Comune di
Livinallongo del Col di Lana

REGOLAMENTO COMUNALE
PER LA PROTEZIONE DEI DATI PERSONALI IN ATTUAZIONE DEL REGOLAMENTO (UE) 2016/679

APPROVATO CON DELIBERAZIONE DEL CONSIGLIO COMUNALE N. 3 DEL 08.02.2023

ENTRA IN VIGORE DAL 11.03.2023

INDICE

ARTICOLO 1
(Oggetto e definizioni del regolamento)

1. Il presente regolamento dispone le misure per l'attuazione del "*Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*".
2. Ai fini del presente regolamento si intendono:
a) *Comune*: il Comune di Livinallongo del Col di Lana nella qualità di titolare del trattamento dei dati personali, le cui funzioni sono svolte dal Sindaco o suo delegato;
b) *RGPD*: il Regolamento (UE) 2016/679;
c) *Dato personale*: qualsiasi informazione che consente l'identificazione delle persone fisiche;
d) *Interessato*: la persona fisica oggetto del trattamento dei propri dati personali;
e) *Trattamento*: qualsiasi operazione o insieme di operazioni che può essere applicata ai dati personali;
f) *Limitazione di trattamento*: la marcatura dei dati personali conservati soggetti a future limitazioni di trattamento;
g) *Archivio*: qualsiasi aggregazione di dati personali accessibili secondo criteri determinati;
h) *Titolare del trattamento* (*di seguito, Titolare)*: Il sindaco o suo delegato che determina le finalità e i mezzi del trattamento dei dati personali nel Comune;
i) *Responsabile del trattamento (di seguito Responsabile)*: il soggetto che tratta i dati personali per conto del titolare del trattamento;
l) *Responsabile della protezione dei dati (di seguito, RPD)* ovvero *Data Protection Officer (DPO)*: il soggetto, designato dal Titolare e dal Responsabile, incaricato di fornire consulenza e assistenza per l'esatta osservanza del RGPD;
m) *Destinatario*: il soggetto che riceve comunicazione di dati personali;
n) *Terzo*: il soggetto che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento;
o) *Valutazione di impatto sulla protezione dei dati (di seguito DPIA)*: procedura di valutazione di un trattamento per valutarne la necessità e la proporzionalità, nonché i relativi rischi;
p) *Violazione dei dati personali di seguito, DATA BREACH)*: qualsiasi forma di trattamento, accidentale o illecita, che comporta la distruzione, la modifica, l'accesso o la divulgazione non autorizzata dei dati personali trattati;
q) *Autorità di controllo*: Il Garante per la protezione dei dati personali.

ARTICOLO 2
(Finalità del trattamento)

1. I dati personali acquisiti dal Comune sono trattati secondo i principi stabiliti dal RGPD e, in particolare, per l'esecuzione di dei compiti di interesse pubblico connessi all'esercizio dei pubblici poteri di cui è investito l'ente dalla normativa vigente.
2. Il trattamento dei dati è svolto, in particolare, per:
- l'esercizio delle funzioni amministrative di competenza comunale (servizi alla persona, gestione del territorio, sviluppo economico, ecc.)
- l'esercizio delle funzioni di competenza statale (stato civile, anagrafe, servizio elettorale, leva militare);
- l'adempimento di obblighi legali ai quali è soggetto il Comune;
- ulteriori funzioni amministrative di competenza statale affidate ai comuni;
- ulteriori funzioni, diverse da quelle precedenti, per le quali è stato espresso il consenso al trattamento dei dati personali.

ARTICOLO 3
(Titolare del trattamento)

1. Il Titolare del trattamento dei dati personali, contenuti in banche dati, informatiche o cartacee, gestite dagli uffici comunali, ai sensi e per gli effetti del Codice è il Comune, rappresentato dal Sindaco pro-tempore.
2. Il Sindaco, in qualità di Titolare:
- mette in atto le misure tecniche e organizzative necessarie a garantire la conformità dei trattamenti a quanto

disposto dal RGPD.
- nomina con proprio atto i responsabili del trattamento dei dati personali, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dagli articoli 13 e 14 del RGDP;
- adotta le misure di sicurezza per la conservazione, protezione e sicurezza dei dati e l'eventuale uso di apparecchiature di videosorveglianza;
- mette in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in modo conforme al RGDP.

