Introduzione

Il presente documento di Privacy Policy, aggiornato con il Regolamento UE (GDPR) 2016/679 armonizzato dal Decreto 101/2018 relativo al trattamento dei dati personali, regola le modalità di trattamento dei dati raccolti dallo Studio di Ingegneria Associato Ferrari & Pacini.
L'esigenza nasce poichè i dati trattati dall'Studio nell'esercizio delle sue funzioni, in particolare per quanto attiene al rapporto con i dipendenti, i committenti e fornitori possono essere di tipo sensibile. Essi difatti possono riguardare:
- la salute;
- dati giudiziari;
- situazione familiare;
- dati di minori;
- dati dei dipendenti.

Il trattamento dei dati dei clienti e dei committenti è intimamente connesso al rapporto di fiducia e al rispetto degli obblighi deontologici tra cui il segreto professionale.
La divulgazione, anche accidentale di tali dati trattati potrebbe ledere i diritti e la libertà delle persone coinvolte: Studio di Ingegneria Associato Ferrari & Pacini dovrà avere una cura particolare nel proteggerli, conformandosi alla nuova normativa che regola la materia.
La protezione dei dati personali, oltre ad essere essenziale, rappresenta un fattore di trasparenza e confidenzialità nel rapporto.
Non meno importanti sono i dati che lo Studio deve trattare nella gestione del proprio rapporto con i dipedenti dello Studio.
Al fine di evitare i pericoli connessi alla gestione di tutti i dati trattati, lo Studio di Ingegneria Associato Ferrari & Pacini presta particolare attenzione a che:

· Le finalità di trattamento dei dati e la loro trasmissione siano chiaramente definite;
· Le misure di sicurezza informatica e fisica siano precisamente individuate, definite e attuate;
· Le persone coinvolte (segreteria, dipendenti, praticanti, colleghi e collaboratori a qualsiasi titolo) siano adeguatamente informate e coinvolte nel processo di protezione dei dati personali.

"Lo studio" ha inoltre tenuto presente del progresso tecnologico nel rispetto degli obblighi deontologici e normative.
In tutte le ipotesi in cui lo studio ha esternalizzato a terzi alcuni servizi (ad esempio la gestione dello stipendio dei dipendenti) ha prestato la massima attenzione a che i soggetti coinvolti trattino i dati in modo sicuro e nel rispetto delle norme (vedesi Addendum all.3).
Secondo il principio della responsabilizzazione (accountability) "lo Studio" ha conformato tutte le misure adottate dalla propria organizzazione alla nuova normativa sulla privacy.

PARTE PRIMA

1. I Principi del GDPR

Il regolamento riafferma principi fondamentali già in vigore con la precedente legislazione e ne aggiunge di nuovi. I principi confermati sono:
-la finalità del trattamento: ne limita l'utilizzo ai soli fini degli obiettivi di tutela, consulenza e prestazioni professionali da parte dello Studio di Ingegneria Associato Ferrari & Pacini (titolare del trattamento);
- **la necessità e proporzionalità:** il trattamento deve essere adeguato, pertinente e necessario allo scopo;
- **la durata limitata:** il trattamento non può protrarsi oltre il tempo necessario per l'espletamento degli incarichi, compresi gli obblighi legali di conservazione.
- **la sicurezza e riservatezza:** lo Studio è tenuto, anche per obblighi deontologici e, nel rispetto del segreto professionale, ad approntare un adeguato livello di sicurezza per i dati degli assistiti. Studio di Ingegneria Associato Ferrari & Pacini nella sua qualità di titolare del trattamento deve prevedere tutte le misure necessarie per garantire la confidenzialità, integrità e disponibilità dei dati

personali. I dati non possono essere consultati da persone non abilitate ed espressamente istruite e autorizzate ad accedervi, sia che si tratti di soggetti interni all'organizzazione dello Studio (addetti alla segreteria, dipendenti, colleghi di studio) o esterni allo stesso (consulenti tecnici, commercialisti etc).
- **il rispetto del diritto delle persone.**

I nuovi principi invece sono:
-**Il principio di accountability**, (o principio di responsabilizzazione);
-**La minimizzazione dei dati**;
-**Il diritto all'oblio**;
- **Il diritto alla portabilità dei dati**;
- **La notificazione dei data breach al Garante e, in talune ipotesi, agli interessati**.

2. Accountalility

Non sono più previste le c.d. misure minime, ma è posta in capo al titolare del trattamento (lo Studio), la responsabilità (accountability) di definire, dopo una attenta analisi, le misure adeguate al fine di garantire il rispetto delle norme del GDPR.
Accountabiliy (Responsabilizzazione) significa, sostanzialmente, che le misure dovranno essere adeguate alla struttura del singolo titolare ed elaborate, caso per caso, ricorrendo ad una preventiva mappatura dei dati trattati, della mole degli stessi, dei rischi di trattamento dei dati gestiti.
Accountability, inoltre, significa anche essere in grado di "rendere conto" delle attività poste in essere nel rispetto dei principi del GDPR.
Lo Studio di Ingegneria Associato Ferrari & Pacini, pertanto, garantisce la conformità al Regolamento dei trattamenti eseguiti. Lo Studio deve adottare criteri e procedure di trattamento certi e una formazione adeguata allo studio.

3. Minimizzazione dei dati

E' il principio secondo il quale i dati personali da trattare per ogni singola attività debbano essere soltanto quelli necessari per il raggiungimento dello scopo.
Lo Studio deve:
-interrogarsi sulla necessità di trattare dati personali per raggiungere le finalità richieste dal trattamento;
-limitare al minimo il ricorso al trattamento dei dati personali per quanto attiene:
a) le categorie di dati trattati;
b) il volume
e deve sapere se sono o meno necessari al trattamento.

Lo Studio deve trattare , per quanto possibile, solo i dati essenziali, necessari e pertinenti per compiere la prestazione richiesta dal cliente.

4. Diritto alla cancellazione – diritto all'oblio

L'art. 17 del GDPR prevede il diritto dell'interessato di ottenere dal titolare del trattamento, lo Studio, la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo da parte del titolare.
L'interessato ha il diritto di chiedere, tramite ritiro del consenso, che siano cancellati e non più sottoposti a trattamento i propri dati personali non più necessari alle finalità per le quali sono stati raccolti o altrimenti trattati.

