PRIVACY POLICY

Sommario

1.PREMESSA

La presente Privacy Policy (“Policy”) è volta ad illustrare i princìpi e gli obblighi ai quali si attengono dipendenti, collaboratori, stagisti e, più in generale, il personale che collabora direttamente o indirettamente con LABORATORI ANALISI SALVO S.R.L. (la “Società” o il “Titolare”), al fine di assicurare il rispetto del Reg. UE n. 679 del 27 aprile 2016 relativo alla protezione e alla libera circolazione dei dati personali ("Regolamento" o "GDPR"), del D. Lgs. del 30 giugno 2003, n. 196 come modificato dal D. Lgs. 101/2018, recante il Codice per la protezione dei dati personali (il “Codice”) e la normativa e i provvedimenti applicabili in materia di protezione dei dati personal (“Normativa Privacy”).

2.DEFINIZIONI

Dato personale: indica 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.

Categorie particolari di dati personali: 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.

Trattamento: indica 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.

Profilazione: indica 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.

Consenso: 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.

Interessato: indica la persona fisica (ivi comprese le ditte individuali e i liberi professionisti) cui i dati personali si riferiscono.

Titolare del trattamento: la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che determina le finalità e i mezzi del trattamento di dati personali, anche rispetto al profilo della sicurezza.

Responsabile: indica la persona fisica o giuridica (quali ad esempio outsourcer, fornitori di servizi, consulenti, distributori ed agenti), l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento ai sensi dell’art. 28, GDPR.

Autorizzato: i dipendenti e/o collaboratori del Titolare che hanno ricevuto una specifica lettera di autorizzazione al trattamento, nonché apposite istruzioni ai sensi dell’art. 29, GDPR e 2-quaterdecies, Codice Privacy.

Violazione dei dati personali o data breach: indica qualsiasi incidente di sicurezza che comporta – accidentalmente o in modo illecito , e anche se temporanea – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Garante: indica l’Autorità Garante per la protezione dei dati personali.

3.REGOLE PER IL CORRETTO TRATTAMENTO DEI DATI PERSONALI

3.1.INFORMATIVA

L'interessato deve ricevere idonea informativa in merito al trattamento dei suoi dati personali. Tale informativa deve essere consegnata al momento in cui i dati personali vengono raccolti. L'informativa, ove i dati personali siano ricevuti per il tramite di terzi o raccolti tramite fonti pubbliche, deve essere fornita:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanza in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi in occasione del primo contatto utile con l'interessato;
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

L'informativa deve contenere talune informazioni espressamente previste dalla legge, con particolare riferimento a quelle di cui agli artt. 13 e 14 GDPR.

3.2.CONSENSO DELL'INTERESSATO

Il consenso esplicito al trattamento dei dati personali dell'interessato è sempre necessario, salve le eccezioni sotto riportate previste ai sensi degli artt. 6 e 9 GDPR.

Il trattamento di dati personali comuni (i.e. diversi dalle categorie particolari di dati di cui all'art. 9, GDPR o dai dati giudiziari di cui all'art. 10, GDPR) è ammesso quando avviene sulle basi giuridiche di cui all'articolo 6 del GDPR, per esempio quando il trattamento:

- è necessario per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento;
- è necessario per l'esecuzione di un contratto del quale è parte l'interessato o all'esecuzione di misure precontrattuali adottate su richiesta dell'interessato;
- è necessario per l'esecuzione di un compito di interesse pubblico;
- l'interessato ha prestato il proprio consenso al trattamento conformemente alla Normativa Privacy;

Il trattamento di dati personali rientranti tra le particolari categorie di dati è proibito a meno che non si verifichi almeno una delle condizioni di cui all'articolo 9 del GDPR, fra le quali, in particolare:

- l'interessato ha prestato il proprio esplicito consenso al trattamento per una o più finalità specifiche;
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- il trattamento riguarda dati resi manifestatamente pubblici dall'interessato;
- il trattamento è necessario per motivi di interesse pubblico rilevante.
- il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità.

Spetta al Titolare individuare, di volta in volta e prima dell'avvio delle operazioni di trattamento, la base giuridica applicabile al singolo caso considerato. La base giuridica del trattamento deve essere comunicata all'interessato insieme con le altre informazioni di cui agli artt. 13 e 14, GDPR.

Il consenso espresso da parte dell'interessato deve essere documentato in formato cartaceo, elettronico o tramite una registrazione e tracciato nei sistemi informatici al fine di poter rispettare il principio di *accountability* e dimostrare di aver legittimamente raccolto il consenso e rispettato la Normativa Privacy.

