STUDIO ASSOCIATO PAGANI

CONSULENZA DEL LAVORO LEGALE E GESTIONALE
HR • LABOUR CONSULTANCY • LEGAL

DOTT. SABRINA PAGANI - PARTNER

AVV. ROBERTO RESPINTI - PARTNER

Procedura

Gestione della violazione di dati personali

(Data Breach) come Responsabile del trattamento

Autore	Studio Associato Pagani
Sintesi	La presente Procedura stabilisce gli adempimenti da porre in essere nel caso in cui si verifichi una violazione di dati personali nell'ambito delle operazioni di trattamento effettuate dallo Studio Associato Pagani in qualità di Responsabile del trattamento nominato da ciascun cliente ai sensi dell'art. 28 del Regolamento UE n. 679/2016
Stato	Vigente
Contatti	privacy@studiopagani.com

Classificazione e Controllo del Documento

Questo documento è classificato come riservato

Prima dello smaltimento, conservare per ulteriori 3 anni da quando il modello / documento / record diventa obsoleto.

Per le modifiche a questo documento o registrazione, contattare il proprietario del documento.

Effective Date	Version	Description	Author	Approver (role)
25/05/2018	V1.0	Prima versione	Studio Associato Pagani	Sabrina Pagani Roberto Respinti
06/10/2020	V2.0	Fine Tuning	Studio Associato Pagani	Sabrina Pagani Roberto Respinti

VIALE TUNISIA 27 - 20124 MILANO - TEL. 02 29003782 - FAX 02 6592245
E-MAIL: consulenza@studiopagani.com - www.studiopagani.com Pec: s.pagani@consulentidellavoropec.it
C.F. - P.I.: 06247610964

Sommario

1.0 Definizioni

«Archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

«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.

«Trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Ai fini della presente Procedura per Trattamento si intendono le operazioni di cui sopra poste in essere dallo Studio, attraverso propri dipendenti e collaboratori, in nome e per conto di ciascun cliente.

«Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri. Ai fini della presente Procedura per Titolare del trattamento si intende il cliente per conto del quale lo Studio tratta dati personali e categorie particolari di dati personali dei relativi dipendenti e altri collaboratori.

«Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. Ai fini della presente Procedura per Responsabile del trattamento si intende lo Studio.

«Violazione dei dati personali»: la 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.

«interessato»: si considerano interessati tutti i soggetti identificati o identificabili i cui dati personali sono trattati dallo Studio nell'ambito delle attività oggetto del contratto stipulato con ciascun cliente. Ai fini della presente Procedura per Interessati si intendono i dipendenti e altri collaboratori dei clienti Titolari del trattamento i cui dati personali e categorie particolari di dati personali vengono trattati dallo Studio in qualità di Responsabile del trattamento.

2.0 Introduzione

Studio Associato Pagani (in seguito, lo "Studio") è stato nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) n. 679 del 27 aprile 2016 (in seguito il "Regolamento Privacy") da ciascun cliente (in seguito il "Cliente" o il "Titolare del trattamento") per compiere tutte le operazioni di trattamento necessarie a dare esecuzione al contratto con gli stessi stipulato (in seguito il "Contratto"). A tal fine, lo Studio è autorizzato a trattare, in nome e per conto di ciascun Cliente, i dati personali ed anche eventualmente le categorie particolari di dati personali e i dati giudiziari dei rispettivi dipendenti e altri collaboratori il cui trattamento sia necessario nell'esecuzione del Contratto.

Lo Studio è responsabile, sia nei confronti degli interessati che nei confronti del Cliente, della protezione delle informazioni e dei dati personali oggetto delle operazioni di trattamento di cui sopra e, ai sensi del Regolamento Privacy, è tenuto a garantire la sicurezza e la confidenzialità dei dati personali trattati.

Il Regolamento Privacy prevede che, al fine di mantenere la sicurezza e prevenire trattamenti in violazione al Regolamento Privacy, il Titolare del trattamento valuti i rischi inerenti al trattamento effettuato per suo conto e attui misure organizzative e tecniche idonee a limitare tali rischi e ad assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi presenti nei trattamenti e alla natura dei dati personali da proteggere.

In particolare il Titolare del trattamento è tenuto a rispettare i seguenti principi:

- La ***privacy by design*** la quale richiede che il Titolare, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, adotti misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati;
- La ***privacy by default*** la quale presuppone che il Titolare metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità di trattamento.