Per lo Studio il diritto all'oblio non può essere esercitato sino quando non sarà maturato il termine di prescrizione dell'azione per la responsabilità professionale. L'esercizio del diritto cede il passo di fronte all'adempimento di alcuni obblighi di archiviazione dei dati per periodi specifici e risulta non utilmente esercitabile ove comprometta l'adempimento ad obblighi fiscali o si ponga in

contrasto necessità archivistiche di pubblico interesse ove il mantenimento del dato sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.

5. La valutazione d'impatto

Secondo l'art. 35 del GDPR, quando sia probabile che un tipo di trattamento possa creare un elevato rischio per i diritti e le libertà delle persone fisiche, ivi compreso il trattamento su larga scala di dati particolari, il titolare del trattamento debba effettuare una preliminare valutazione d'impatto (DPIA). Ad onta di ciò, tuttavia, la valutazione di impatto è comunque necessaria laddove vengano soddisfatti almeno due dei nove dei criteri indicati:

- valutazione-punteggio;
- decisione automatica con effetto legale o simili;
- monitoraggio sistematico;
- raccolta di dati sensibili;
- collezione dati personali su larga scala;
- riferimenti incrociati di dati;
- persone vulnerabili;
- uso innovativo;
- esclusione del beneficio di un diritto-contratto.

Maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare
del trattamento ha previsto di adottare. Le valutazioni d'impatto consentono
ai titolari ed ai responsabili del trattamento di identificare e trattare rischi che non sarebbero stati altrimenti rilevati e per prevenire violazioni che diversamente si sarebbero verificate.
Attraverso questo strumento lo Studio prende coscienza nel trattare dati personali e sensibili del cliente, e provvede per essi l'adozione di misure di sicurezza adeguate.

6. La portabilità dei dati

Il diritto alla portabilità attribuisce agli interessati la facoltà di esigere dal titolare del trattamento la trasmissione dei loro dati ad un altro titolare, senza che il primo si possa opporre.
L'art. 20 del GDPR attribuisce all'interessato il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e di trasmettere tali dati a un altro titolare del trattamento senza impedimenti qualora:
a) il trattamento si basi sul consenso o su un contratto;
b) il trattamento sia effettuato con mezzi automatizzati.

Ciò significa che lo Studio che tratta i dati dei clienti con mezzi automatizzati (per esempio, adottando un gestionale informatico o anche solo tenendo uno schedario sotto forma di foglio di calcolo) è tenuto a comunicare i dati del suo cliente al collega.

Pertanto, se cliente richiede la trasmissione dei suoi dati ad un collega, lo Studio dovrà trasferirli in formato strutturato comunemente usato e leggibile da una macchina.

Peraltro, il diritto alla portabilità non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Secondo il nuovo GDPR il diritto alla portabilità si applica **solo se il trattamento è effettuato con l'aiuto di procedure automatizzate, e pertanto non è esteso ai fascicoli cartacei,** che rimangono dunque esclusi dal diritto alla portabilità.

Deve però essere ricordato che, lo Studio non ha diritto a trattenere i dati se non il tempo necessario alla tutela dei propri diritti.

7. L’informativa al trattamento

L'art. 13, paragrafo 1, del GDPR impone allo Studio che acquisisce i dati degli assistiti di fornire le seguenti informazioni:

1. l'identità e i dati di contatto del titolare dello studio e, ove applicabile, del suo rappresentante all’estero;
2. i dati di contatto del responsabile della protezione dei dati (ove applicabile);
3. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
4. le categorie di dati personali in questione;
5. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
6. l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale (ove applicabile) e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

Il titolare del trattamento dovrà anche fornire all'interessato ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

1. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
2. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
3. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
4. il diritto di proporre reclamo a un'autorità di controllo;
5. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
6. l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'art. 14 enumera poi le informazioni da comunicare nell'ipotesi in cui i dati non siano stati ottenuti presso l'interessato. La persona deve essere informata degli elementi previsti dall'art. 13, ma allo stesso modo anche di quali dati personali e le modalità con le quali sono state raccolte. .

Gli Studi di consulenza che agiscono quali titolari dei dati sono liberi di determinare i mezzi occorrenti per assicurare l'informativa alle persone.

Tutte le persone hanno diritto di opporsi al trattamento dei dati per motivi legittimi, a meno che il trattamento non presenti un carattere obbligatorio.

Contenuto dell’informativa.

Alla luce dell’art. 13 del Regolamento, gli interessati al trattamento da parte dello Studio saranno informati su:

• L'identità e i dettagli di contatto del titolare del trattamento);
• i dettagli di contatto del responsabile o dei responsabili della protezione dei dati, qualora nominati;
• Le finalità del trattamento
• La base giuridica del trattamento (prestazione contrattuale o precontrattuale su richiesta del cliente);

• interesse legittimo del titolare se costituisce la base giuridica del trattamento ex art. 6. Comma 1 lettera f;
• destinatari di dati (subappaltatori, tecnici, ecc.);
• flussi transfrontalieri;
• la durata di conservazione;
• i diritti che gli interessati possono esercitare;
• le condizioni e le modalità per l'esercizio dei diritti degli interessati;
• il diritto di revocare il consenso, se questo è la base giuridica del trattamento;
• il diritto di presentare un reclamo all'autorità di controllo;
• le informazioni sulla natura normativa o contrattuale del trattamento quando si tratta della base giuridica del trattamento.

Come va resa l'informativa.

Alla luce del considerando n. 58 e dei chiarimenti resi al riguardo dal Garante, l'informativa deve avere forma concisa, trasparente, comprensibile per l'interessato e facilmente accessibile (vedi all.1).

Essa dev'essere scritta in un linguaggio chiaro e semplice ma può essere resa anche in formato elettronico (ad esempio, se destinate al pubblico, attraverso un sito web) o comunicata via email (ad esempio, in occasione della trasmissione di una nota di onorario in particolare per regolarizzare la situazione con i clienti che non sono stati adeguatamente informati).

L''informativa sul trattamento non è dovuta:

a) se l'interessato dispone già dell'informazione;
b) se la registrazione o la comunicazione dei dati personali sono previste per legge;
c) se informare l'interessato si rivela impossibile o richiederebbe uno sforzo sproporzionato.