3.3.RICHIESTE DELL'INTERESSATO IN MERITO ALL'ESERCIZIO DEI SUOI DIRITTI

Gli interessati possono esercitare i diritti di cui al presente paragrafo inviando una richiesta via e-mail al seguente indirizzo: labsalvo@hotmail.com, o tramite posta all'indirizzo Via Calatafimi 8/C – 91026 Mazara del Vallo (TP).
In caso di invio di una richiesta da parte di un interessato, il ricevente dovrà inoltrarla immediatamente al Titolare del trattamento, nella persona del suo Legale Rappresentante. Quest'ultimo è tenuto, previo confronto con il D.P.O. aziendale, ad annotare in un registro, sotto la sua responsabilità, tutte le richieste di esercizio dei diritti.

Allo stesso modo, qualora la richiesta dell'interessato venga formulata da un terzo che tratta i suoi dati personali per conto di LABORATORI ANALISI SALVO S.R.L. (e.g. un fornitore), tale terzo dovrà darne immediata comunicazione al Titolare del trattamento, nella persona del suo Legale Rappresentante.

Una volta ricevuta una richiesta da parte dell'interessato, il Titolare del trattamento o un suo incaricato dovranno osservare i seguenti step:

a) verificare l'identità dell'interessato che ha formulato l'istanza, confrontando i dati di cui alla richiesta con i dati già in possesso della Società, ove disponibili;
b) qualora vengano riscontrate delle discrepanze o dati non sufficienti a identificare l'interessato, contattare l'interessato stesso, richiedendogli di inviare copia del suo documento di identità.

In seguito all'accertamento dell'identità del richiedente, provvedere a:

a) coordinarsi con i dipartimenti competenti per poter circoscrivere l'oggetto della richiesta e garantire una risposta tempestiva;
b) dare pronto riscontro, in forma scritta, all'interessato entro e non oltre 30 giorni di calendario dalla prima richiesta.

Ove la richiesta venga ritenuta particolarmente complessa dagli uffici competenti, provvedere a:

a) comunicare all'interessato l'eventuale proroga del termine motivando in dettaglio le ragioni di carattere eccezionale che hanno richiesto una tempistica di evasione del riscontro maggiore di 30 giorni di calendario dalla sua richiesta;
b) fornire riscontro all'interessato entro un massimo di due mesi dalla comunicazione di proroga.

Non è possibile applicare alcun corrispettivo per dare seguito alle richieste degli interessati ad eccezione del caso in cui:

a) la richiesta dell'interessato sia manifestatamente infondata o eccessiva in ragione del carattere ripetitivo della stessa;
b) con riferimento al diritto di accesso, l'interessato richieda delle copie aggiuntive rispetto a quelle fornite con la prima richiesta;
c) con riferimento al diritto alla portabilità, la richiesta sia manifestamente eccessiva o infondata.

3.3.1.Diritto di accesso dell'interessato

L'interessato ha il diritto di richiedere la conferma che sia o meno in corso un trattamento di dati personali che lo riguarda e, in tal caso, ha il diritto di:

a) ottenere l'accesso ai propri dati personali;
b) conoscere l'origine dei propri dati personali;
c) conoscere le finalità del trattamento;
d) conoscere le categorie di dati personali trattati;
e) ove possibile, conoscere il periodo di conservazione dei dati personali, ovvero i criteri utilizzati per determinare tale periodo;
f) chiedere al Titolare la rettifica o la cancellazione dei dati o la limitazione del trattamento dei dati che lo riguardano o di opporsi al loro trattamento;
g) essere messo a conoscenza dell'esistenza di un processo decisionale automatizzato, ivi inclusa la profilazione e delle relative conseguenze di tale processo;

h) conoscere i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza, in particolare se tali destinatari si trovano in Paesi terzi - in tal caso il titolare dovrà altresì fornire evidenza dell'esistenza di garanzie adeguate al trasferimento;
i) di proporre reclamo al Garante.

Il soggetto cui i dati personali si riferiscono può altresì richiedere una copia dei dati trattati purché questo non violi i diritti e le libertà di altri interessati.

3.3.2.Diritto di rettifica e di integrazione

L'interessato ha il diritto di ottenere la rettifica dei dati personali inesatti o l'integrazione dei dati personali incompleti, scrivendo ai recapiti che il Titolare ha comunicato nell'informativa e nei canali istituzionali di comunicazione di volta in volta applicabili (e.g., bacheca dei lavoratori, pagine web del Titolare, etc.)