Tra i rischi presentati dal Trattamento il Regolamento Privacy individua la "violazione dei dati personali", intesa come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Una violazione dei dati personali, se non affrontata in modo adeguato e tempestivo, può infatti provocare danni alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il Regolamento Privacy prevede inoltre che in caso di violazione dei dati personali, il Titolare del trattamento sia tenuto a notificare la violazione all'autorità di controllo competente e, quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, anche all'interessato senza ingiustificato ritardo.

Lo Studio, in qualità di Responsabile del trattamento, ai sensi del Regolamento Privacy, dopo essere venuto a conoscenza della violazione, è tenuto ad informare senza ingiustificato ritardo il Titolare del trattamento affinché lo stesso possa procedere alle comunicazioni di cui sopra.

Lo Studio presta la massima cura e attenzione al tema della tutela dei diritti e delle libertà delle persone fisiche e della protezione dei dati che tratta in nome e per conto del Titolare del trattamento e, a tal fine, attua le misure tecniche e organizzative necessarie ad assicurare l'attuazione del Regolamento Privacy e delle istruzioni impartite dal Titolare del trattamento.

In particolare lo Studio pone in essere le misure appropriate e specifiche al fine di evitare la violazione dei dati personali ed in particolare il rischio di perdita dei dati o di accesso dei dati a soggetti non autorizzati.

Nonostante ciò, nella eventualità che una violazione dei dati personali si verifichi nell'ambito dei Trattamenti effettuati dallo Studio in nome e per conto del Cliente, è fondamentale attuare il prima possibile un idoneo piano di gestione delle violazioni al fine di ridurre al minimo qualsiasi rischio relativo alla violazione occorsa.

Pertanto, con la presente procedura lo Studio intende predisporre un piano di gestione delle violazioni di dati personali al fine di ottemperare alle previsioni del Regolamento Privacy.

3.0 Scopo

Lo scopo della presente Procedura è di assicurare all'interno dello Studio:

- ⇨ la gestione controllata e strutturata degli incidenti nel caso in cui si verifichi una violazione di dati personali oggetto di trattamento;
- ⇨ che l'eventuale violazione di dati personali nell'ambito del trattamento effettuato dallo Studio venga affrontata secondo un processo di gestione della violazione idoneo ad assicurare che le azioni di risposta alla stessa siano attuate con velocità e efficacia, in maniera uniforme all'interno dello Studio, al fine di evitare/limitare il danno eventualmente verificatosi e di ridurre al minimo la possibilità di un nuovo incidente;
- ⇨ che il Titolare del trattamento sia messo nelle condizioni di poter adempiere agli obblighi posti a suo carico dal Regolamento Privacy di cui al paragrafo che precede.

4.0 Ambito di applicazione

La presente Procedura si applica con riferimento a tutte le informazioni e dati che lo Studio tratta in qualità di Responsabile del trattamento.

La presente Procedura si applica a tutti i dipendenti, i collaboratori, i consulenti, i fornitori, i Partner e i soggetti facenti parte del vertice dello Studio, nonché a qualunque altro soggetto che sia incaricato del trattamento di dati personali per conto dello Studio (in seguito i "**Destinatari**").

Nel caso in cui uno dei soggetti sopra elencati ponga in essere azioni in violazione del Regolamento Privacy, di altra normativa privacy applicabile o delle istruzioni impartite da ciascun Cliente attraverso il contratto di nomina dello Studio a Responsabile del trattamento (in seguito l'"**Accordo**"), lo Studio potrebbe essere soggetto a significative sanzioni contrattuali, penali o amministrative, anche pecuniarie, nonché incorrere in rilevanti danni reputazionali e di immagine.

Pertanto, 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 dipendenti e collaboratori inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

5.0 Attuazione e piano di revisione

La presente Procedura è immediatamente efficace e in vigore alla data della sua approvazione e tutti i responsabili dovranno assicurare che i dipendenti e collaboratori sottoposti alla loro supervisione e controllo siano a conoscenza dei contenuti previsti dalla stessa e delle azioni da intraprendere in caso di violazione di dati personali.

La presente Procedura potrà essere oggetto di aggiornamenti o revisioni in seguito a:

(i) eventi di violazione di dati personali;

(ii) modifiche organizzative interne allo Studio;

(iii) pianificazione di nuove operazioni di trattamento che presentano rischi diversi o ulteriori;

(iv) modifiche legislative;

(v) pubblicazioni di decisioni giudiziarie;

(vi) emissioni di nuovi pareri o linee guida da parte delle autorità competenti.

Lo Studio si impegna in ogni caso a effettuare una revisione annuale della presente Procedura al fine di verificare che siano soddisfatti gli obiettivi perseguiti dalla stessa.

