Il GDPR e il Professionista: dalla teoria alla pratica

Roma, lì 8 marzo 2023

Avv. Milena Castiello

.

Il Professionista e la privacy..la “*teoria*”

Novità del Regolamento Europeo

Modifiche	Novità
Definizioni esistenti	Principio accountability
Specificazione dei ruoli Titolare e Responsabile	Principio Privacy by design e Privacy by default
Informativa più chiara e completa	Nuove definizioni
Consenso sempre esplicito, strumento di garanzia anche on line	Responsaible della protezione dei dati (cd.“Data Protection Officer)
Regole più rigorose per garantire il Trasferimento dati all’estero	Registro dei trattamenti
Trattamenti automatizzati - limiti alla possibilità per il titolare di adottare decisioni solo sulla base di un trattamento automatizzato dei dati	Mappatura dei rischi
Inasprimento delle sanzioni	Pia (Privacy Impact assesment – Valutazione d’impatto)
	Notifica Data Breach
	Nuovi diritti dell’interessato(Diritto all’oblio, portabilità dei dati)

Principi

Il principio di *accountability* (responsabilizzazione) è il *«principio madre»* il quale costituisce il punto di maggiore novità e interesse nonché cardine della disciplina.

I principi fondamentali che regolano il GDPR sono e ai quali è necessario attenersi per un corretto e conforme trattamento dei dati sono:

- - liceità, correttezza e trasparenza;
- - limitazione della finalità e della conservazione;
- - minimizzazione dei dati;
- - esattezza, integrità e riservatezza;
- - accountability;
- - *privacy by design* e *privacy by default*.

Ambito di applicazione materiale

- Si applica solo al trattamento dei dati personali di **persone fisiche, il cd. Interessato;**
- Riguarda trattamenti interamente o parzialmente **automatizzati o non automatizzati, se i dati personali sono contenuti in un archivio o sono** destinati a confluirvi;
- Il Regolamento non si applica ai trattamenti di dati personali effettuati:

  a) da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

  b) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

  c) dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

  d)effettuati da Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V capo 2, TUE (politica estera e sicurezza comune)

Ambito di applicazione materiale

Il Regolamento riconosce tutela a tutti i trattamenti automatizzati o manuali, sempreché destinati ad un archivio, che consiste in “un insieme strutturato di dati personali accessibili secondo criteri determinati”.

Ambito di applicazione territoriale

Il Regolamento si applica:

1) al trattamento di dati personali effettuato da un **Titolare o Responsabile stabilito nella UE, indipendentemente dal fatto che il trattamento sia** effettuato o meno nella UE;

2) al trattamento di dati personali effettuato da **Titolari o Responsabili non stabiliti nell'UE, indipendentemente dal fatto che il trattamento sia** effettuato o meno nell'Unione, se il **trattamento ha ad oggetto dati personali di interessati che si trovano nella UE e riguarda:**

(i) l'offerta di beni o servizi (anche non a pagamento) ai suddetti interessati

(ii) il **monitoraggio del loro comportamento nel territorio della UE;**

3) al trattamento effettuato da un Titolare stabilito in uno **Stato extra UE soggetto al diritto di uno Stato UE in virtù del diritto internazionale**

Definizioni:
Dati personali e dati particolari

Il **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;

Categorie particolari di dati personali (dati particolari) : dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

Dati relativi alla salute: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Definizioni:
Dati personali e dati particolari (segue)

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati

Dati giudiziari: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (*ad esempio*, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Definizioni: Trattamento

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.

Definizioni: Violazione

«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.

Definizioni: Soggetti

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;

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;

Contitolare del trattamento: due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento.

Definizioni: Soggetti *(segue)*

Incaricati/ designati del trattamento: categoria di soggetti, identificata con le *"persone autorizzate al trattamento" non è definita formalmente, ma* disciplinata indirettamente. Viene previsto per il Titolare l'obbligo di indicare le persone autorizzate all'interno della sua struttura;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

Obblighi ed adempimenti

- Il Titolare deve attuare **misure tecniche ed organizzative** adeguate per garantire e dimostrare che il trattamento è effettuato conformemente al Regolamento.