8. La conservsazione dei dati

I dati personali possono essere conservati solo per il tempo necessario per il completamento dell'obiettivo perseguito durante la loro raccolta.

In generale, i dati dei clienti possono essere tenuti per la durata del mandato professionale. Possono ovviamente essere conservati anche dopo la cessazione del rapporto professionale, al fine di tutelare i diritti dello Studio nei confronti del cliente, sia quanto al diritto a conseguire i compensi, sia per resistere ad eventuali azioni di responsabilità: per tale ragione, si ritiene che la conservazione dei dati possa prolungarsi per tutto il tempo di prescrizione ordinaria, prima della loro cancellazione definitiva.

È inoltre importante ricordare che i dati acquisiti in sede di identificazione e adeguata verificata ai sensi del decreto legislativo n. 231 del 2007 in materia di antiriciclaggio devono essere conservati per un periodo di 10 anni dalla cessazione del rapporto.

9. Il consenso

Il consenso è definito dall'art. 4, par. 1 n. 11, del GDPR come "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".

L'art. 6, par. 1, del GDPR indica le condizioni di liceità del trattamento, individuando 6 condizioni di cui almeno una deve ricorrere affinché il trattamento possa essere considerate lecito. Delle condizioni indicate, si evidenziano le seguenti:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
Quantunque non sia richiesto un consenso scritto, e sebbene l'attività professionale possa rientrare nella lettera b), è preferibile precostituirsi la prova di avere ottenuto il consenso, lo Studio, quindi, può sottoporre al cliente per la firma una dichiarazione di consenso in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. È facoltà dell'interessato revocare il proprio consenso in qualsiasi momento, ma "la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca".
10. il diritto di accesso
Il GDPR apporta le rilevanti modifiche anche sul diritto di accesso. Qualsiasi persona fisica che giustifichi la sua identità ha diritto di interrogare il titolare
- per sapere se sta trattando i suoi dati;
- per ottenere la comunicazione dei dati in forma comprensibile e tutte le informazioni disponibili per quanto attiene l'origine del trattamento;
- per ottenere informazioni sulla finalità del trattamento i dati raccolti e i destinatari
Il tempo di risposta a una richiesta è ora un mese dal ricevimento della richiesta . Viene tuttavia offerta l'opportunità di prorogare questo termine di due mesi, "data la complessità e il numero di applicazioni", a condizione che l'interessato riceva comunque un'informazione al riguardo entro un mese dal ricevimento della richiesta.
Il regolamento prevede un principio di gratuità copie fornite come parte di una richiesta di accesso (Articolo 12.5). Solo quando la domanda è manifestamente infondata o eccessiva il il responsabile del trattamento può richiedere il pagamento di "costi ragionevoli" che tengono conto dei costi amministrativi sostenuti per la fornitura delle informazioni. La medesima regola si applica quando viene richiesta una copia aggiuntiva dei dati.
Il regolamento prevede che se la persona inoltra una domanda per via elettronica, l'informazione richiesta è comunicata in forma elettronica di uso comune, a meno che l'interessato non richieda diversamente.
E' previsto inoltre che il responsabile del trattamento assista il titolare nell'adempimento dei suoi obblighi riguardo al diritto di accesso (articolo 28 e).
11. Privacy by default e by design
L'art. 25 del GDPR prevede l'obbligo Integrare di default il concetto di dati personali nella progettazione di nuovi prodotti e servizi. Quando lo Studio cambia i suoi software, pertanto, si deve interrogare sin dall'inizio in merito all'impatto dell'evoluzione sui dati che tratta. Ciò implica in particolare l'integrazione di tecniche di protezione e misure organizzative per limitare i rischi di violazione dei diritti e delle libertà delle persone.

PARTE SECONDA
1. Il titolare del trattamento
Ai sensi dell'art 4 comma. 7 il titolare del trattamento è 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.
Lo Studio di Ingegneria Associato Ferrari & Pacini è titolare del trattamento di tutte le informazioni che vengono allo stesso fornite dagli assistiti in virtù o in correlazione del mandato contrattuale ricevuto e di tutte le informazioni che tratta relativamente a dipendenti e fornitori.
Il GDPR prevede la figura dei **contitolari** del trattamento quando più titolari determinano congiuntamente le finalità e i mezzi del trattamento. Si reputa che nel mondo forense **questa figura**

possa ravvisarsi in tutti i casi in cui vi sia un mandato a più colleghi che lavorano insieme ed in collaborazione determinando insieme le finalità e le modalità del trattamento. In tutti questi casi Studio di Ingegneria Associato Ferrari & Pacini esplicita un accordo interno che definisce le rispettive responsabilità ed osservanza degli obblighi, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR.

I responsabili del trattamento sono soggetti ad oneri ed obblighi del tutto similari a quelli previsti per i titolari, devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.

Il registro delle attività di trattamento elenca le informazioni sulle caratteristiche dei trattamenti effettuati dal titolare del trattamento. Ogni titolare del trattamento di dati dovrà tenere un registro delle categorie di trattamento dei dati personali implementati sotto la sua responsabilità. Tale obbligo non vige per le organizzazioni con meno di 250 dipendenti, a meno che il trattamento non includa un rischio per i diritti e le libertà delle persone interessate, non occasionale o se si riferisce in particolare a dati sensibili o a dati relativi a condanne e reati.

Il registro, in conformità con l'articolo 30 del GDPR, deve includere le seguenti informazioni:

• Il nome e i dettagli di contatto del titolare, del contitolare, del responsabile e, se del caso, il rappresentante del responsabile della' elaborazione e responsabile della protezione dei dati;
• Gli scopi del trattamento;
• Una descrizione delle categorie di dati trattati, nonché delle categorie di persone coinvolte nel trattamento;
• Categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi I destinatari dei paesi parti terze o organizzazioni internazionali;
• Ove applicabile, i trasferimenti di dati personali verso un paese terza parte o un'organizzazione internazionale, compresa l'identificazione di paese terzo o di tale organizzazione internazionale e i documenti che certificano l'esistenza di garanzie adeguate;
• Ove possibile il termine ultimo previsto per la cancellazione dei dati;
• Ove possibile una descrizione generale delle misure di sicurezza tecniche ed organizzative

Lo Studio di Ingegneria Associato Ferrari & Pacini in quanto titolare del trattamento gestisce:

- i dati relativi al personale dipendente ed ai collaboratori;
- i dati relativi ai clienti;
- i dati relativi a fornitori.