I Destinatari, ai fini della gestione della violazione di dati personali che si possa verificare all'interno dello Studio, devono sempre tener conto, oltre che della presente Procedura, altresì delle diverse disposizioni date dal Titolare del trattamento con l'Accordo che sono reperibili cliccando sul seguente link: \\srv-app\privacy\04 Soggetti Terzi (nomine da parte dei Clienti)\Clienti - SAP nomina a Responsabile Esterno\SAP\Documenti inviati. Analogo link è reperibile accedendo a: *Studios (\\srv-app) (G:)*.

Per qualsiasi domanda o chiarimento in merito alle disposizioni di cui alla presente Procedura e alle disposizioni impartite da ciascun Titolare del trattamento, i Destinatari potranno rivolgersi alla dott.ssa Sabrina Pagani e all'avv. Roberto Respinti, ovvero ai referenti dagli stessi, tempo per tempo, designati.

6.0 Normativa di riferimento

Lo Studio è tenuto a rispettare le normative, i provvedimenti giudiziari, i pareri e le linee guida in tema di protezione di dati personali vigenti in Italia e in Unione Europea, nonché negli eventuali Paesi Terzi in cui lo Studio compia operazioni di trattamento, tra cui:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 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;
- Decreto legislativo 30 giugno 2003, n. 196 così come da ultimo modificato dal Decreto legislativo n. 101 del 2018 (in seguito il "**Codice Privacy**");
- Linee guida e provvedimenti del Garante per la Protezione dei Dati Personali;
- Pareri del Working Party Article 29 tra cui "*Guidelines on Personal data breach notification under Regulation 2016/679*" - Ottobre 2017.

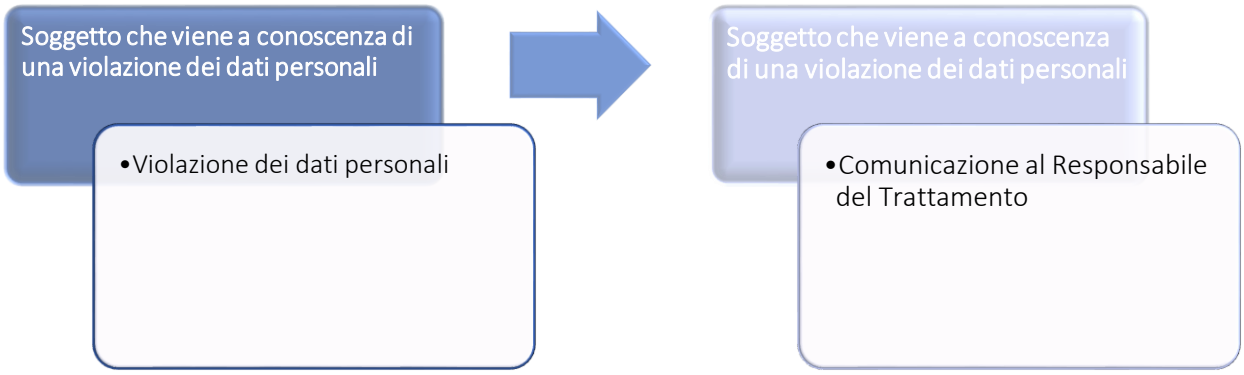
7.0 Tipologie di incidenti relativi alla sicurezza dei dati

La presente Procedura disciplina la gestione e la comunicazione di incidenti relativi alla sicurezza dei dati che possono causare la violazione di dati personali; tra i possibili incidenti si ricordano a titolo esemplificativo:

- ⇨ *perdita o furto di strumenti IT (pc, smartphone, chiavette USB, hardware);*
- ⇨ *rivelazione di informazioni a soggetti non autorizzati;*
- ⇨ *accesso non autorizzato ai dati personali;*
- ⇨ *violazione delle misure di sicurezza fisiche dei locali dove i dati personali sono archiviati;*
- ⇨ *caricamento/divulgazione per errore di dati personali in rete;*
- ⇨ *errore umano (per esempio: perdita di dati personali archiviati presso luoghi non sicuri);*
- ⇨ *mancata previsione di eventi di rischio per la sicurezza dei dati quali allagamenti o incendi;*
- ⇨ *attacco esterno ai sistemi IT aziendali;*
- ⇨ *reati informatici.*