ARTICOLO 4
(Responsabili del Trattamento)

1. Il Titolare, in considerazione della complessità e della molteplicità delle funzioni istituzionali del Comune, designa quali Responsabili del trattamento dei dati personali i responsabili che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento sia effettuato in conformità al RGDP.
2. Al Responsabile sono assegnati i seguenti compiti da specificare nell'atto di nomina:
- trattamento dei dati personali;
- garanzia che i soggetti autorizzati al trattamento dei dati personali siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adozione delle misure di sicurezza dei trattamenti previste dal RGDP (articolo 32);
- ricorso ad altro responsabile del trattamento nelle forme previste dal RGDP (articolo 28, par. 2 e 4);
- assistenza del Titolare, con misure tecniche e organizzative adeguate, per l'attuazione delle disposizioni del RGPD in materia di diritti dell'interessato (Capo III);
- assistenza del Titolare nel rispetto degli obblighi di sicurezza dei dati personali previsti dal RGDP (articoli 32 – 36);
3. Il Titolare può individuare quali Responsabili, dei soggetti esterni, purché sia in possesso delle garanzie tecniche e organizzative adeguate a garantire le prescrizioni del RGPD.
4. Nel caso in cui il Titolare affidi a soggetti esterni proprie attività comportanti un trattamento di dati personali, questi saranno nominati responsabili del trattamento, unitamente al dirigente/responsabile dell'area di competenza.
5. Il Titolare informa ciascun Responsabile, delle responsabilità che gli sono affidate in relazione a quanto disposto dal RGDP.
6. I responsabili del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata adozione delle misure di sicurezza.

ARTICOLO 5
(Responsabile della protezione dei dati – RPD
ovvero Data Protection Officer - DPO)

1. Il Titolare designa il Responsabile della protezione dei dati – RPD/DPO.
2. Il RPD è un professionista esterno, in possesso della competenza specifica della normativa e delle prassi in materia di protezione dei dati.
3. Il RPD deve essere in possesso di:
a) un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
b) deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
c) operare alle dipendenze del titolare del trattamento oppure sulla base di un contratto di servizio.
4. Il RPD è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.
5. Il Titolare mette a disposizione del RDP le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.
6. Il RDP svolge i seguenti compiti:
a) informa e fornisce consulenze al titolare del trattamento, nonché ai dipendenti che eseguono il trattamento

dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
b) verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
c) fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
d) funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
e) funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva, di cui all'art. 36 del RGDP.

ARTICOLO 6
(Registro unico delle attività di trattamento)

Il Titolare delega la sua tenuta e aggiornamento ai Responsabili del trattamento di cui al precedente art. 4 ovvero può decidere di affidare tale compito al RPD, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.
Il registro è tenuto in forma telematica e contiene le seguenti informazioni:
a) Il nome e i dati di contatto del Comune, del Titolare, del Responsabile del trattamento e del RPD;
b) Le categorie dei trattamenti effettuati;
c) Le categorie di destinatari a cui i dati personali sono o saranno comunicati;
d) L'indicazione delle cautele specifiche, a cui ciascun responsabile deve attendere in modo che siano appropriate rispetto ai trattamenti verso cui dovrà rispondere;
e) Eventuale possibilità di trasferimenti di dati all'estero;
f) Una descrizione generale delle misure di sicurezza tecniche e organizzative.

ARTICOLO 7
(Valutazione d'impatto sulla protezione dei dati – DPIA)

1. La DPIA deve essere realizzata dal Titolare prima di procedere al trattamento, quando questo, considerata sua natura, il contesto e le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
2. Il titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il RPD.
3. Il Titolare definisce prioritariamente l'elenco delle tipologie di trattamenti soggette al requisito della DPIA.
4. La valutazione del rischio viene svolta tenendo conto degli elementi che costituiscono il rischio: origine, natura, gravità, probabilità, impatto sui diritti e le libertà degli interessati e deve riguardare non solo la sicurezza ma anche gli effetti complessivi del trattamento.
5. Gli aspetti riguardanti la sicurezza sono:
- disponibilità (distruzione, indisponibilità, perdita);
- integrità (alterazione);
- riservatezza (divulgazione, accesso).
6. La valutazione degli effetti complessivi del trattamento deve tenere conto dei seguenti elementi:
- Danno per la reputazione;
- Discriminazione;
- Furto d'identità;
- Perdite finanziarie;
- Danni fisici ed economici;
- Perdita di controllo dei dati;
- Altri svantaggi economico-sociali;
- Impossibilità di esercitare diritti, servizi o opportunità.
7. Le misure per la gestione del rischio (accountability) devono riguardare le seguenti aree:
- qualità dei dati;