Nell'ambito dei rapporti di collaborazione o di lavoro (ad esempio con una segretaria o il tecnico del computer) della gestione del libro paga e la gestione amministrativa del personale, Studio di Ingegneria Associato Ferrari & Pacini – in qualità di datore di lavoro effettua un trattamento di dati.

Nel contesto della gestione dei suoi dipendenti e, più in generale, il suo personale, Studio di Ingegneria Associato Ferrari & Pacini come il datore di lavoro può raccogliere principalmente due tipi di dati:

• Dati necessari per ottemperare a un obbligo legale.
• Dati utili per:
(i) gestione amministrativa del personale;
(ii) organizzazione lavoro;
(iii) azione sociale.

Durante il colloquio per l'assunzione, i dati dovrebbero essere usati solo per valutare la capacità del candidato di eseguire il lavoro proposto.

Potranno pertanto essere raccolti solo i dati relativi alla qualifica e all'esperienza del collaboratore (esempi: diplomi, precedenti lavori, ecc.)

È pertanto vietato:

• raccogliere dati sulla famiglia del candidato;
• raccogliere dati su opinioni politiche o appartenenza sindacale il candidato.

Studio di Ingegneria Associato Ferrari & Pacini non può utilizzare strumenti per controllare l'attività dei dipendenti o del personale.
Ad esempio, Studio di Ingegneria Associato Ferrari & Pacini potrebbe determinare le condizioni di utilizzo dell'accesso a Internet da parte di dipendenti e personale sul luogo di lavoro: può inserire i filtri per bloccare determinati contenuti (pornografia, pedofilia, ecc.).
È anche possibile limitare l'uso di Internet per motivi di sicurezza, ad esempio il download di software, o predisporre strumenti atti a controllare le ore di lavoro o l'accesso da parte dei dipendenti ai files.
Non è invece possibile estendere al controllo dell'attività dei dipendenti con l'utilizzo di un eventuale software.
In base al principio generale per cui il trattamento non può protrarsi oltre il tempo necessario per l'espletamento degli incarichi, ovvero il tempo necessario in funzione della finalità del trattamento stesso, i dati relativi ai dipendenti o ai collaboratori potranno essere conservati per il tempo della durata del rapporto, aumentato dell'eventuale tempo di maturazione della prescrizione, al fine di far valere i diritti nascenti dal rapporto.
In conformità con i requisiti dell'Articolo 13 del GDPR, i dipendenti e i collaboratori dello studio dovrebbero essere informati in merito a:
• L'identità e i dettagli di contatto del titolare del trattamento;
• I dettagli di contatto del responsabile della protezione dei dati quando ce n'è uno;
• L'obiettivo perseguito (gestione amministrativa del personale e assunzioni);
• la base legale del trattamento;
• interesse legittimo del titolare se costituisce la base giuridica del trattamento ex art. 6. Comma 1 lettera f;
• Destinatari dei dati (chi tiene i libri paga, ecc.);
• flussi transfrontalieri;
• la durata di conservazione;
• Condizioni di esercizio dei loro diritti di opposizione, accesso, rettifica e limitazione, ecc.;
• Il diritto di revocare il consenso se è la base giuridica del trattamento;
• Il diritto di presentare un reclamo all'autorità di controllo;
• Informazioni sulla natura normativa o contrattuale del trattamento quando si tratta della base giuridica del trattamento.
Questa informazione può essere inserita nell'accordo di collaborazione o nel contratto di lavoro, ovvero può essere oggetto di documento visualizzato o può essere inviata comunicazione via e-mail, in particolare per regolarizzare la situazione con dipendenti e personale che non sono stati adeguatamente informati.
Lo Studio di Ingegneria Associato Ferrari & Pacini:
1. VERIFICA CHE I DATI RACCOLTI NON SIANO ECCESSIVI RISPETTO ALLA FINALITA' DEL TRATTAMENTO
2. VERIFICA CHE CI SIA UNA BASE LEGALE PER IL TRATTAMENTO DEI DATI
3. RISPETTA IL PRINCIPIO DI MINIMIZZAZIONE
4. VERIFICA I DISPOSITIVI DI CONTROLLO DELL'ATTIVITA' DEL PERSONALE E LA LORO PERTINENZA
5. INSERISCE I DATI NEL REGISTRO DI TRATTAMENTO DEI DATI (ove tenuto)
6. DEFINISCE LA DURATA DI CONSERVAZIONE DEI DATI
7. FORNISCE L'INFORMATIVA AGLI INTERESSATI
2. Dati tratti nel rapporto con il cliente
Dati particolari
Nell'ambito dell'esercizio della professione , il trattamento dei dati personali del cliente riguarda tutti i dati necessari per la prestazione consulenziale.
Data la diversità dei campi di intervento dei consulenti, questi dati possono essere molto diversi e possono essere relativi alla vita personale, ma anche i dati di che rivestono una particolare

sensibilità: lo studio infatti potrebbe avere a che fare con dati personali che rivelano l'origine razziale o opinioni etniche, politiche, credenze religiose o filosofiche, l'appartenenza sindacale, così come l'elaborazione di dati genetici, dati biometrici ai fini dell'individuazione di una persona fisica, dati sanitari unici o di vita, orientamento sessuale.
L' articolo 9, comma 1 del GDPR prevede il divieto in linea di principio del trattamento di tali dati.
Dati relativi a condanne penali e reati.
L' articolo 10 del GDPR prevede che tale trattamento possa essere effettuato solo sotto il controllo dell'autorità pubblica, o regolamentato da disposizioni specifiche previste dalla legge nazionale.
Trattamento dei dati del cliente
Laddove il trattamento di dati particolari sia effettuato dallo Studio in modo non occasionale è opportuno che sia previsto nel registro dei trattamenti un apposito modulo relativo ai dati del cliente, che deve includere i seguenti elementi:
- Identità e dettagli di contatto del titolare del trattamento;
- Scopi;
- Categorie di persone interessate;
- Categorie di dati personali;
- Categorie di destinatari;
- Trasferimenti verso un paese terzo o un'organizzazione internazionale;
- Termine finale del trattamento;
- Descrizione generale delle misure di sicurezza tecniche e organizzative.