3.3.3.Diritto alla cancellazione

L'interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano ove:

a) i dati dell'interessato non sono più necessari rispetto alle finalità per le quali sono stati raccolti;
b) l'interessato ha revocato il consenso su cui si basa il trattamento e non sussiste altra base giuridica per il trattamento;
c) l'interessato si oppone al trattamento;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere ad un obbligo legale;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Laddove non sussistano circostanze nelle quali i dati dell'interessato devono essere conservati per obblighi di legge, gli uffici competenti del Titolare collaboreranno al fine di garantire che tali dati siano cancellati senza ingiustificato ritardo, e comunque entro i 30 giorni dalla data in cui l'Interessato ha comunicato la propria volontà di esercitare un diritto previsto dalla Normativa Privacy.

3.3.4.Diritto di limitazione di trattamento

L'interessato può ottenere la limitazione del trattamento dei dati che lo riguardano rendendoli, per un ristretto periodo di tempo, inutilizzabili ove:

a) contesti l'esattezza dei suoi dati personali (in tale caso la limitazione del trattamento è circoscritta al periodo di tempo necessario a verificare la correttezza dei dati stessi);
b) il trattamento sia illecito e l'interessato si opponga alla cancellazione dei dati chiedendone la sola limitazione
c) i dati siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) si sia opposto al trattamento per motivi connessi alla sua situazione in attesa che il Titolare verificasse l'eventuale prevalenza di motivi legittimi per effettuare il trattamento.

Al verificarsi di quanto sopra, il Titolare tratterà i dati personali dell'interessato solo per finalità di conservazione, secondo modalità definite dagli uffici competenti del Titolare.

In pendenza della limitazione del trattamento, il Titolare potrà effettuare attività di trattamento dei dati diverse dalla conservazione soltanto laddove:

a) l'interessato abbia fornito il proprio consenso;
b) ciò sia necessario per la difesa di un proprio diritto in giudizio;
c) ciò sia necessario a garantire la tutela dei diritti di un terzo;
d) vi siano rilevanti motivi di interesse pubblico.

3.3.5.Diritto alla portabilità

L'interessato ha il diritto di:

a) ottenere i dati personali che lo riguardano; e
b) richiederne la trasmissione diretta ad altro titolare del trattamento;

Ciò nel caso in cui:

a) il trattamento sia effettuato con mezzi automatizzati;
b) il trattamento si basi sul consenso dell'interessato o su un contratto di cui l'interessato è parte;
c) i dati oggetto di portabilità siano stati forniti dall'interessato (a tal proposito si rileva che tra i dati forniti dall'interessato sono inclusi anche i dati personali osservati sulla base delle attività svolte dagli utenti, ma non i dati personali che siano derivati o dedotti dalle informazioni fornite dall'interessato).

3.3.6.Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento di dati personali che lo riguardano. Il Titolare del trattamento si astiene in tal caso dal trattare ulteriormente i dati personali, salvo dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

3.3.7.Diritto a non subire decisioni unicamente basate su trattamenti automatizzati

L'interessato ha infine la possibilità di richiedere di non essere soggetto a decisioni basate unicamente su trattamenti automatizzati, ivi inclusa la profilazione, ad eccezione del caso in cui:

a) tale decisione sia necessaria ai fini della conclusione o esecuzione di un contratto tra l'interessato e il Titolare;
b) tale decisione sia basata sul consenso esplicito dell'interessato medesimo.

4.TEMPI DI CONSERVAZIONE

Ai sensi del GDPR, i dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. Onde assicurare che i dati personali non siano conservati (in una forma che consenta l'identificazione degli interessati) più a lungo del necessario, il Titolare del trattamento deve stabilire un termine per la cancellazione o per la verifica periodica. Stabilire tempi di conservazione dei dati in misura strettamente necessaria è, nello stesso tempo, funzionale a garantire l'adozione di misure tecniche e organizzative adeguate al rispetto dei diritti degli interessati.

I tempi di conservazione dei dati devono essere indicati nell'informativa consegnata agli interessati - non solo quando i dati sono raccolti direttamente dall'interessato ma anche quando siano stati ottenuti da una terza parte - e devono essere strettamente necessari al fine di dare esecuzione alla finalità specifica indicata nell'informativa stessa. I tempi di conservazione dei dati sono rilevanti, tra le altre cose, anche nel caso di esercizio dei diritti da parte degli interessati secondo le modalità e procedure delineate sopra.

LABORATORI ANALISI SALVO S.R.L. stabilisce un tempo di conservazione dei dati di dieci anni, indicati nello specifico nel registro delle attività di trattamento adottato ai sensi dell'art. 30 GDPR . Alla scadenza del termine di conservazione, i dati saranno irreversibilmente cancellati e/o anonimizzati secondo procedure idonee a garantire l'impossibilità oggettiva e soggettiva di re-identificare, anche indirettamente, l'interessato.