- cifratura;
- conservazione adeguata;
- anonimizzazione dei dati;
- minimizzazione;
- misure tecnologiche (policy di sicurezza logiche e fisiche, aggiornamenti servizi e software, test, controllo accessi e tracciamento operazioni);
- misure organizzative (ruoli, governance, istruzioni, formazione, procedure, audit, strumenti di controllo per gli interessati, contatti)

8. Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.

ARTICOLO 8
(Misure di sicurezza)

1. Il Comune, garantisce l'applicazione di idonee e preventive misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
2. Il Titolare e i Responsabili del trattamento mettono in atto misure e tecniche organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono:
a) la pseudonimizzazione e la cifratura dei dati personali trattati;
b) procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Il Titolare e il Responsabile del trattamento fanno sì che chiunque agisce sotto la loro autorità e ha accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare.

ARTICOLO 9
(**Violazione dei dati personali – Data Breach**)

1. La comunicazione dell'avvenuta violazione dei dati personali è effettuata dal Titolare, senza ingiustificato ritardo, al Garante dei dati personali.
2. Le modalità operative da seguire in caso di violazione dei dati personali avvenuta sia a seguito di trattamento informatizzato sia a seguito di trattamento cartaceo è descritta nel documento “Procedura Data Breach” allegato al presente Regolamento (Allegato 1).

ARTICOLO 10
(Misure per il rispetto dei diritti degli interessati)

1. Il Comune adotta idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dal RGDP.
2. Le misure comprendono, in particolare:
a) soluzioni volte a rispettare, in relazione a prestazioni o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;
b) l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;
c) soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni personali;
d) cautele volte ad evitare che le prestazioni avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;

e) il rispetto della dignità dell'interessato in occasione di ogni operazione di trattamento dei dati;
f) la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati;
g) la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

ARTICOLO 11
(Rinvio)

1. Per quanto non espressamente previsto dal presente regolamento si applicano le disposizioni del RGDP e le altre disposizioni previste in materia di tutela della riservatezza dei dati personali.

Allegato 1
al "Regolamento Comunale per la protezione dei dati personali
in attuazione del Regolamento (UE) 2016/679"

COMUN DA FODOM
COMUNE DI LIVINALLONGO DEL COL DI LANA
32020 – PROVINZIA DE BELUM / PROVINCIA DI BELLUNO

PROCEDURA
DATA BREACH

Scheda descrittiva

Anagrafica del documento

Titolo	**:**	Procedura data breach
Tipo documento	**:**	Procedura
Descrizione	**:**	Il documento descrive le modalità operative da seguire in caso di violazione dei dati personali avvenuta sia a seguito di trattamento informatizzato sia a seguito di trattamento cartaceo.

INDICE

1 PREMESSA

Il 25 maggio 2018 è diventato definitivamente applicabile in tutti i Paesi europei il Regolamento generale sulla protezione dei dati 2016/679 (di seguito "GDPR") con ricadute organizzative, operative e tecnologiche che riguardano i principali processi di gestione dei dati personali. Tra le novità contenute nel Regolamento, anche alcuni oneri aggiuntivi per la gestione degli incidenti di sicurezza che comportano la violazione di dati personali (data breach).

Il presente documento descrivere i criteri per individuare una violazione di dati personali e per valutare i casi in cui la violazione debba essere notificata all'Autorità di controllo e agli interessati, in conformità con le indicazioni del GDPR.

Nel paragrafo 5 sono presi in considerazione gli eventi relativi a trattamenti informatizzati nel caso in cui la eventuale violazione avvenga nell'ambito dei servizi messi a disposizione dal Comune di Livinallongo del Col di Lana, di seguito anche "Ente".

Nel paragrafo 6, invece, sono trattati gli eventi relativi a trattamenti non informatizzati.