  Le misure devono essere riesaminate periodicamente e aggiornate,ove necessario. L'adesione a Codici di condotta o a meccanismi di certificazione, può essere utilizzata come elemento per dimostrare il rispetto degli obblighi imposti al Titolare del trattamento;

- In caso di **contitolarità del trattamento**: i Contitolari devono stipulare tra loro uno specifico **accordo interno** che disciplini in modo trasparente le rispettive responsabilità e rifletta adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo va messo a disposizione

Obblighi ed adempimenti

Nomina Responsabile del Trattamento va documentata con un "***contratto o altro atto giuridico",*** stipulato in forma scritta anche su supporto elettronico, che regoli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

Ammessa la designazione di Sub-Responsabili previa autorizzazione scritta, specifica o generale del Titolare del trattamento.

Incaricati del trattamento: categoria di soggetti, identificata con le ***"persone autorizzate al trattamento"*** non è definita formalmente, ma disciplinata indirettamente. Viene previsto per il Titolare l'obbligo di indicare le persone autorizzate all'interno della sua struttura.

Il Responsabile della protezione dei dati
(Data Protection Officer)

La designazione del DPO è **obbligatoria** (da parte del Titolare o del Responsabile del trattamento) solo se:

1. il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali;
2. le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per natura, ambito di applicazione e/o finalità, richiedono **il monitoraggio regolare e sistematico degli interessati su larga scala;**
3. le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, **su larga scala**, di categorie particolari di dati di cui all'art. 9 o 10 del Regolamento (dati che rivelino l'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute o alla vita sessuale o orientamento sessuale, o dati relativi a condanne penali e a reati).

Il Responsabile della protezione dei dati

(Data Protection Officer)

Cosa si intende per MONITORAGGIO REGOLARE E SISTEMATICO"

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il considerando 24 menziona il "monitoraggio del comportamento di detti interessati" ricomprendendovi senza dubbio **tutte le forme di tracciamento e profilazione** su Internet anche per finalità di pubblicità comportamentale.

Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Il Responsabile della protezione dei dati

(Data Protection Officer)

Cosa si intende per MONITORAGGIO REGOLARE E SISTEMATICO*"(segue)*

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

Il Responsabile della protezione dei dati

(Data Protection Officer)

Cosa significa "su larga scala"?

Il regolamento non definisce cosa rappresenti un trattamento "su larga scala". Il Gruppo di lavoro WP29 raccomanda di tenere conto, in particolare, dei fattori qui elencati al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food*;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Il Responsabile della protezione dei dati

(Data Protection Officer)

Il DPO va designato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i propri compiti.

Può essere un dipendente del Titolare o del Responsabile del trattamento *oppure un consulente esterno che assolve i suoi compiti in base a un contratto* di servizi.

Un gruppo imprenditoriale può nominare un unico DPO.

I dati di contatto del DPO vanno comunicati al Garante per la protezione dei dati personali, al personale interno della Società e resi pubblici.

Il DPO deve essere autonomo ed indipendente:

- non deve ricevere dal Titolare o dal Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati né è soggetto a potere disciplinare o sanzionatorio per l'adempimento dei propri compiti;
- deve avere le risorse necessarie e il potere di spesa per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere le proprie conoscenze specialistiche (es. aggiornamento professionale).

Il Responsabile della protezione dei dati
(Data Protection Officer)

Il Regolamento individua icompiti assegnati al DPO:

- Informare e fornire al Titolare, al Responsabile nonché ai dipendenti che eseguono il trattamento, consulenza in merito agli obblighi normativi in materia;
- Sorvegliare l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche in materia del Titolare o del Responsabile del trattamento, compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale che partecipa al trattamento e al controllo in merito;
- Fornire, se richiesto, pareri sulla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- Cooperare con l'Autorità di controllo;
- Fungere da punto di contatto con il Garante per la protezione dei dati di personali per questioni connesse al trattamento.