Il Titolare verifica che i presidi adottati siano idonei a garantire la tempestiva cancellazione o anonimizzazione dei dati allo scadere del tempo di conservazione previsto.

4.1.Modalità di archiviazione dei documenti cartacei ed elettronici contenenti dati personali

Tutti i soggetti che trattano dati per conto del Titolare (e.g., responsabili del trattamento) e/o che fanno parte delle persone autorizzate al trattamento devono attenersi alle seguenti prescrizioni:

a) i cassetti delle scrivanie, gli armadi e gli altri contenitori o gli uffici ove sono depositati documenti contenenti informazioni riservate o dati personali utilizzati per le attività lavorative devono essere chiusi a chiave;

b) i documenti contenenti dati personali non possono essere lasciati sulle scrivanie, specialmente in caso di assenza, ma devono essere conservati nei cassetti delle scrivanie e negli archivi con chiusura a chiave;
c) l'accesso ai singoli archivi ove dove sono conservati dati personali dovrà essere limitato a quei dipendenti il cui accesso a tali documenti sia giustificato dallo svolgimento dell'attività lavorativa;
d) i documenti rimossi da archivi o armadi dovranno esservi nuovamente depositati non appena terminato l'uso richiesto e gli archivi o armadi dovranno essere chiusi a chiave;
e) gli strumenti di lavoro aziendali dati in dotazione devono essere correttamente custoditi come previsto dalle procedure aziendali;
f) qualsiasi apparato per l'archiviazione dei dati, incluse se autorizzate pennette USB, schede di memoria, hard disk esterni etc. quando non in uso dovranno essere riposti in cassetti o armadi chiusi a chiave;
g) non è possibile salvare sul proprio computer o dispositivo alcun documento, file o contenuto, ma questi dovranno essere salvati unicamente nei file di rete;
h) documenti che contengano informazioni riservate o dati personali di LABORATORI ANALISI SALVO S.R.L devono essere prontamente rimossi dalle stampanti e dai fax;
i) non devono essere lasciati documenti, dispositivi elettronici e strumenti di archiviazione di dati nelle sale riunioni, in luoghi al di fuori del controllo immediato del relativo utente;
j) non devono essere fatte delle foto, video o in generale non devono essere raccolte immagini di documenti, informazioni o dati personali relativi all'attività lavorativa svolta per conto del Titolare;
k) è necessario adottare un livello di attenzione elevato in modo tale da evitare che documenti, dispositivi elettronici e strumenti di archiviazione di dati siano resi visibili a soggetti non espressamente autorizzati a tal fine (ivi compresi altri colleghi) e/o lasciati incustoditi sia all'interno degli uffici che in viaggio, in luoghi pubblici o in altri luoghi accessibili al pubblico.

5.CONTRATTUALISTICA E NOMINA DI TERZI RESPONSABILI ESTERNI

Ogni qualvolta un fornitore, un agente o in generale un soggetto esterno abbia accesso a dati personali trattati dal Titolare, sarà necessario procedere alla verifica dell'idoneità di tale soggetto a trattare dati personali per conto di LABORATORI ANALISI SALVO S.R.L. in conformità con l'art. 28, GDPR. In particolare, LABORATORI ANALISI SALVO S.R.L. dovrà:

a) effettuare audit e controlli. Laddove a seguito di tali controlli risulti che il fornitore non è in grado di fornire garanzie sufficienti dal punto di vista tecnico ed organizzativo circa il trattamento dei dati personali, non sarà possibile sottoscrivere il contratto con tale fornitore. Al contrario, ove risulti che il fornitore è in grado di fornire garanzie sufficienti dal punto di vista tecnico ed organizzativo circa il trattamento dei dati personali, l'ufficio responsabile del rapporto contrattuale dovrà predisporre e stipulare un apposito accordo sul trattamento ai sensi dell'art. 28, GDPR;
b) inviare a ciascun responsabile esterno del trattamento una specifica richiesta, volta a valutare la permanenza in capo al responsabile esterno del trattamento dell'idoneità a trattare dati personali in conformità con la normativa applicabile e la correttezza del trattamento durante il periodo pregresso.

6.DATA PROTECTION OFFICER (RESPONSABILE DELLA PROTEZIONE DEI DATI)

E' la persona che, designata dal Titolare e nel rispetto di quanto previsto dal Regolamento UE 679/2016, assiste l'Organizzazione sugli obblighi derivanti dalla Normativa Privacy e collabora con il Titolare medesimo per garantire l'osservanza di quanto previsto dall'art. 39, par. 1, del GDPR. In sintesi, è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

- informare e fornire consulenza al Titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- cooperare con il Garante per la protezione dei dati personali e fungere da contatto per questioni connesse al trattamento.