2 CONTESTO DI RIFERIMENTO E QUADRO GIURIDICO

Le norme di riferimento sono:

1. Regolamento UE n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);
2. Documento WP 250 "Guidelines on Personal data breach notification under Regulation 2016/679" del 3 ottobre 2017;
3. Linee guida 01/2021 sugli esempi riguardanti la notifica di violazione dei dati.

3 CRITERI PER INDIVIDUARE E CLASSIFICARE UN DATA BREACH

Un data breach, o violazione di dati personali, è un incidente di sicurezza che *"comporta 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".*

In relazione ad un evento che si è verificato o che si presume si possa verificare (minaccia) come conseguenza di un altro evento illecito o accidentale, la violazione di dati personali viene classificata in tre tipologie:

Tipologia di violazione	Evento/Minaccia
Violazione di riservatezza	Accesso o trattamento non autorizzato o illecito
	Divulgazione non autorizzata
Violazione di integrità	Modifica non autorizzata o accidentale
Violazione di disponibilità	Perdita o distruzione accidentale o illegale
	Indisponibilità temporanea o prolungata

Tabella 1 – Classificazione di un data breach

Le tipologie non sono mutuamente esclusive: una violazione di dati personali può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità, una di esse o una loro combinazione.

4 NOTIFICHE E COMUNICAZIONI

Il GDPR prevede che il Titolare del trattamento debba notificare la violazione di dati personali all'Autorità di controllo e agli interessati se questa comporta dei rischi per i diritti e le libertà delle persone fisiche coinvolte.

In presenza di un data breach, quindi, il Titolare stima tale rischio e decide, sulla base del risultato ottenuto e delle circostanze in cui l'evento si è verificato, se procedere alle relative notifiche.

I prossimi paragrafi riportano:

- le modalità di valutazione del rischio per i diritti e le libertà degli interessati in caso di violazione di dati personali;
- i criteri che fanno scattare l'obbligo di notifica all'Autorità di controllo e le modalità di notifica;
- i criteri che fanno scattare l'obbligo di comunicazione agli interessati e le modalità di notifica.

4.1 VALUTAZIONE DEL RISCHIO PER I DIRITTI E LE LIBERTÀ DELL'INTERESSATO

Nel seguito viene illustrata la metodologia adottata per la valutazione del rischio per i diritti e le libertà dell'interessato derivante da un trattamento di dati personali che avvenga sia mediante strumenti informatici e telematici, sia manuali.

Il rischio per l'interessato, che può assumere i valori Medio (M) o Alto (A), viene valutato sulla categoria dei dati personali trattati (cfr. Appendice 2) in base alla gravità del danno (fisico-biologico, finanziario, reputazionale e di identità) e alla probabilità di accadimento delle minacce riportate nella Tabella 1.

Minaccia	Categoria di dati personali	Rischio per l'interessato
Accesso, trattamento non autorizzato o illecito	Dati personali comuni	M
	Dati particolari	A
	Dati giudiziari	A
Divulgazione non autorizzata o accidentale	Dati personali comuni	M
	Dati particolari	A
	Dati giudiziari	A
Modifica non autorizzata o accidentale	Dati personali comuni	M
	Dati particolari	A
	Dati giudiziari	A

Perdita, distruzione accidentale o illecita	Dati personali comuni	M
	Dati particolari	A
	Dati giudiziari	A
Indisponibilità temporanea o prolungata	Dati personali comuni	M
	Dati particolari	A
	Dati giudiziari	A

Tabella 2 - Valori di rischio per i diritti e le libertà dell"interessato

Una volta individuato e classificato un data breach come descritto nel paragrafo 3, vengono considerati i valori di rischio corrispondenti agli eventi che si sono verificati o che si presume si possano verificare in seguito all'incidente.

Come si desume dalla tabella, il rischio per l'interessato è Medio solo nel caso in cui i dati trattati appartengano alla categoria "dati personali comuni" (cfr. Appendice 2).

Il rischio per l'interessato può essere aumentato in considerazione dei seguenti fattori:

- la natura, la sensibilità e il volume dei dati violati. Una violazione di più dati personali riferiti alla stessa persona, infatti, può aumentare la gravità del danno per l'interessato;
- la facilità di identificare specifici individui;
- l'analisi del contesto in cui si è verificata la violazione (attacco informatico, errore umano, …);
- le caratteristiche specifiche degli interessati (minori, categorie vulnerabili, …);
- la numerosità degli interessati, qualora indica sulla gravità del danno.