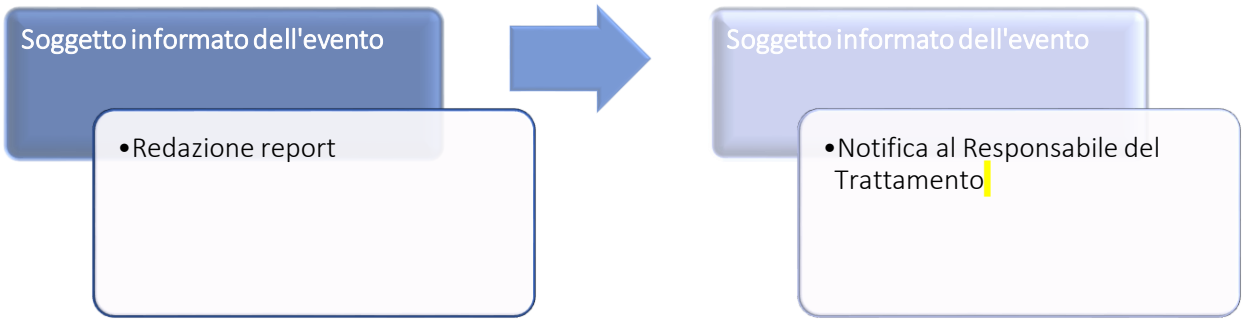
8.0 Piano di gestione della violazione dei dati

1) <u>Scoperta o sospetta violazione dei dati</u>



Il soggetto che viene a conoscenza di una violazione dei dati personali, anche solo sospetta e non ancora accertata, deve informare **immediatamente** il Responsabile ai seguenti contatti: dott.ssa Sabrina Pagani e avv. Roberto Respinti, ovvero i referenti dagli stessi, tempo per tempo, designati.

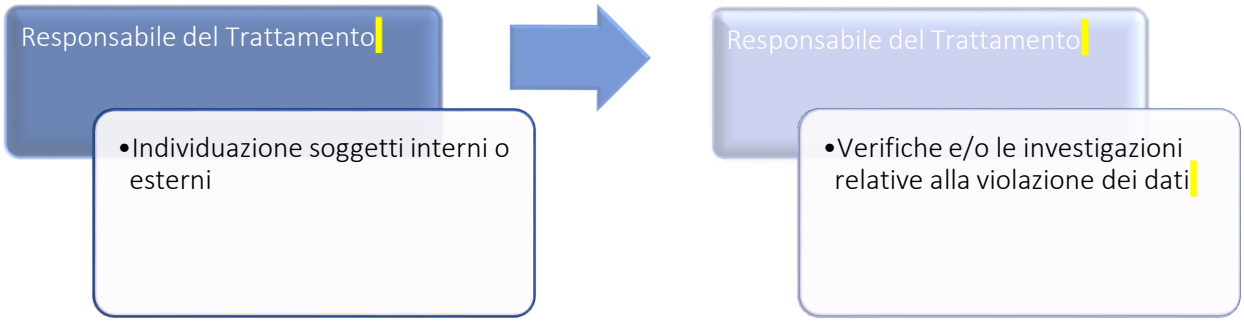
2) <u>Report interno della violazione</u>



Il Responsabile del Trattamento, che viene così informato dell'evento di violazione dei dati deve quindi, se possibile **entro 24 ore** dalla notifica ricevuta, redigere un report interno relativo all'evento accaduto eventualmente supportato dal Responsabile IT se la violazione coinvolge sistemi IT. Il report interno deve contenere i dettagli noti della violazione:

- data e ora;
- soggetti dello Studio coinvolti;
- descrizione dell'incidente;
- dati personali apparentemente violati;
- sistemi IT/archivi/database coinvolti;
- azione eventualmente intraprese per mitigare gli effetti della violazione.

3) <u>Valutazione del rischio per i diritti e le libertà delle persone</u>



Il Responsabile del Trattamento sulla base delle circostanze concrete della violazione verificatasi o sospettata e del potenziale rischio per i diritti e le libertà degli interessati, se necessario individuerà tempestivamente i soggetti, interni o esterni allo Studio, dotati delle necessarie competenze al fine di eseguire le verifiche e/o le investigazioni relative alla violazione dei dati e valutare gli eventuali danni provocati dalla stessa.

I Destinatari non devono mai condurre personalmente verifiche o investigazioni al fine di non distruggere le prove eventualmente esistenti, salvo che siano stati formalmente incaricati di tali compiti.

Le verifiche poste in essere devono valutare se la violazione dei dati abbia comportato o meno un rischio per i diritti e le libertà delle persone fisiche, il quale è da considerarsi sicuramente presente laddove la violazione possa causare danni materiali o immateriali alle persone fisiche, tra cui a titolo esemplificativo: perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Nel valutare il rischio, è necessario tenere in considerazione i seguenti fattori: il tipo di violazione, la natura, la gravità, il volume di dati personali, la facilità di identificazione degli interessati, le caratteristiche particolari degli interessati o del titolare, oltre che il numero di persone interessati coinvolti.