7.REGISTRO DEI TRATTAMENTI

È un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal Titolare e, se nominato, dal responsabile del trattamento.

Costituisce uno dei principali elementi di *accountability* del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro deve avere forma scritta, eventualmente anche elettronica, ed essere esibito su richiesta al Garante

8.DATA BREACH REPORTING

La Privacy Policy mira a definire le modalità attraverso le quali l'Organizzazione gestisce eventuali eventi di *Data Breach* (violazione dei dati) e adempie agli obblighi di notifica della violazione dei dati all'autorità di Protezione dei Dati e alla comunicazione agli argomenti dei dati in conformità con le leggi sulla privacy.

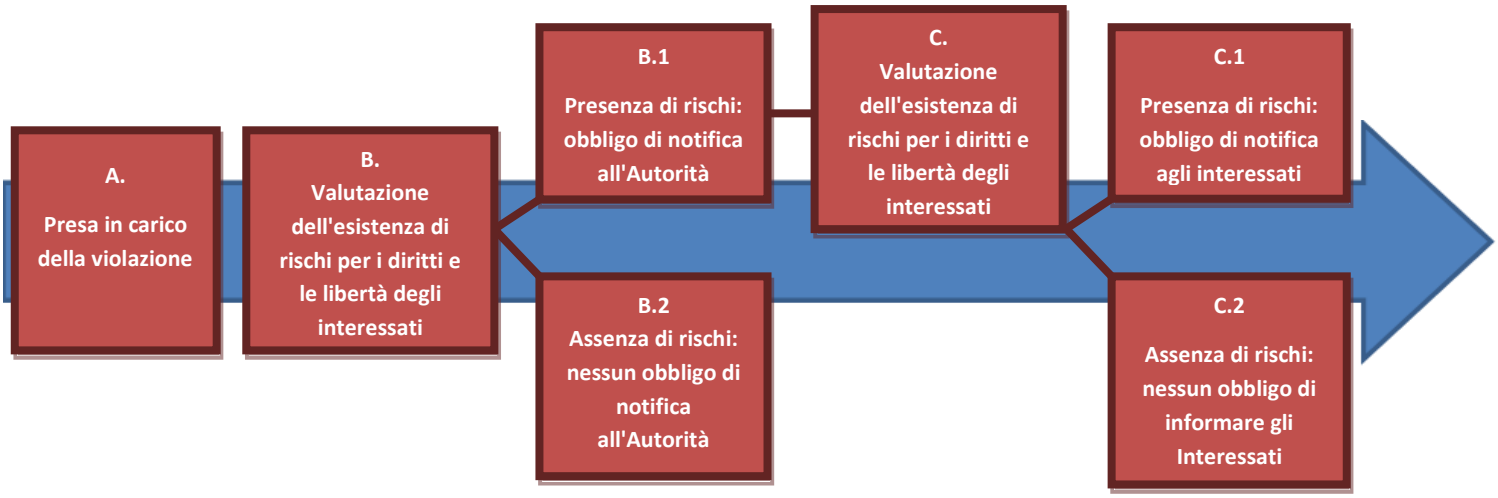
8.1.COS'È LA VIOLAZIONE DEI DATI

Il *Data Breach* può assumere diverse forme, che possono essere classificate come segue:

- **violazioni della riservatezza**: si riferiscono a casi di accesso non autorizzato o condivisione accidentale o accesso ai dati personali;
- **violazioni dell'integrità**: si riferisce ai casi in cui viene apportata una modifica non autorizzata o accidentale ai dati personali;
- **violazioni della disponibilità**: indica i casi in cui l'accesso ai dati personali viene perso o distrutto, accidentalmente o da persone non autorizzate, o in cui i dati personali vengono persi.

Anche le violazioni temporanee devono essere considerate come violazione dei dati: la mancanza di accesso ai dati personali, anche per un breve periodo, può infatti avere un impatto considerevole sui diritti e sulle libertà dei soggetti di dati.

8.2.LA GESTIONE DELLE VIOLAZIONI DEI DATI



In ogni caso, indipendentemente dal fatto che il Titolare sia tenuto o meno ad effettuare la notifica, la violazione deve essere documentata in un registro interno di violazione dei dati.