4.2 NOTIFICA ALL'AUTORITÀ DI CONTROLLO IN CASO DI INDISPONIBILITÀ DEI DATI PERSONALI

Il GDPR prevede che il Titolare del trattamento debba notificare all'Autorità di controllo una violazione di dati personali *"senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche".*

Per quanto riguarda il caso particolare della indisponibilità temporanea o prolungata di dati personali dovuta ad indisponibilità del servizio che li tratta tra i fattori di valutazione deve essere incluso il tempo in cui i dati non sono disponibili. Se viene garantita la continuità operativa o il ripristino in tempi adeguati per scongiurare un danno per gli interessati, la notifica all'Autorità di controllo non è necessaria.

Nel caso in cui la violazione non riguardi solo l'indisponibilità, ma anche altri eventi certi o presunti (ad esempio si suppone che i dati, oltre a essere indisponibili, siano stati acceduti illecitamente), la valutazione, pur tenendo conto dei tempi di indisponibilità indicati in tabella, deve comprendere l'analisi di tutti gli eventi correlati.

4.3 COMUNICAZIONE AGLI INTERESSATI

Quando il rischio per l'interessato, valutato come specificato nel paragrafo 4.1, assume il valore Alto ("rischio elevato", GDPR art. 34), la violazione deve essere comunicata anche agli interessati.

Fanno eccezione i seguenti casi:

- i dati violati sono stati preventivamente protetti da misure tecniche e organizzative adeguate a scongiurare un rischio residuo elevato per gli interessati (ad esempio la cifratura o la pseudonimizzazione);
- i dati personali sono stati indisponibili per un periodo di tempo inferiore a 1 ora e non si è verificata alcuna altra tipologia di violazione;
- la comunicazione richiede un impegno spropositato. È il caso, ad esempio, di violazioni massive di dati. In queste circostanze si può procedere a una comunicazione pubblica o di pari efficacia.

La comunicazione deve descrivere, con un linguaggio semplice e chiaro, la natura della violazione e deve inoltre contenere:

- il nome e i dati di contatto del Responsabile della protezione dei dati, del Titolare del trattamento o di altro contatto da cui ottenere maggiori informazioni;
- la descrizione delle probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e attenuarne i possibili effetti negativi.

4.4 PROCESSO DI VERIFICA E NOTIFICA DI PRESUNTO DATA BREACH

Tale procedura si applica, tenendo conto delle rispettive specificità, sia a trattamenti informatizzati sia a trattamenti eseguiti senza l'ausilio di strumenti informatici.

Per trattamenti informatizzati nell'ambito di questo documento si intendono quelli effettuati mediante applicazioni o strumenti di office automation. In tale ambito si fa riferimento alle misure tecniche ed organizzative adottate per la riduzione del rischio residuo come descritte nel Registro dei Trattamenti.

Per trattamenti non informatizzati nell'ambito di questo documento si intendono quelli effettuati senza l'ausilio di strumenti elettronici, ovvero nei casi in cui i dati risiedono su supporto cartaceo. In tale ambito assumono significativa rilevanza le istruzioni impartite per iscritto, sia al momento della nomina sia mediante apposite policies aziendali, alle persone autorizzate (c.d. Autorizzati al trattamento) finalizzate all'utilizzo, al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali, in special modo se contenenti dati personali sensibili, ipersensibili e giudiziari, e l'adozione degli adeguati comportamenti da parte degli autorizzati stessi.

In particolare il Titolare:

- individua, e verifica periodicamente, gli incaricati del trattamento che utilizzano strumenti non automatizzati per la raccolta e la gestione di dati personali e impartisce loro istruzioni scritte relative alla gestione dei dati e alla loro custodia;
- identifica e comunica agli incaricati gli archivi in cui riporre i documenti contenenti i dati personali e/o categorie particolari di dati (armadi chiusi a chiave, stanze chiuse a chiave, casseforti di sicurezza, ecc.);
- istruisce le persone autorizzate affinché i documenti cartacei vengano conservati in archivi adeguatamente protetti per evitare la lettura e/o il prelievo non autorizzato, garantendo, quindi, la riservatezza e l'integrità dei dati personali in essi contenuti;
- dispone che i documenti cartacei vengano custoditi in appositi archivi chiusi a chiave,