Informativa al cliente
In conformità con i requisiti della sezione 13 del GDPR, i clienti e devono essere informati su:
• L'identità e i dettagli di contatto del titolare del trattamento;
• i dettagli di contatto del responsabile della protezione dei dati quando ce n'è uno;
• L'obiettivo perseguito (gestione e monitoraggio dei file dei clienti);
• La base giuridica del trattamento (prestazione contrattuale o precontrattuale su richiesta del cliente);
• interesse legittimo del titolare se costituisce la base giuridica del trattamento ex art. 6. Comma 1 lettera f;
• destinatari di dati (responsabili, consulenti, ecc.);
• flussi transfrontalieri;
• la durata di conservazione;
• i diritti che hanno;
• condizioni per l'esercizio di questi diritti;
• Il diritto di revocare il consenso se è la base giuridica del trattamento;
• Il diritto di presentare un reclamo all'autorità di controllo;
• Informazioni sulla natura normativa o contrattuale del trattamento quando si tratta della base giuridica del trattamento.

Queste informazioni possono essere incluse nell'accordo con il cliente; possono anche essere comunicate via e-mail o in occasione della trasmissione di una nota di onorario, in particolare per regolarizzare la situazione con i clienti che non sono stati adeguatamente informati.
Tempo di conservazione dei dati del cliente
Studio di Ingegneria Associato Ferrari & Pacini titolare del trattamento deve definire una politica di durata e di conservazione dei dati nel suo ufficio. I dati personali possono essere conservati solo per il tempo necessario per il completamento dell'obiettivo perseguito durante la loro raccolta.
In generale, i dati dei clienti possono essere tenuti per la durata del mandato professionale.
I dati dovranno essere conservati inoltre, prima della loro cancellazione definitiva sino a che un'eventuale azione di responsabilità professionale in cui potrebbe essere implicato lo Studio, non sia prescritta.
Revoca del mandato

Come già rilevato più sopra con riferimento al diritto di portabilità dei dati, lo Studio che ha inizialmente trattato i dati è tenuto a comunicare i dati del suo cliente o di un collega alle seguenti condizioni:
- l cliente ha espresso il suo consenso al trattamento dei suoi dati personali o il trattamento è necessario per l'esecuzione di un contratto a cui il il cliente è parte o l'esecuzione delle misure precontrattuali adottate a richiesta del cliente;
- e il trattamento è stato effettuato con mezzi automatizzati.

Pertanto, se il suo cliente richiede la trasmissione dei suoi dati ad un collega, dovrà trasferirli in formato strutturato comunemente usato e leggibile da una macchina.
Si rammenta che ove il fascicolo fosse tenuto in modalità esclusivamente cartacea, non si applica il diritto alla portabilità, ma il fascicolo deve essere consegnato al cliente nel minor tempo possibile.
La sicurezza del fascicolo
È necessario adottare misure di sicurezza adeguate alla sensibilità dei trattamenti. Per fare ciò, è necessario verificare che l'accesso ai locali in cui sono conservati o memorizzati i fascicoli sia sufficientemente sicuro (uffici bloccati, accesso, ecc.). È anche importante verificare la sicurezza del sistema informatico su quali file sono memorizzati in format digitale (firewall, password robuste per accesso, diritti, ecc.).
Buona prassi
Studio di Ingegneria Associato Ferrari & Pacini deve prestare cura a non lasciare incostudite o in vista pratiche relative ai clienti.
Lo Studio di Ingegneria Associato Ferrari & Pacini:
1. VERIFICA CHE I DATI RACCOLTI NON SIANO ECCESSIVI RISPETTO ALLA FINALITA' DEL TRATTAMENTO
2. VERIFICA CHE CI SIA UNA BASE LEGALE PER IL TRATTAMENTO DEI DATI
3. RISPETTA IL PRINCIPIO DI MINIMIZZAZIONE
4. DEFINISCE LA DURATA DI CONSERVAZIONE DEI DATI
5. INSERISCE I DATI NEL REGISTRO DI TRATTAMENTO DEI DATI (ove tenuto)
6. VERIFICA CHE I FASCICOLI DEI CLIENTI TANTO DIGITALI CHE CARTACEI SIANO CONSERVATI IN MODO SICURO
7. VERIFICA LA SICUREZZA DEL SISTEMA INFORMATICO CON IL FORNITORE IT
8. EFFETTUA BACK UP PERIODICO DEI DATI CONSERVATI
9. SI CURA DI RICEVERE I CLIENTI IN AMBIENTI ORDINATI PRIVI DI FASCICOLI IN VISTA RIPONENDO TUTTE LE SERE I FASCICOLI IN ARMADIO CHIUSO

3. Rapporti con soggetti esterni allo studio

La figura del responsabile del trattamento
Ai sensi dell'art. 4, par. 8 il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che "tratta dati personali per conto del titolare del trattamento".
È importante sottolineare il concetto del trattamento dei dati personali "per conto" del titolare del trattamento. Il responsabile, in sostanza, effettua il trattamento in quanto i dati personali gli sono comunicati dal titolare del trattamento.
In pratica, è la persona che tratta dati personali per conto dello studio come un contabile, un editore di software, un host web, ecc.
Il responsabile è da considerarsi solo "esterno" allo Studio di Ingegneria Associato Ferrari & Pacini; pertanto non è possibile nominare un Collega, un dipendente o un collaboratore come responsabile della protezione dei dati. I soggetti a cui lo studio comunica i dati personali trattati sono considerati responsabili del trattamento (es.: commercialista, consulente del lavoro, consulente, fornitori di servizi digitali, conservatori di documenti informatici, ecc.).
Nella ipotesi in cui vi sia un responsabile del trattamento (un soggetto esterno) e qualora fosse una persona fisica, la prima cosa da fare è fornire l'informativa al momento della raccolta dei suoi dati personali.