L'INFORMATIVA ALL'INTERESSATO

L'informativa deve essere concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

L'Informativa **va resa per iscritto o con altri mezzi, anche elettronici.**

Anche **oralmente, purché sia richiesto dall'interessato e sia comprovata con** altri mezzi l'identità dell'interessato.

Le informazioni possono essere fornite anche in combinazione con **icone standardizzate per dare, in modo facilmente visibile, intelligibile e** chiaramente leggibile, un **quadro d'insieme del trattamento previsto. Se** presentate elettronicamente, le icone devono essere leggibili da qualsiasi dispositivo.

L'INFORMATIVA ALL'INTERESSATO *(segue)*

Elementi obbligatori da indicare nell'informativa privacy :

- l'identità ed i dati di contatto del titolare del trattamento e, ove applicabile del responsabile;
- **i dati di contatto della nuova figura del DPO, ove prevista;**
- **le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;**
- qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse del titolare del trattamento o di terzi, **la specificazione di quali siano i legittimi interessi perseguiti dal titolare del trattamento o** da terzi;
- gli eventuali destinatari e le eventuali categorie di destinatari dei dati pesonali;
- **l'ambito del trasferimento all'estero (ovviamente extra UE) o a** un'organizzazione internazionale dei dati personali

L'INFORMATIVA ALL'INTERESSATO *(segue)*

- il **periodo di conservazione dei dati personali oppure, se non è** possibile, i criteri utilizzati per determinare tale periodo;
- la **specifica esistenza del diritto alla portabilità dei dati;**
- l'esistenza del **diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata** sul consenso prestato prima della revoca;
- il diritto di **proporre reclamo al Garante per la protezione dei dati personali.**
- Nel caso in cui i dati personali oggetto del trattamento non siano raccolti presso l'interessato, l'informativa dovrà essere fornita al più tardi **entro un mese dall'ottenimento** dei dati o, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato o con un terzo, al più tardi al momento di tale comunicazione.

Il Consenso al trattamento dei dati

Il **consenso,** in base al nuovo Regolamento Generale (art. 4 GDPR), è qualsiasi **manifestazione di volontà libera, specifica, informata e** inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. Il presupposto indefettibile è che il soggetto che conferisce il consenso abbia la capacità giuridica per farlo.

In caso di trattamento di dati di minori, occorre acquisire il consenso dai genitori o dagli esercenti la patria potestà se l'interessato ha meno di 16 anni.

Inoltre, in base al Considerando 32: "*il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso*".

Il Consenso al trattamento dei dati *(segue)*

Caratteristiche del consenso:

Il consenso deve essere, quindi:

- inequivocabile;
- libero;
- specifico;
- informato;
- verificabile;
- revocabile.

Il Consenso al trattamento dei dati *(segue)*

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.

In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20).

Il Registro del Trattamento

Imprese o organizzazioni con numero di dipendenti pari o superiore a 250: deve essere redatto (anche in formato elettronico) sia dal Titolare che dal Responsabile del trattamento e **va esibito su richiesta** al Garante per la protezione dei dati personali;

Imprese **con meno di 250 dipendenti: obbligo di redazione se il** trattamento da esse svolto

(i) presenta un rischio per i diritti e le libertà dell'interessato;

(ii) non è occasionale o include dati personali “particolari”o relativi a condanne penali e reati.

Rappresenta l’elemento fondamentale in relazione all’obbligo di elaborare un **sistema documentale di gestione della privacy** contenente tutti gli atti, regolarmente aggiornati, redatti per soddisfare i requisiti di conformità al Regolamento ("***accountability"***)

Il Registro del Trattamento

Il Garante della Privacy ha pubblicato, sul proprio sito, le Faq sul Registro delle attività di trattamento (https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento) per chiarire alcuni dubbi in merito all'obbligatorietà, all'uso, alla compilazione e conservazione del registro stesso; inoltre, il Garante ha messo a disposizione due fac-simile di modelli di registro e nello specifico il modello semplificato delle attività di trattamento del titolare per PMI e il modello semplificato delle attività di trattamento del responsabile per PMI.

Il Garante per la protezione dei dati personali, nella Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali (http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali) dispone che: "*il registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali*", e invita tutti i titolari del trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a dotarsi di tale registro.