- in armadi o stanze, al termine della giornata lavorativa; le chiavi devono essere risposte in un luogo sicuro e non lasciate nelle serrature stesse;
- prevede, ove possibile, la conservazione dei documenti contenenti dati personali di categorie particolari (ad esempio sensibili e/o giudiziari) separata dai documenti contenenti dati personali comuni;
- dispone che il trattamento di dati personali e/o di categorie particolari degli stessi avvenga nel rispetto del principio di limitazione della finalità, ovvero unicamente per lo scopo per cui sono stati raccolti;
- istruisce le persone autorizzate affinché:
  - i dati personali e/o le categorie particolari degli stessi non vengano diffusi o comunicati a soggetti non autorizzati al trattamento;
  - non vengano lasciati incustoditi documenti contenenti i dati personali e/o le categorie particolari degli stessi durante e dopo l'orario di lavoro;
  - non vengano lasciati in luoghi accessibili al pubblico i documenti contenenti i dati personali e/o le categorie particolari degli stessi;
  - i documenti vengano riposti negli archivi quando non più operativamente necessari;
  - limitino allo stretto necessario l'effettuazione di copie dei suddetti documenti;
  - verifichino la corretta esecuzione delle procedure di distruzione dei documenti, quando non più necessari o quando richiesto dall'interessato, attraverso l'utilizzo diopportuni strumenti (distruggidocumenti), in modo da rendere impossibile la ricostruzione del documento.

Nel caso in cui, nonostante le misure adottate dal Titolare, si verifichino uno o più eventi di cui alla tabella 1, il flusso operativo che viene seguito è di seguito illustrato:

1. ogni autorizzato al trattamento deve avvisare immediatamente l'assistenza tecnica e il DPO segnalando le violazioni o gli incidenti informatici che ha rilevato e che possono avere impatto significativo sui dati personali, con la più ampia libertà di forme e procedure (anche per le vie brevi e/o oralmente);
2. dovrà seguire nel più breve tempo possibile (si ricorda che il GDPR fissa in 72 ore il tempo massimo che deve intercorrere dal momento in cui ne è venuto a conoscenza e la notifica al garante se del caso) formale comunicazione con mail all'indirizzo dpo@veronicadeirossi.com completa dei dettagli sull'evento segnalato;
3. ai fini del rispetto dei tempi prescritti dalla normativa, il Titolare del trattamento provvederà immediatamente e comunque non oltre le 24 ore successive alla ricezione della comunicazione ad effettuare la valutazione preliminare sulla probabilità e gravità dei rischi per i diritti e le libertà degli interessati che possono derivare da trattamenti dei dati personali oggetto di violazione;
4. il Titolare, coordinato con il DPO, dovrà quindi curare e documentare l'attività istruttoria, acquisendo tutti gli elementi probatori necessari per una adeguata valutazione;
5. all'esito delle attività dovrà essere raccolta la documentazione di supporto, ricognitiva delle analisi e degli esiti della valutazione effettuata nonché delle conseguenti proposte operative, da ponderare per la decisione finale;

6. Sulla base della documentazione relativa alla segnalazione, in relazione all'esito della valutazione del rischio, il Titolare procederà nel seguente modo:

   - ove risulti probabile che dalla violazione possano derivare rischi per i diritti e per le libertà degli interessati, provvederà a:

     a) notificare il data breach all'Autorità di Controllo (art. 33 GDPR);

   - ove risulti probabile che dalla violazione possano derivare elevati rischi per i diritti e le libertà degli interessati, provvederà a:

     a) notificare il data breach all'Autorità di controllo (art. 33 GDPR);

     b) comunicare il data breach ai soggetti cui si riferiscono i dati (c.d. Interessati) nei limiti e secondo quanto previsto dall'art. 34 GDPR;

   - ove invece risulti improbabile che dalla violazione possano derivare rischi per i diritti e le libertà degli interessati, il Titolare del trattamento non procederà con le notifiche e comunicazioni di cui ai precedenti punti.

La comunicazione deve essere redatta con particolare cura ed attenzione in quanto potrebbe dar luogo ad un intervento dell'Autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal Regolamento medesimo.