Nel caso in cui vi sia un responsabile del trattamento dei dati l'art. Articolo 28, comma. 3, del GDPR prevede l'obbligo di stipulare un contratto tra titolare e responsabile del trattamento, dettagliando i suoi contorni e stabilendo requisiti rigorosi sugli aspetti severi e più importanti.
Il contratto dovrà includere:
• l'oggetto;
• la durata;
• natura;
• lo scopo;
• il tipo di dati personali;
• le categorie di persone interessate;
• i diritti e gli obblighi del responsabile del trattamento;
• le misure di sicurezza attuate in relazione al trattamento dei dati che sarà effettuato.
Il contratto deve anche definire gli obblighi del responsabile relativi a:
• la possibilità di elaborare dati solo su un'istruzione documentata del titolare del trattamento anche per quanto riguarda i flussi transfrontalieri;
• riservatezza dei dati;
• l'esercizio dei diritti delle persone interessate;
• l'assistenza che deve essere fornita al titolare tramite con misure tecniche e organizzative adeguate, nella misura in cui sia possibile, per consentire al titolare di adempiere all'obbligo di rispondere alle richieste delle persone interessate;
• l'assistenza fornita al titolare per assicurare il rispetto dei suoi obblighi in relazione alla natura del trattamento e delle informazioni a disposizione del responsabile;
• la cancellazione dei dati in questione alla fine del trattamento, o la loro restituzione al titolare o alla loro conservazione se richiesto da a disposizione nazionale o europea;
• la messa a disposizione del titolare dei dati tutte le informazioni necessarie a dimostrare la conformità agli obblighi e a consentire condurre verifiche, comprese le ispezioni, da parte del titolare o di suo incaricato, e collaborare in questi audit;
Le clausole contrattuali che vincolano i titolari e responsabili devono pertanto essere molto precise sia sulle modalità di trattamento che sulla gestione delle loro relazioni e sullo scambio di informazioni tra di loro.
Ai sensi dell'articolo 28, paragrafo 1, del GDPR il responsabile del trattamento dei dati ha l'obbligo di incaricare solo responsabili "che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".
Il GDPR stabilisce (art. 28, par. 2, GDPR) che il responsabile può nominare a sua volta un responsabile (subresponsabile) ma tale nomina è subordinata a esplicita autorizzazione scritta del titolare del trattamento.
Ai sensi dell'art. 29 del GDPR "Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri". Pertanto, sono esplicitamente richieste istruzioni specifiche al responsabile del trattamento da parte del titolare; tali istruzioni potranno essere indicate nel contratto tra il titolare e il responsabile.
Gli studi devono interpellare i loro subappaltatori sulle garanzie adottate per garantire la loro conformità con il GDPR.
Nel caso in cui lo studio identifichi lacune nelle misure adottate dal responsabile dovranno integrare il contratto al fine di colmarle.

Lo Studio di Ingegneria Associato Ferrari & Pacini:

1. IDENTIFICA I RESPONSABILI DEL TRATTAMENTO

2. VERIFICA LA CONFORMITA' DEI RESPONSABILI E LE MISURE ADOTTATE NEL CONTRATTO STIPULATO CON IL RESPONSABILE

3. MODIFICA, OVE NECESSARIO IL CONTRATTO GIA' ESISTENTE

4. Il Sito Web

Gli Studi di Consulenza possono utilizzare siti web per promuovere la loro attività, presentare I componenti dello studio, o pubblicare articoli ma il sito web può anche consentire la raccolta di dati personali con diverse modalità:

• un questionario online;
• una consultazione online;
• un modulo di contatto;
• creazione di un account online;
• attraverso i cookies

La titolarità di un sito web comporta principalmente la pubblicazione di una informativa, redatta ai sensi degli articoli 13 e 14 del GDPR.

Raccolta di dati attraverso il sito internet

Qualora il sito web dello studio permetta l'inserimento di dati personali (es. modulo di contatto), è opportuno che sia utilizzata la connessione con protocollo sicuro HTTPS (tecnologia "SSL") per garantire il rispetto delle misure di sicurezza in funzione della confidenzialità delle informazioni scambiate con il professionista.

Lo Studio dovrà inserire, all'interno del registro delle attività di trattamento, un apposito modulo dedicato al trattamento dei dati sul sito web che deve includere i seguenti elementi:

• Identità e dettagli di contatto del titolare
• scopi;
• Categorie di persone;
• Categorie di dati personali;
• Categorie di destinatari;
• trasferimenti verso un paese terzo o un'organizzazione internazionale;
• Scadenze per la cancellazione;
• Descrizione generale delle misure di sicurezza tecniche e organizzative.

Qualora lo Studio riceva una proposta di incarico tramite il sito web sussiste l'obbligo di formalizzare il mandato accertando l'identità del cliente.

Come rendere l'informativa nel sito in caso di utilizzazione dei cookies

Come prima cosa, gli Studi dovranno verificare l'effettiva presenza di cookie sul loro sito web attraverso il dipartimento IT dell'azienda, i fornitori di servizi o controllando gli strumenti utilizzati, ecc.

Successivamente, è necessario determinare i tipi di cookie utilizzati sul sito web.

In effetti, alcuni cookie richiedono il consenso dell'utente, questo è il caso per:

• cookie pubblicitari;
• cookie "social network" generati dai pulsanti di condivisione quando raccolgono dati personali senza il consenso delle persone interessate;
• alcuni cookie di misurazione degli accessi

In questo caso, il consenso deve essere precedente all'inserimento o alla lettura del contenuto del sito. Finché il cliente non ha dato il suo consenso, questi cookie non possono essere depositati o letti dal sito stesso.

Lo Studio di Ingegneria Associato Ferrari & Pacini UTILIZZA SITI WEB in maniera conforme al nuovo GDPR

5. Buona prassi

Come già si è detto, è essenziale garantire la sicurezza e la riservatezza dei dati trattati dagli studi garantendo un livello di sicurezza adeguato al rischio di trattamento.