A. La presa in carico della violazione - la valutazione iniziale

Compito	Se un dipendente di una Società scopre una violazione di dati, è pregato di informare immediatamente il Titolare, compilando l'Allegato A (*Record violazione dati*). Il Titolare, previa consultazione del D.P.O. aziendale, avvia la procedura volta a valutare se la violazione è avvenuta, se deve essere considerata come violazione del dato e se ha comportato una compromissione dei dati personali: nello svolgimento dell'indagine, può chiedere la collaborazione del Consulente Legale, delle persone appartenenti all'Ufficio coinvolto o del soggetto che ha segnalato la violazione, nonché dell'Ufficio IT. In ogni caso, anche il DPO deve essere **immediatamente** informato della violazione e deve essere coinvolto durante l'intera gestione della violazione. Nei casi in cui il trattamento sia effettuato nell'ambito di un accordo di contitolarità e/o di un accordo di trattamento dei dati ai sensi dell'art. 28, GDPR, il Titotale accerta se il Data Breach grava sulla Società o sul contitolare. Qualora la Società non sia obbligata ad effettuare la verifica, Titolare segnalerà il sospetto di violazione del dato al contitolare e/o al responsabile del trattamento, collaborando con il loro secondo i termini dell'accordo concluso.
Incaricato	Il Titolare del trattamento
Attori coinvolti	Persone coinvolte nell'Ufficio, il DPO, il contitolare (se presente), il responsabile del trattamento (se presente) il Dipartimento IT, il Consulente legale
Fattore scatenante	Qualsiasi segnalazione che possa portare alla compromissione dei dati personali detenuti dall'Organizzazione
Calcolo del tempo	**Immediatamente** e comunque **entro 24 ore**

Le violazioni dei dati possono essere segnalate attraverso vari canali. Le principali fonti di segnalazione sono riassunte di seguito:

Meccanismi di allerta per garantire che i sistemi di protezione siano in grado di rilevare e registrare qualsiasi potenziale violazione dei dati

Ogni Ufficio deve informare tempestivamente il Titolare in caso di perdita di dati o di incidenti di sicurezza dei dati, o laddove vengano rilevati rischi

Segnalazione automatica

Segnalazione d'ufficio

Segnalazione di terze parti

Segnalazione del responsabile del trattamento dei dati

Secondo questa procedura, chiunque all'interno dell' Organizzazione deve informare di una presunta violazione, anche se il trattamento dei Dati Personali non fa parte dei propri doveri

Il responsabile del trattamento deve informare tempestivamente il Titolare, e in ogni caso entro 24 ore dalla scoperta, se ritiene o ha ragionevoli motivi per ritenere che sia avvenuta un'operazione illecita di trattamento o una raccolta, accesso, utilizzo, perdita, appropriazione indebita, distruzione o divulgazione illeciti di dati personali

B. La valutazione dell'esistenza di rischi per i diritti e le libertà degli interessati: notifica all'Autorità ai sensi dell'articolo 33 GDPR

Compito	Il Titolare, anche con il supporto del DPO, deve valutare se sia possibile escludere la notifica della violazione all'Autorità, in quanto è improbabile che il Data Breach presenti un rischio per i diritti e le libertà delle persone fisiche.[1] Per effettuare tale accertamento, deve valutare con l'ausilio del Consulente Legale e di ogni altra figura che ritenga opportuno coinvolgere (*es*. DPO) la gravità del Data Breach, tenendo conto del rischio per i diritti e le libertà degli interessati coinvolti. A questo proposito, tiene conto e applica: • le *raccomandazioni per una metodologia di valutazione della gravità delle violazioni dei dati personali* pubblicate dall'Agenzia dell'Unione europea per la cybersicurezza; • le *linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento 2016/679 (wp250rev.01)* emanate dal gruppo di lavoro 29; • le *linee guida 01/2021 sugli esempi di notifica di violazione* dei dati emesse dal comitato europeo per la protezione dei dati; • qualsiasi altro strumento e/o metodologia di valutazione che ritenga opportuno nella misura in cui non violi le Leggi sulla Privacy. Nel caso in cui valuti: – **la presenza di rischi:** la violazione è notificata all'Autorità Garante per la protezione dei dati personali competente (si veda la procedura di *segnalazione online* messa a disposizione dal Garante per la protezione dei dati personali) e copia dell'analisi e della notifica è conservata nell'Archivio Documentale; – **improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche**: la violazione NON è notificata all'autorità competente per la protezione dei dati, ma il responsabile della violazione deve (i) conservare nell'archivio documentale una copia dell'analisi effettuata; e (ii) completare l'allegato A da inserire nel registro delle violazioni.
Incaricato	Il Titolare del trattamento
Attori coinvolti	Il DPO, il Consulente Legale ed ogni altra figura che il Titolare ritenga opportuno coinvolgere
Fattore scatenante	Il Titolare termina la procedura di verifica preliminare.
Calcolo del tempo	Entro 48 ore dal termine della fase precedente e comunque **entro 72 ore dal momento in cui il Titolare è venuto a conoscenza del Data Breach.**[2]

Notifica all'Autorità competente. L'autorità può essere informata anche come segue[3]:

– **notifica per fasi**: l'Organizzazione comunica la valutazione preliminare sulla violazione dei dati entro il termine di 72 ore previsto dal GDPR, presentando una notifica preliminare, e condivide le successive informazioni ottenute attraverso indagini più approfondite man mano che le stesse vengono effettuate;

[1]Un Violazione dei dati può potenzialmente avere un numero di effetti negativi significativi sulle persone, inclusi danni fisici, materiali o immateriali, come perdita di controllo da parte degli interessati sui loro dati personali, limitazione dei loro diritti, discriminazione, furto o usurpazione di identità, perdita finanziaria, la decrittazione della pseudonimizzazione, il danno alla reputazione e la perdita della riservatezza dei dati personali protetti dal segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone interessate.

[2]Il momento esatto in cui si può ritenere che un responsabile del trattamento sia "a conoscenza" di una violazione dei dati dipenderà dalle circostanze della violazione dei dati stessa. In alcuni casi sarà relativamente ovvio fin dall'inizio che si è verificata una violazione dei dati, mentre in altri potrebbe essere necessario del tempo per stabilire se i dati sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sull'adozione di azioni tempestive per indagare su un incidente, per determinare se i dati personali siano stati effettivamente violati e, in tal caso, intraprendere azioni correttive e notificare se necessario.

[3]Si raccomanda di condividere con un consulente legale l'eventuale necessità di procedere con una notifica scaglionata o tardiva.

- **notifica tardiva**: l'Organizzazione notifica la violazione dopo il termine di 72 ore specificato nel GDPR. In tal caso, deve indicare i motivi del ritardo.

La notifica contiene almeno le seguenti informazioni:

a) una descrizione della natura della violazione dei dati, compresi, ove possibile, le categorie e il numero approssimativo di interessati e le categorie e il numero approssimativo di dati violati;
b) il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto presso il quale è possibile ottenere maggiori informazioni, se del caso;
c) una descrizione delle probabili conseguenze della violazione;
d) una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione e anche, se del caso, per mitigarne i possibili effetti negativi.

C. La valutazione dell'esistenza di un rischio elevato per i diritti e le libertà degli interessati: la comunicazione agli interessati ai sensi dell'articolo 34 del GDPR

Compito	Il Titolare deve valutare, con il supporto del DPO, se sia possibile escludere la comunicazione della violazione agli interessati, in quanto la violazione non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.[4] A tal fine, dovrebbe [5]effettuare la valutazione nell'ambito della precedente attività **B**, tenendo conto (non solo delle conseguenze immediate ma anche) delle cosiddette conseguenze secondarie[6] per gli interessati. Nel caso in cui: – **viene accertata** la presenza di **rischi elevati**: la violazione dei dati viene comunicata agli interessati coinvolti. I mezzi di comunicazione devono essere scelti caso per caso. Una copia di tale comunicazione è conservata dal Titolare; – **è accertata l'assenza di rischi**[7]: la violazione non viene comunicata agli interessati coinvolti. Viene conservata una copia della valutazione. In ogni caso, il Titolare (o un suo incaricato) completa l'Allegato A che viene poi inserito nel registro Data Breach dell'Organizzazione.
Incaricato	Il Titolare del trattamento
Attori coinvolti	Il DPO, il Consulente Legale ed ogni altra figura che il Titolare ritenga opportuno coinvolgere
Fattore scatenante	Il Titolare completa la procedura di verifica iniziale e determina che esiste una ragionevole probabilità che si sia verificata una violazione dei dati personali
Calcolo del tempo	Al termine della fase di valutazione iniziale della violazione: l'accertamento e l'eventuale comunicazione della violazione agli interessati devono essere effettuati senza ingiustificato ritardo (più lungo è il ritardo, maggiore è il rischio di responsabilità per danni)

La comunicazione contiene almeno le seguenti informazioni:

[4] Con ciò si intende, in generale, il rischio di danni fisici, materiali o immateriali alle persone i cui dati sono violati (ad es., discriminazione, furto di identità, danni alla reputazione, perdita finanziaria, perdita di riservatezza dei dati personali protetti dal segreto professionale, pseudonimizzazione non autorizzata, ecc).

