accesso alle informazioni soggetti che non sono autorizzati o non hanno un legittimo motivo per accedervi. L'entità della perdita di confidenzialità può variare in base all'ambito della divulgazione (es. il numero potenziale di soggetti che possono aver avuto accesso illegalmente alle informazioni) **(da 0 a 0,5 punti)**.

- **Perdita di integrità**: avviene quando le informazioni originali sono state alterate e la sostituzione dei dati può pregiudicare i soggetti interessati. La situazione più grave si verifica quando ci sono serie possibilità che i dati modificati siano stati usati in modo da arrecare danno ai soggetti interessati **(da 0 a 0,5 punti)**.
- **Perdita di disponibilità**: avviene quando non si può avere accesso ai dati originali nel momento in cui se ne abbia la necessità. Può essere sia temporanea (i dati possono essere recuperati, ma dopo un periodo di tempo che può risultare dannoso per i soggetti interessati) o permanente (i dati non possono essere in alcun modo recuperati) **(da 0 a 0,5 punti)**.
- **Comportamento doloso**: questo elemento valuta se la violazione è dovuta ad un errore, umano o tecnico, o se è stata causata da un'azione volontaria dovuta a un comportamento doloso. Il comportamento doloso è un fattore che può incrementare la probabilità che i dati vengano utilizzati con un intento dannoso per i soggetti interessati, potendo essere questo lo scopo originale della violazione **(0,5 punti)**.

A differenza di DPC ed EI, dove viene scelto il massimo punteggio ottenuto, nella stima del valore di CB i punti ottenuti da ciascun elemento vengono sommati per ottenere il punteggio finale, potendo presentarsi circostanze diverse all'interno della stessa violazione.

Il valore di CB si somma al valore iniziale calcolato della gravità della violazione, definendo il valore finale di **SE**.

Il valore finale della gravità **SE** della violazione può essere calcolato mediante la seguente formula:

SE = DPC X EI + CB

Il risultato ricadrà in un certo intervallo di valori che corrisponderà ad uno di quattro possibili livelli di gravità: **trascurabile (se il punteggio è sotto o uguale a 2)**, **basso (se il punteggio è tra 2 e 3)**, **medio (se il punteggio è tra 3 e 4)**, **alto (se il punteggio è superiore a 4)**.

ALLEGATO D – REGISTRO DELLE VIOLAZIONI

Si riporta un facsimile del registro delle violazioni da compilare a cura del Team Privacy, con il supporto del DPO.

N° violazione	Data violazione	Natura della violazione	Categoria di interessati	Categoria di dati perosnali coinvolti	Numero approssimativo di registrazioni dei dati personali	Conseguenze della violazione	Contromisure adottate	E' stata effettuata notifica all'Autorità Garante privacy?	E' stata fatta comunicazione agli interessati?