In caso di documenti o fascicoli analogici è necessario mettere in atto misure di sicurezza fisica nello studio:

ad esempio:

• Limitare l'accesso all'ufficio;

• Non archiviare fascicoli o documenti contenenti dati personale in locali dello studio accessibili a tutti;
• Installare gli allarmi nei locali dello studio.
In caso di documenti o fascicoli gestiti digitalmente
E' necessario:
• Autenticare gli utenti: impostare una password minima di 8 caratteri contenenti maiuscole, lettere minuscole, numeri e caratteri speciale; non condividerla; non scriverla chiaramente su un foglio; evitare la pre-registrazione; cambiarla regolarmente;
• gestire i diritti e istruire gli utenti: determinare persone che hanno il diritto di accedere ai dati personali;
• rimuovere le autorizzazioni di accesso obsolete;
• Fornire mezzi di crittografia per computer portatili e dispositivi di archiviazione rimovibili (chiavette USB, CD, DVD), evitare di memorizzare dati personali sensibili dei clienti.
• eseguire il backup e pianificare la business continuity: implementare i backup regolarmente, conservare i supporti di backup in un luogo sicuro,

Lo Studio di Ingegneria Associato Ferrari & Pacini:

1. LIMITA L'ACCESSO ALLO STUDIO
2. VERIFICA E METTE IN SICUREZZA I LUOGHI OVE SONO CONSERVATI I FASCICOLI
3. HA INSTALLATO UN SISTEMA DI ALLARME
4. PREVEDE MISURE DI IDENTIFICAZIONE DELL'UTILIZZATORE
5. HA GESTITO LE ABILITAZIONI E SENSIBILIZZATO L'UTILIZZATORE
6. HA METTESSO IN SICUREZZA I DISPOSITIVI MOBILI
7. HA EFFETUATO IL CENSIMENTO DEGLI ASSET UTILIZZATO NEL TRATAMENTO DEI DATI
8. HA EFFETTUATO LA VALUTAZIONE DEI RISCHI CONNESSI A CIASCUN ASSENT E ADOTTATO LE RELATIVE CONTROMISURE
9. HA PIANIFICATO LA BUSINESS CONTINUITY
1O. HA ADOTTATO PROCEDURE DI NOTIFICAZIONE DELLE VIOLAZIONI DEI DATI

6. Il responsabile delle protezione dei dati – il DPO

Ai sensi dell'articolo 37 del GDPR, i titolari del trattamento e i responsabili dovranno nominare un responsabile della protezione dei dati ogni qualvolta:

- il trattamento sia effettuato da un'autorità, un organismo ovvero un ente pubblico;
- le attività principali del titolare del trattamento e del responsabile del trattamento richiedano il monitoraggio regolare e sistematico degli interessati su larga scala;
- se le loro attività principali (core business) li portano a trattare (su larga scala) categorie specifiche di dati, noti come dati "sensibili" e dati su condanne penali e reati;

Negli altri casi, la nomina di un responsabile della protezione dei dati è ovviamente possibile, come opzione organizzativa ulteriore e di maggior cautela.
I titolari del trattamento possono optare per un responsabile per la protezione di dati condiviso con altri, ovvero per un delegato interno all'organizzazione od esterno.
Se viene nominato un responsabile della protezione dei dati, lo studio è obbligato a pubblicare le informazioni relative al DPO e a farne comunicazione all'autorità di controllo competente.
Tuttavia, la previsione dell'art. 37 (così come quella dell'art 35) si applica sempre al titolare o al responsabile del trattamento di categorie dati particolari. Queste disposizioni richiedono la nomina del DPO nei casi in cui le attività principali della persona del titolare o del responsabile consistono in un trattamento su larga scala delle categorie di dati di cui all'articolo 9.
Secondo le linee guida dei responsabili della protezione dei dati, "per "attivita principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento, comprese tutte quelle

attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare del trattamento o del responsabile del trattamento.
Va inoltre correttamente interpretata l'espressione "larga scala", e ciò in quanto anche un piccolo studio potrebbe dover affrontare trattamenti di una notevole mole di dati sensibili: al riguardo, si evidenzia che il considerando 91 del GDPR - così come le stesse esemplificazioni delle linee guida - consentono di sostenere che questo requisito non si applica ai professionisti organizzati su base individuale.
La valutazione dell'opportunità o meno di nominare un delegato alla protezione i dati deve essere effettuata caso per caso, in funzione in particolare dei seguenti parametri:

- numero di persone interessate dal trattamento di dati personali
- volume dei dati trattati,
- la durata
- permanenza delle attività del trattamento
- estensione geografica dell'attività di trattamento.

Vale, in ogni caso, la medesima regola espressa per il DPIA (documento di valutazione di impatto per la protezione dei dati): per quanto non obbligatoria, la designazione di un Data Protection Officer potrebbe essere valutata come un'opportunità nella gestione dei trattamenti.
I compiti del DPO
Il GDPR impone ai DPO degli obblighi importanti:

- Informare e consigliare il titolare o il responsabile, e i loro dipendenti;
- Assicurare il rispetto del regolamento e della legge nazionale in merito alla protezione dei dati;
- Informare l'organizzazione sulla realizzazione di studi di impatto sulla protezione dati e verificarne l'esecuzione;
- Collaborare con il Garante ed esserne il punto di contatto.
- Collaborare nell'adeguamento agli obblighi imposti dal regolamento europeo, fornendo informazioni sul contenuto dei nuovi obblighi imposti dal regolamento europeo;
- Condurre un inventario del trattamento dei dati della propria organizzazione;
- Progettare azioni di sensibilizzazione;
- Gestire in maniera continuativa la conformità dell'organizzazione al regolamento.

Le responsabilità che sorgono in capo alla persona designata come DPO sono quindi rilevantissime.
Lo Studio di Ingegneria Associato Ferrari & Pacini :
ALLO STATO NON REPUTA NECESSARIO NOMINARE UN DATA PROTECTION OFFICER
7. Il data breah
In virtù degli artt. 33 e 34 del GDPR uno studio che agisce quale titolare del trattamento deve notificare tutte le violazioni dei dati personali al Garante e comunicare con le persone interessate in caso di alto rischio per i diritti e la libertà personali.
La violazione dei dati personali, il c.d. data breach, è una violazione della sicurezza che comporta accidentalmente o illecitamente, distruzione, perdita, alterazione, divulgazione o accesso non autorizzati di dati di natura personale trasmessi, conservati o altrimenti elaborati.
Il titolare del trattamento ha l'obbligo di documentare - e di esibire ad eventuale richiesta del Garante - qualsiasi violazione dei dati personali, le circostanze che l'hanno causata, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
Se lo studio si è avvalso di un responsabile del trattamento, quest'ultimo ha l'obbligo di notificare al titolare, senza ingiustificato ritardo dal momento in cui ne viene a conoscenza, qualsiasi violazione dei dati personali. È raccomandabile che tale obbligo sia oggetto di una specifica clausola contrattuale con il responsabile.