[5] Nel valutare il rischio per gli individui derivante da una violazione dei dati, il titolare del trattamento dovrebbe considerare le circostanze specifiche della violazione, inclusa la gravità del potenziale impatto e la probabilità che tale impatto si verifichi. La valutazione tiene conto dei seguenti criteri:

- Tipo di valutazione
- Natura, sensibilità e volume dei dati personali
- Facile identificazione degli interessati
- Gravità delle conseguenze per gli individui
- Caratteristiche particolari degli interessati
- Caratteristiche peculiari del Titolare del trattamento
- Numero di interessati coinvolti
- Aspetti generali delle attività di trattamento

[6] Ad esempio, l'accesso non autorizzato a un sito web aziendale, tramite il quale vengono rubati nomi, credenziali, Mi piace e Non mi piace degli utenti, non sembra essere uno dei casi che devono essere comunicati agli interessati, in quanto le conseguenze dannose sembrano molto limitate. Tuttavia, se si considera che spesso vengono utilizzate password identiche per più servizi, è possibile che gli utenti le utilizzino anche per accedere all'home banking o al proprio Fascicolo sanitario elettronico. Le conseguenze cosiddette secondarie, quindi, possono essere molto gravi, anche se le conseguenze immediate non sono molto significative, e la notifica del Data Breach può consigliare agli Interessati di modificare immediatamente gli accessi agli altri utenti di cui dispongono e per cui sono state utilizzate le medesime credenziali (l'esempio è tratto - ed è stato liberamente interpretato - dal Parere 3/2014 sulla Notifica di violazione dei dati personali, pubblicato il 25 marzo 2014 dal Gruppo di lavoro Articolo 29 per la protezione dei dati).

[7] Si prega di notare che in uno qualsiasi dei seguenti casi, la notifica all'interessato non è richiesta ma il Titolare deve documentare se (i) ha posto in essere adeguate misure di protezione tecniche e organizzative e tali misure sono state applicate all'interessato dei dati personali soggetti a violazione - come quelli per rendere i dati personali incomprensibili a persone non autorizzate, come la crittografia; (ii) ha adottato misure per prevenire il verificarsi di un rischio elevato per i diritti e le libertà degli interessati; o (iii) la divulgazione della violazione dei dati richiederebbe sforzi sproporzionati e, pertanto, viene effettuata una divulgazione pubblica o una misura simile.

a) il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto presso il quale è possibile ottenere maggiori informazioni;
b) una descrizione delle probabili conseguenze della violazione dei dati;
c) una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati e anche, se del caso, per mitigarne i possibili effetti negativi.

In linea di principio, la violazione dei dati dovrebbe essere comunicata direttamente agli interessat, a meno che ciò non richieda uno sforzo sproporzionato per l'Organizzazione[8].

Quando si comunica una violazione dei dati agli interessati, devono essere utilizzati messaggi dedicati (ovvero non inviati insieme ad altre informazioni, come aggiornamenti regolari, newsletter o messaggi standard), assicurando che la comunicazione sia accessibile in formati alternativi appropriati e nelle lingue pertinenti. A tal fine, il Titolare potrebbe utilizzare, ad esempio, i seguenti mezzi:

- messaggistica diretta (ad es. e-mail, SMS, messaggio diretto);
- banner o notifiche sui siti web della Società, comunicazioni postali e pubblicazioni di stampa pertinenti.

Allegato A - Record violazione dati

Indipendentemente dal fatto che una violazione debba essere notificata o meno all'autorità competente in materia di protezione dei dati, il Titolare del trattamento deve registrare l'evento in un registro dedicato, indicando le sue circostanze, le sue conseguenze e le misure adottate per porvi rimedio.

Incidente n. [●]	
Data, ora e luogo della violazione dei dati	
Data in cui il Titolare è venuto a conoscenza della violazione	
Mezzi con cui il Titolare è venuto a conoscenza della violazione	
Natura della violazione (perdita di riservatezza, perdita di integrità, perdita di disponibilità)	
Descrizione della violazione	
Causa della violazione	
Categorie di interessati (o altri stakeholder) coinvolti	
Numero di interessati (o altri stakeholder) coinvolti	
Categorie di dati personali coinvolte	
Descrizione dei sistemi e delle infrastrutture IT coinvolti nella violazione, compresa la loro ubicazione	
Nome e dati di contatto del fornitore esterno o di altre organizzazioni coinvolte (se presente, ad es. fornitore IT esterno)	
Conseguenze della violazione	
Misure tecniche e organizzative adottate come bonifica	
Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire violazioni analoghe in futuro	
Indicazione del coinvolgimento degli interessati (o di altri stakeholder) di altri Paesi (specificare i Paesi)	
Indicazione di qualsiasi notifica effettuata ad autorità estere per la protezione dei dati	
Decisione sulla notifica della violazione dei dati e motivazioni (se del caso, specificare la data e allegare una copia del modulo di notifica a questo registro)	
Indicazione di eventuali ritardi nella notifica e motivi di stasi (se applicabile)	

[8] In tal caso, sarà adottato un avviso pubblico o misura analoga per informare gli interessati con identica efficacia.