SCHEDE PRATICHE

1. **L'ITAL (nelle sue articolazioni territoriali: reg.le o prov.le) QUALE TITOLARE DEL TRATTAMENTO DEI DATI.**

Ai sensi dell'art 4 comma. 7 GDPR (C74) 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. Nel caso di società o associazioni è sempre l'ente giuridico - in nome del legale rappresentante - ad essere qualificato titolare.

Il termine inglese "Data Controller" ben si concilia con il carattere gestionale di colui che può determinare finalità e mezzi del trattamento. L'Ital, tramite i suoi responsabili territoriali, sarà titolare del trattamento di tutte le informazioni che vengono allo stesso fornite dagli assistiti in virtù o in correlazione del mandato ricevuto.

Il GDPR prevede altresì (art. 26, C79) la **figura dei contitolari del trattamento** quando più titolari determinano congiuntamente le finalità e i mezzi del trattamento. In questi casi è necessario un esplicito accordo interno che definisca 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;

Ai sensi dell'art. 4 par. 8 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 (come è per il Patronato) o a dati relativi a condanne e reati. Il Patronato sarà quindi soggetto all'obbligo di istituire un registro delle attività trattamento allorché il trattamento sia riferito a particolari categorie di dati. In ogni caso la detenzione del registro è fortemente consigliata, anche nel caso non vi sia l'obbligo, perché

consente di mappare più chiaramente i trattamenti e di monitorare gli stessi ai fini del rispetto dei principi del GDPR e dei diritti degli interessati, oltre a risultare molto utile, ove occorra, per fornire prova dell'esatto adempimento all'obbligo adeguamento al principio dell'accountability.

Tale 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

Quali dati tratta il Patronato?

Il patronato tratta:

- i dati relativi al personale dipendente ed ai collaboratori;
- i dati relativi agli assistiti;
- i dati raccolti attraverso il sito internet

a. I dati relativi ai dipendenti e ai collaboratori

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, il Patronato – in qualità di datore di lavoro effettua un trattamento di dati. Lo deve pertanto effettuare in conformità alle norme del GDPR, ricordando che l'art. 88 prevede discrezionalità Commissione degli stati membri nella regolamentazione del trattamento dei dati nell'ambito del rapporto di lavoro (ad oggi il decreto legislativo non è ancora stato emanato). Nel contesto della gestione dei suoi dipendenti e, più in generale, il suo personale, il Patronato come 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 e (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 del candidato. Il Patronato 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 l'utilizzo di un eventuale software installato al fine di calcolare il tempo dedicato dal dipendente allo studio o alla predisposizione di atti di una pratica.

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'art. 13 del GDPR i dipendenti e i collaboratori del Patronato 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.

RIASSUMENDO

COSA DEVE FARE IL PATRONATO?

1. VERIFICARE CHE I DATI RACCOLTI NON SIANO ECCESSIVI RISPETTO ALLA FINALITA' DEL TRATTAMENTO

2. VERIFICARE CHE CI SIA UNA BASE LEGALE PER IL TRATTAMENTO DEI DATI
3. RISPETTARE IL PRINCIPIO DI MINIMIZZAZIONE
4. VERIFICARE I DISPOSITIVI DI CONTROLLO DELL'ATTIVITA' DEL PERSONALE E LA LORO PERTINENZA 5. INSERIRE I DATI NEL REGISTRO DI TRATTAMENTO DEI DATI (ove tenuto)
6. DEFINIRE LA DURATA DI CONSERVAZIONE DEI DATI
7. DARE L'INFORMATIVA AGLI INTERESSATI

******

B) I DATI RELATIVI AGLI ASSISTITI

Nell'ambito dell'esercizio della propria attività istituzionale di patronato, il trattamento dei dati personali dell'assistito riguarda tutti i dati necessari per la presentazione delle domande tese ad ottenere i benefici assistenziali e previdenziali e per la difesa, anche giudiziale dei relativi interessi. Data la diversità dei campi di intervento, questi dati possono essere molto diversi e possono essere relativi alla vita personale, ma anche i dati che rivestono una particolare sensibilità: il patronato infatti potrebbe avere a che fare con dati personali che rivelano l'origine razziale o opinioni etniche, politiche, credenze religiose, l'appartenenza sindacale, così come l'elaborazione di dati genetici, dati biometrici, 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.