In ottemperanza agli artt. 33 e 34 del GDPR uno studio che agisce quale titolare del trattamento, in caso di alta probabilità di rischio dei diritti e delle libertà personali, deve notificare al Garante e comunicare agli interessati tutte le violazioni dei dati personali di cui viene a conoscenza.
In applicazione del principio generale di accountability, è rimessa altitolare del trattamento la valutazione di probabilità o meno che lo specifico data breach possa presentare un rischio per i diritti e le libertà degli assistiti e degli interessati. Laddove la valutazione abbia esito affermativo, non oltre le 72 ore dalla presa di coscienza (GDPR, Art. 33) lo Studio (titolare del trattamento) deve notificare la violazione al Garante della protezione dei dati personali (in qualità di autorità competente), specificando, tra l'altro:

- la natura della violazione dei dati personali (categorie e numero approssimativo di persone e record di dati in questione);
- Il nome e le informazioni di contatto del DPO (laddove applicabile) o, comunque, di un punto di contatto da cui è possibile ottenere ulteriori informazioni;
- le probabili conseguenze della violazione;
- le misure adottate o da adottare per mitigare qualsiasi conseguenze negative.

Il modulo per la notifica – solo online – della violazione dei dati personali è a disposizione del titolare sul sito del Garante.
Lo Studio di Ingegneria Associato Ferrari & Pacini deve:

- mettere in atto misure per analizzare i rischi del trattamento istituito per i diritti e le libertà delle persone fisiche;
- assicurarsi che le violazioni siano notificate entro 72 ore, in caso contrario spiegare accuratamente le motivazioni del ritardo all'autorità garante;
- indicare nella notifica i fatti della violazione, la natura della violazione, i suoi effetti e le misure adottate per porvi rimedio;
- fare ogni sforzo per documentare il più possibile qualsiasi violazione per consentire all'autorità di vigilanza di verificare la conformità ai requisiti imposti dal GDPR;
- mettere immediatamente in atto misure di emergenza per porre rimedio alla violazione e mitigare le conseguenze.

Comunicazione alle persone interessate.
Laddove il titolare valuti che sia probabile che la violazione sia suscettibile di presentare un elevato rischio per i diritti e le libertà di una persona fisica, sarà necessario comunicare anche all'interessato il data breach. Tale comunicazione deve contenere almeno:

- le informazioni del nome e dei dati di contatto del DPO (ove applicabile) o di altro punto di contatto presso cui ottenere maggiori informazioni;
- la descrizione - con un linguaggio semplice e chiaro - la natura della violazione dei dati personali e delle probabili conseguenze, le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne I possibili effetti negativi.

La comunicazione all'interessato può non essere necessaria se:

- le misure tecniche e organizzative preventivamente approntate dal titolare abbiano hanno reso i dati incomprensibili per qualsiasi persona; ciò capita, ad esempio, quando tali dati, pur diffusi, sono stati cifrati o crittografati;
- sono state adottate misure per garantire che il rischio sia scongiurato e non possa più verificarsi;
- la comunicazione richieda "sforzi sproporzionati", ma in questo caso è autorizzata una comunicazione "pubblica" piuttosto che diretta sempreché la stessa possa raggiungere ed informare gli interessati con analoga efficacia della comunicazione diretta.

La comunicazione gli interessati può anche essere richiesta dall'Autorità garante se quest'ultima reputa, dopo aver esaminato la notificazione, che vi sia un alto rischio per gli interessati derivante dal data breach.
Lo Studio di Ingegneria Associato Ferrari & Pacini IN CASO DI DATA BREACH:

1. AVVISERA' SENZA INDUGIO LE PERSONE COMPETENTI
2. QUALIFICHERA' LA VIOLAZIONE
3. ADOTTARA' LE MISURE NECESSARIE PER MINIMIZZARE LE CONSEGUENZE
4. EFFETTUERA' LE NOTIFICAZIONI ALL'AUTORITÀ GARANTE,
5. SE IL RISCHIO È ELEVATO EFFETTUERA' LE COMUNICAZIONI AGLI INTERESSATI
6. IN OGNI CASO ANNOTERA' TUTTE LE VIOLAZIONI (ANCHE SE NON NOTIFICATE) NEL REGISTRO DELLE VIOLAZIONI

8. Le sanzioni

Titolari e responsabili del trattamento possono essere soggetti a sanzioni amministrative significative per il mancato rispetto delle disposizioni del GDPR L'autorità Garante per la protezione dei Dati personali, può, in particolare:

- rivolgere avvertimenti;
- ammonire l'associazione o la società professionale;
- limitare temporaneamente o permanentemente un trattamento;
- sospendere i flussi di dati;
- ordinare di soddisfare richieste per l'esercizio dei diritti delle persone;
- ordinare la rettifica, limitazione o cancellazione dei dati;
- ritirare la certificazione di conformità concessa all'avvocato, allo studio, all'associazione o alla società professionale, ovvero ordinarne il ritiro all'autorità di certificazione;
- comminare una sanzione amministrativa di importo compreso tra i 10 ed i 20 milioni di euro, ovvero, in caso di grandi studi internazionali di importo compreso tra il 2% ed il 4% del fatturato mondiale.

Si specifica che il sito web dello studio di ingegneria associato non fa uso di cookies.

Savona lì, 25 febbraio 2024

Responsabili del trattamento dei dati:
Massimo Pacini e Paolo Ferrari in qualità di ingegneri associati

Studio di Ingegneria Associato Ferrari & Pacini
Sede: I – 17024 Finale Ligure (SV) – via Saccone 6/4 – tel. 019 694082
C.F. e P.Iva: 01117170090
Email: segreteria@ingegneri-associati.it
PEC: ferraripacini@pec.ingegneri-associati.it