Il Titolare del trattamento documenta qualsiasi violazione dei dati personali comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Atteso che tale documentazione consente all'Autorità di Controllo di verificare in qualsiasi momento, il rispetto del GDPR in materia di data breach, la stessa sarà custodita, con la massima cura e diligenza, dal Titolare del trattamento il quale dovrà tenere apposito registrocronologico elaborato secondo variabili di interesse, dei casi di violazione dei dati.

4.5 FORM DI NOTIFICA ALL'AUTORITA' DI CONTROLLO

La notifica all'Autorità di Controllo (il Garante per la Privacy ha espressamente previsto nel proprio sito web una piattaforma ad hoc per le notifiche di data breach) conterrà necessariamente i seguenti dati:

- tipologia di incidente;
- descrizione del servizio impattato e/o della banca/banche dati oggetto di violazione di dati personali;
- intervallo temporale dell'incidente;
- luogo dell'incidente;
- misure tecniche di sicurezza applicate ai dati violati;
- misure attivate per il contenimento e la prevenzione;
- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- descrizione della probabile conseguenza della violazione dei dati personali;
- descrizione delle misure di sicurezza adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione di dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;

- proposta di comunicazione di violazione di dati personali all'/agli interessato/i in base ad un'analisi dei dati oggetto di violazione (qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche) e non ricorrendo alcuna delle condizioni di cui all'articolo 34, comma 3, del GDPR, che escludono la necessità di comunicazione della violazione all'interessato;
- il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- i dati organizzativi di riferimento e i relativi recapiti dell'Istituto;
- il livello di gravità della violazione;
- l'eventuale comunicazione agli interessati e le relative modalità;
- qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, i motivi del ritardo.

Appendice 1 – Acronimi e Glossario

Autorità di controllo (o autorità Garante)	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR.
Data breach (o violazione di dati personali)	"Violazione di sicurezza che comporta 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" (GDPR, art. 4 punto 12).
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" (GDPR, art. 4 punto 1).
Danno	Conseguenza negativa derivante dal verificarsi di una determinata minaccia; il danno può qualificarsi come materiale quando determina una concreta lesione all'ambito fisico o patrimoniale dell'interessato oppure immateriale quando riguarda le possibili conseguenze dannose derivanti dal trattamento di dati personali, di natura non patrimoniale e che affliggono la sfera interiore del soggetto interessato.
Responsabile della protezione dei dati o DPO	Soggetto cui è attribuito dal Titolare del trattamento il compito di informare e fornire consulenza sugli obblighi derivanti dal GDPR e di sorvegliarne l'osservanza. Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (PIA) e ne sorveglia lo svolgimento. Coopera con l'Autorità di controllo e funge da punto di contatto con essa (GDPR, art. 37, 38, 39).
GDPR	Regolamento Ue n. 679/2016 "*General Data Protection Regulation",* in italiano indicato come "Regolamento generale sulla protezione dei dati".
Interessato	La persona fisica cui si riferiscono i dati personali.
Minaccia	Una serie di eventi dannosi che possono compromettere le caratteristiche di integrità, riservatezza e disponibilità del dato personale.
Misura di sicurezza	Accorgimento tecnico e organizzativo utilizzato per garantire che i dati non vadano distrutti o persi anche in modo accidentale, per garantire che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.

Privacy Impact Assessment (PIA)	Valutazione d'impatto che deve essere compiuta dal titolare quando "un tipo di trattamento (…) può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (GDPR, art. 35).
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica o altro organismo che tratta dati personali per conto del titolare del trattamento.
Servizio ICT	Insieme di funzionalità informatiche omogenee destinate a supportare un processo o un'attività lavorativa. Un servizio informatico è composto da una o più applicazioni software e dalla relativa infrastruttura tecnologica di supporto.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Trattamento	Operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali, come la raccolta, la registrazione, la conservazione, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione, la distruzione, ecc.