Tuttavia, l'articolo 9 prevede un'eccezione al comma 2.f) per "*accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionale*". Il Patronato può quindi trattare dati particolari nell'esercizio della propria attività purché i dati in questione siano strettamente necessari per esercitare o difendere i diritti degli assistiti. Ovviamente è raccomandata una interpretazione rigorosa di questa necessità, anche nel rispetto del principio di minimizzazione di cui si è detto più sopra.

Laddove il trattamento di dati particolari sia effettuato dal Patronato 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 agli assistiti

In conformità con i requisiti della sezione 13 del GDPR, gli assistiti dovrebbero essere informati su: • L'identità e i dettagli di contatto del titolare del trattamento (la ditta); • 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 (subappaltatori, ufficiali giudiziari, 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'atto di incarico dell'assistito; possono anche essere comunicate via e-mail, in particolare per regolarizzare la situazione con gli assistiti che non sono stati adeguatamente informati.

Per quanto tempo devono essere conservati i dati dell'assistito?

Il Patronato, 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 degli assistiti i 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 il Patronato non sia prescritta.

Cosa deve fare il Patronato in caso di revoca del mandato?

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

Pertanto, se l'assistito richiede la trasmissione dei suoi dati ad un altro patronato, l'Ital dovrà trasferirli in formato strutturato comunemente usato e leggibile da una macchina.

La sicurezza del fascicolo telematico e\o cartaceo.

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 badge, ecc.). È anche importante verificare la sicurezza del sistema informatico su quali file

sono memorizzati in formato digitale (firewall, password robuste per accesso, diritti, ecc.)

RIASSUMENDO:

COSA DEVE FARE IL PATRONATO?

1. VERIFICARE CHE I DATI RACCOLTI NON SIANO ECCESSIVI RISPETTO ALLA FINALITA' DEL TRATTAMENTO
2. VERIFICARE CHE CI SIA UNA BASE LEGALE PER IL TRATTAMENTO DEI DATI
3. RISPETTARE IL PRINCIPIO DI MINIMIZZAZIONE
4. DEFINIRE LA DURATA DI CONSERVAZIONE DEI DATI
5. INSERIRE I DATI NEL REGISTRO DI TRATTAMENTO DEI DATI (ove tenuto)
6. VERIFICARE CHE I FASCICOLI DEGLI ASSISTITITI TANTO DIGITALI CHE CARTACEI SIANO CONSERVATI IN MODO SICURO
7. VERIFICARE LA SICUREZZA DEL SISTEMA INFORMATICO CON IL FORNITORE

***

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 del PATRONATO come un consulente, un contabile, un editore di software, un host web, ecc.

I soggetti a cui il Patronato comunica i dati personali trattati sono considerati responsabili del trattamento (es.: commercialista, consulente del lavoro, consulente medico, 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 di persone giuridiche si può procedere con la sottoscrizione del contratto.

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 conformità agli obblighi e a consentire condurre verifiche, comprese le ispezioni, da parte del titolare o di suo incaricato, e collabora in questi audit; • l'eventuale assunzione da parte del responsabile di altro responsabile per l'esecuzione di specifiche attività di trattamento per conto del titolare.

L'incarico che deve essere formalizzato in un contratto che preveda tutti gli obblighi sopra elencati. 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. RIASSUMENDO

COSA DEVE FARE IL PATRONATO RISPETTO AI RESPONSABILI DEL TRATTAMENTO?