Il Registro del Trattamento

Il Garante per la protezione dei dati personali ha chiarito che devono redigere il registro, ad esempio:

- esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- il condominio ove tratti "categorie particolari di dati" (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Il Registro del Trattamento *(segue)*

Il Registro del Trattamento redatto dal **Titolare del trattamento contiene:**

a) Nome e dati di contatto del Titolare, contitolare, rappresentante del Titolare e DPO;

b) Finalità del trattamento;

c) Categorie di interessati e di dati personali;

d) Ambito di comunicazione**, anche verso Paesi terzi;**

e) Ove possibile, i termini ultimi per la cancellazione delle diverse categorie dei dati;

f) Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Il Registro del Trattamento *(segue)*

Il Registro del Trattamento tenuto dal **Responsabile del trattamento** contiene:

a) Nome e dati di contatto del/i Responsabile/i, del Titolare per cui egli agisce, del rappresentante del Titolare o del Responsabile e del DOP;

b) Categorie dei trattamenti effettuati per conto di ogni Titolare;

c) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale identificati e eventuali garanzie;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Esempio di Registro del Trattamento

Trattamento	Ufficio	Finalità	Tipo di dati personali	Categorie di interessati	consenso	informativa	conservazione	Misure di sicurezza tecniche ed organizzative	Contitolare del trattamento	Rappresentante del titolare	responsabile del titolare	Destinatari delle comunicazioni dei dati personali	Paese terzo o organizzazione internazionale

Diritti degli interessati

- **DECRETO LEGISLATIVO N.196/2003**
- **Art. 7 - Diritto dì accesso ai dati personali**
-
- **REGOLAMENTO UE 2016/679**
- **Art. 15 Diritto di Accesso dell'interessato**
- **Art. 16 Diritto di rettifica**
- **Art. 17 Diritto alla cancellazione (Diritto all'Oblio) non applicabile in virtù.**
- **Art. 18 Diritto di limitazione di trattamento**
- **Art. 19 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento**
- **Art. 20 Diritto alla portabilità dei dati**
- **Art. 21 Diritto di opposizione**

Il Soggetto interessato, inoltre, ha **diritto di proporre reclamo all'Autorità di Controllo** (Garante della Privacy).

Diritti dell'interessato

Diritto All'oblio

In assenza delle suddette condizioni, il trasferimento è ammesso **soltanto se si verifica una delle seguenti condizioni:**

a) l'interessato, debitamente informato, abbia **acconsentito esplicitamente al** trasferimento;

b) il trasferimento sia necessario all'esecuzione di un **contratto o all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;**

c) il trasferimento sia necessario alla conclusione o esecuzione di un **contratto** stipulato tra il Titolare e un terzo **a favore dell'interessato;**

d) il trasferimento sia necessario per importanti **motivi di pubblico interesse;**

e) il trasferimento sia necessario per accertare, esercitare o difendere un **diritto in sede giudiziaria;**

f) il trasferimento sia necessario per **tutelare gli interessi vitali dell'interessato o di terzi, qualora l'interessato si trovi nell'impossibilità fisica o giuridica di prestare** consenso;

g) il trasferimento sia effettuato a partire da un **registro pubblico.**

Il Trasferimento dei dati personali all'estero

Con il nuovo Regolamento **il legislatore europeo ha ampliato la sfera soggettiva di protezione dei dati trasferiti all'estero**, stabilendo che non si considerano destinatari solo i Paesi terzi (e tutte le imprese ivi sono stabilite) ma **anche le Organizzazioni Internazionali** (definite all'articolo 4, comma 26 del Regolamento, come "*un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro istituto da o sulla base di un accordo tra due o più stati*").

Viene inoltre attuato un **ampliamento della sfera di protezione dal punto di vista temporale**: ex articolo 44, affinché si integri un trasferimento all'estero di dati, non è necessario che essi vengano trattati immediatamente al momento dei trasferimento, ma basta che siano "***destinati a essere oggetto*** *di un trattamento* ***dopo il trasferimento*** *verso un paese terzo o un'organizzazione internazionale,* ***compresi i trasferimenti successivi di dati personali*** *da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale*".