Tali verifiche devono essere svolte e, se possibile, concluse **entro 24 ore** dal momento in cui il Responsabile del Trattamento ha ricevuto la notifica da parte del soggetto che ha assistito al verificarsi dell'incidente relativo alla sicurezza e che ha causato la violazione dei dati.

4) Esito valutazione

a) Valutazione del rischio: esito negativo ➔ chiusura report interno

Qualora all'esito di tali valutazioni, la violazione dei dati personali non presenta un rischio per i diritti e le libertà delle persone fisiche, il Responsabile:

i. integra il report interno con le risultanze delle verifiche e della valutazione del rischio effettuate sotto il suo controllo, specificando i criteri adottati per il giudizio di probabilità del rischio e descrivendo le ulteriori azioni poste in essere per mitigare gli effetti della violazione;

ii. annota nel registro interno delle violazioni (si veda paragrafo 9.0 che segue) tutti i dettagli della violazione oggetto di valutazione del rischio.

b) Valutazione del rischio: esito positivo ➔ Comunicazione al Titolare del trattamento

Qualora invece all'esito di tali verifiche e valutazioni risulti probabile che la violazione dei dati personali presenti un rischio o un elevato rischio per i diritti e le libertà delle persone fisiche, ove possibile, entro 24 ore dalla chiusura delle verifiche e valutazioni in merito alla violazione dei dati verificatasi e dalla redazione del relativo report interno, il Responsabile comunica la avvenuta violazione al Titolare del trattamento tramite apposito modulo allegato alla presente Procedura (All. 1 – Modulo di comunicazione della violazione al Titolare del trattamento).

La comunicazione della violazione dei dati personali al Titolare del trattamento deve contenere almeno i seguenti dati:

a) una 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 oggetto di violazione (quali, ad esempio, archivi di dati relativi alla salute o contenenti dati relativi a conti correnti bancari);

b) il nome ed il contatto dei Titolari dello Studio, ovvero dei referenti dagli stessi, tempo per tempo designati, cui gli interessati possano rivolgersi per avere maggiori informazioni;

c) una descrizione delle misure di sicurezza già implementate o che lo Studio propone di implementare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire tutte le informazioni richieste nel Modulo contestualmente, il Responsabile potrà fornire inizialmente sommarie informazioni in relazione alla violazione verificatasi, purché ciò avvenga immediatamente dopo l'avvenuta conoscenza della stessa, integrando poi la comunicazione in un momento successivo. Tali sommarie informazioni devono in ogni caso consentire al Titolare del trattamento di effettuare una prima valutazione dell'entità della violazione per procedere con la comunicazione della stessa al Garante per la protezione dei dati personali entro 72 ore dal momento in cui viene a conoscenza della violazione stessa (e, in caso di rischio elevato per i diritti e le libertà degli interessati, altresì per procedere alla comunicazione all'interessato cui la violazione di dati personali si riferisce). Ulteriori dettagli potrebbero essere richiesti dal Titolare del trattamento nel corso di un'eventuale attività istruttoria avviata nei suoi confronti dal Garante per la protezione dei dati personali.

9.0 Accountability e tenuta del registro delle violazioni

Lo Studio deve documentare tutte le violazioni verificatesi o anche solo sospettate nell'ambito delle attività svolte come Responsabile del trattamento in nome e per conto di ciascun Cliente, indipendentemente dal fatto che esse siano state comunicate o meno al Titolare del trattamento, al fine di poter dimostrare che il trattamento dei dati è effettuato conformemente alla normativa privacy applicabile.

A tal fine lo Studio deve tenere un registro interno delle violazioni (All. 2 – Modello di registro delle violazioni) in cui vengano di volta in volta registrati tutti i dati, le informazioni e le circostanze riguardanti le violazioni di dati personali, anche solo sospette, verificatesi nell'ambito dei trattamenti effettuati dallo Studio come Responsabile del trattamento (tra cui, ad esempio, le sue cause, le circostanze dell'incidente e quali dati personali siano stati compromessi, le conseguenze della violazione e le contromisure adottate dal titolare del trattamento). Lo Studio attua le misure di sicurezza tecnologiche e organizzative al fine di garantire la protezione dei dati contenuti nel Registro (es. che il registro sia accessibile solo da personale preventivamente autorizzato, dotato di accesso riservato e protetto tramite credenziali riservate etc.).