1. IDENTIFICARE I RESPONSABILI DEL TRATTAMENTO

2. VERIFICARE LA CONFORMITA' DEI RESPONSABILI E LE MISURE ADOTTATE NEL CONTRATTO STIPULATO CON IL RESPONSABILE
3. MODIFICARE, OVE NECESSARIO IL CONTRATTO GIA' ESISTENTE

***

L'ADOZIONE DI BUONE PRASSI PER LA SICUREZZA DEI DATI

Come già si è detto, è essenziale garantire la sicurezza e la riservatezza dei dati trattati, 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: ad esempio: • Limitare l'accesso all'ufficio; • Non archiviare fascicoli o documenti contenenti dati personale in locali accessibili a tutti; • Installare gli allarmi nei locali dell'ufficio.

In caso di documenti o fascicoli gestiti digitalmente Si consiglia di: • 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; scrivere un regolamento di utilizzo del computer e inserirlo nel regolamento interno nell'ipotesi che sia stato adottato; • mobile computing sicuro: 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, ecc

RIASSUMENDO

MISURE DI SICUREZZA FISICHE

1. LIMITARE L'ACCESSO ALLO STUDIO
2. VERIFICARE E METTERE IN SICUREZZA I LUOGHI OVE SONO CONSERVATI I FASCICOLI
3. INSTALLARESISTEMA DI ALLARME

MISURE DI SICUREZZA DIGITALI

1. PREVEDERE MISURE DI IDENTIFICAZIONE DELL'UTILIZZATORE
2. GESTIRE LE ABILITAZIONI E SENSIBILIZZARE L'UTILIZZATORE
3. METTERE IN SICUREZZA I DISPOSITIVI MOBILI
4. Effettuare il censimento degli asset (beni fisici o digitali) utilizzati nel trattamento dei dati
5. Effettuare la valutazione dei rischi connessi a ciascun asset e adottare le relative contromisure
6. PIANIFICARE LA BUSINESS CONTINUITY

- ADOTTARE UN REGOLAMENTO DI UTILIZZO DEL COMPUTER
- ADOTTARE PROCEDURE DI NOTIFICAZIONE DELLE VIOLAZIONI DEI DATI PERSONALI

IL RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO

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

Il gruppo di lavoro articolo 29 (WP29), composto da rappresentanti delle Autorità Nazionali per la protezione dei dati degli Stati membri dell'UE ha pubblicato linee guida sul ruolo dei responsabili della protezione dei dati e fornito raccomandazioni per adottare buone prassi.

Se viene nominato un responsabile della protezione dei dati, il Patronato 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 "attività 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",

Vale, in ogni caso, la medesima regola espressa per il DPIA (documento di valutazione di impatto per la protezione dei dati): anche quando non obbligatoria, la designazione di

un Data Protection Officer potrebbe essere valutata come un'opportunità organizzativa nell'ormai imprescindibile gestione dei trattamenti.

Il GDPR impone ai DPO degli obblighi importanti: sono come dei direttori di orchestra della conformità in materia di protezione dei dati personali in seno all'organismo che li ha nominati, sono incaricati:

- 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.

DATA BREACH

In virtù degli artt. 33 e 34 del GDPR un patronato 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 legale 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 un patronato 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 al patronato, titolare

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) il 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.

Si raccomanda inoltre di: 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.
RIASSUMENDO
IN CASO DI DATA BREACH:
1. AVVISARE SENZA INDUGIO LE PERSONE COMPETENTI
2. QUALIFICARE LA VIOLAZIONE
3. ADOTTARE LE MISURE NECESSARIE PER MINIMIZZARE LE CONSEGUENZE
4. EFFETTUARE LE NOTIFICAZIONI ALL'AUTORITÀ GARANTE, A MENO CHE NON SIA IMPROBABILE CHE SUSSISTA UN RISCHIO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE
5. SE IL RISCHIO È ELEVATO EFFETTUARE LE COMUNICAZIONI AGLI INTERESSATI
6. IN OGNI CASO ANNOTARE TUTTE LE VIOLAZIONI (ANCHE SE NON NOTIFICATE) NEL REGISTRO DELLE VIOLAZIONI

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 IL PATRONATO,
- 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
- Può inoltre ritirare la certificazione di conformità concessa ovvero ordinarne il ritiro all'autorità di certificazione;
- comminare una elevata sanzione amministrativa.