Appendice 2 – Categorie di dati personali

Dati personali comuni	
Anagrafici	Dati personali anagrafici quali nome, cognome, data e luogo di nascita, stato civile, residenza.
Contabili, fiscali, inerenti possidenze e riscossione	Dati personali quali versioni parziali/integrali di documenti contabili, dati di dettaglio risultanti dalle dichiarazioni fiscali oppure dai cedolini dello stipendio di ciascun lavoratore, indicazioni di dati riferiti a percettori di somme (e.g. i recapiti individuali e le coordinate bancarie utilizzate per effettuare i pagamenti), complesso dei beni posseduti (e.g case, terreni, altre proprietà).
Inerenti il rapporto di lavoro	Dati personali inerenti l'esecuzione del rapporto di lavoro: tipologia di contratto e livello contrattuale, dettagli di assunzione, irrogazione di sanzioni disciplinari, stipendio, trasferimenti del lavoratore, etc.
Tracciamenti	Dati personali presenti nei tracciati record generati dalla registrazione delle operazioni svolte su sistemi, applicativi, ecc.
Dati inerenti situazioni giudiziarie civili, amministrative, tributarie	Trattamento di dati personali quali cartelle tributarie, pagamenti, rateizzazioni, procedure in corso, assenza o esistenza di condanne emesse, contenziosi pendenti.
Dati personali (comuni) specifici	
Dati che consentono geolocalizzazione	Dati personali derivanti dalla rilevazione di coordinate satellitari relative alla geolocalizzazionedi apparati elettronici di tipo radio mobili e veicolari, celle territoriali agganciate dai ricevitori GPS, dati relativi agli indirizzi IP.
Audio/video/foto	Audio, video, fotogrammi, immagini che possano far riconoscere, tramite riconoscimento facciale, vocale e/o comportamentale, la persona fisica.
Dati di profilazione	Dati riguardanti aspetti personali relativi a una persona fisica, che ne consentano di identificare preferenze, interessi, analizzare o prevedere il rendimento professionale, la situazione economica, la salute, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti del soggetto.
Dati personali finanziari	
Dati relativi all'esistenza di rapporti finanziari (coordinate bancarie, consistenze saldi, movimenti, giacenza media, etc.)	Dati relativi alla situazione bancaria attuale e/o passata dell'interessato, informazioni gestite da operatori finanziari quali: i saldi iniziali e finali del rapporto, il totale dei movimenti annuali in entrata e in uscita, la c.d. giacenza annuale media etc.

Dati personali particolari	
Convinzioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	Dati personali che possano rivelare convinzioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.
Stato di salute, assistenza sanitaria, orientamento/vita sessuale	Attinenti: - lo stato di salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, dati idonei a rivelare informazioni relative al suo stato di salute, ad esempio, certificato medico, cartella clinica, etc. - l'orientamento sessuale e/o la vita sessuale della persona fisica
Genetici	Dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione.
Dati personali biometrici	
Impronte digitali	Dati personali relativi ad impronte digitali e caratteristiche della topografia della mano, utilizzate per l'identificazione degli esseri umani.
Altre caratteristiche biometriche	Dati relativi ad altre caratteristiche fisiche quali: retina, vascolarizzazione, forma del volto. Possono intendersi caratteristiche biometriche anche caratteristiche comportamentali quali impronta vocale, movimenti del corpo, stile di battitura sulla tastiera.
Firma grafometrica	Firma grafometrica, analoga alla firma “olografa”, inserita in un'apposita tavoletta elettronica conl'ausilio di una penna elettronica.
Dati personali giudiziari	
Casellario giudiziale	Dati contenuti all'interno del certificato penale del casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione).
Qualità di indagato/imputato o altre situazioni giudiziarie e reati o connesse misure di sicurezza	Dati idonei a rivelare che un determinato soggetto è stato sottoposto ad indagini di polizia giudiziaria, al termine delle quali, è stato accusato di un reato nell'ambito di un Procedimento penale (certificato dei carichi pendenti).

Registro delle violazioni dei dati (data breach)

Data e ora in cui si è venuti a conoscenza della violazione	
Data presunta della violazione	
Circostanze della violazione	
Trattamenti di dati interessati	
Tipo di violazione	
Dispositivo oggetto della violazione	
Descrizione sintetica dei sistemi coinvolti e ubicazione	
Categorie di dati coinvolti nella violazione	
Categorie particolari di dati	
Misure tecniche e organizzative applicate ai dati colpiti dalla violazione	
Numero di interessati	
Livello di gravità	
Conseguenze ipotizzabili	
Provvedimenti adottati per porre rimedio	
La violazione è da notificare al Garante Privacy?	
Data di notifica (se notificata al Garante)	
La violazione è da notificare agli interessati?	
Data di notifica (se notificata agli interessati)	
Misure tecniche ed organizzative assunte per contenere la violazione dei dati e prevenire simili violazioni future	