Il Trasferimento dei dati personali all'estero

Il Regolamento non introduce particolari novità

Condizioni di liceità:

- **trasferimento sulla base di una decisione di adeguatezza (ove la Commissione** UE abbia deciso che il Paese terzo, un territorio o uno o più settori specifici all'interno del Paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato; in tal caso il trasferimento non necessita di autorizzazioni specifiche);
- **trasferimento soggetto a garanzie adeguate** (il Titolare o il Responsabile del trattamento può trasferire dati personali verso un Paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate, come ad esempio le norme vincolanti d'impresa, le clausole contrattuali standard, l'esistenza di un codice di condotta, l'esistenza di un meccanismo di certificazione, specifiche clausole contrattuali)

Il Trasferimento dei dati personali all'estero

In assenza delle suddette condizioni, il trasferimento è ammesso **soltanto se si verifica una delle seguenti condizioni:**

a) l'interessato, debitamente informato, abbia **acconsentito esplicitamente al** trasferimento;

b) il trasferimento sia necessario all'esecuzione di un **contratto o all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;**

c) il trasferimento sia necessario alla conclusione o esecuzione di un **contratto** stipulato tra il Titolare e un terzo **a favore dell'interessato;**

d) il trasferimento sia necessario per importanti **motivi di pubblico interesse;**

e) il trasferimento sia necessario per accertare, esercitare o difendere un **diritto in sede giudiziaria;**

f) il trasferimento sia necessario per **tutelare gli interessi vitali dell'interessato o di terzi, qualora l'interessato si trovi nell'impossibilità fisica o giuridica di prestare** consenso;

g) il trasferimento sia effettuato a partire da un **registro pubblico.**

Il regime sanzionatorio previsto dal GDPR

Art. 83 **Condizioni generali per infliggere sanzioni amministrative pecuniarie**

Art. 84 **Delega agli stati membri ad adottare norme che prevedono sanzioni per violazioni non richiamate dal Regolamento**

Il regime sanzionatorio previsto dal GDPR

Principali innovazioni:

- **Innalzamento rilevante delle sanzioni con la previsione di un tetto massimo, ma non di un tetto minimo che potrà essere previsto dai singoli Stati membri**
- **Alternatività della sanzione pecuniaria e dei poteri correttivi dell'Autorità di controllo (art. 58 parag 2 lettera da a) ad h) e J: avvertimenti, ammonizioni , ingiunzioni limitazioni, ecc)**
- **Inserimento della violazione di tutti i principi e tutti gli obblighi tra gli illeciti amministrativi**

Il regime sanzionatorio previsto dal GDPR

Art. 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. **Principio di proporzionalità** delle sanzioni amministrative pecuniarie inflitte a seguito delle violazioni del Regolamento
2. Sanzioni **effettive, proporzionate e dissuasive**
3. **Valutazione caso per caso** con riferimento alle circostanze concrete che si presentano
4. Sanzioni comminate in aggiunta o in luogo delle misure previste dall'art. 58 co 2 , avvertimenti, ammonimenti al titolare, ingiunzioni, a soddisfare le richieste dell'interessato o a conformare il trattamento dei dati alle disposizioni del regolamento, limitazioni provvisorie o definitive al trattamento dei dati personali

Il regime sanzionatorio previsto dal GDPR

Art. 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie *(segue)*

1. **Sanzione pecuniaria alle persone fisiche**: il principio di proporzionalità è ulteriormente specificato ed è adattarsi massimamente al caso di specie al fine di conseguire proporzionalità delle sanzioni amministrative pecuniarie in concreto e non semplicemente in astratto. (Considerando 148)

   Se la sanzione pecuniaria è un onere sproporzionato per la persona fisica è ammessa la possibilità di rivolgerle un ammonimento

Il regime sanzionatorio previsto dal GDPR

Art. 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie (segue)

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso **effettive, proporzionate e dissuasive**.

2. Le sanzioni amministrative pecuniarie sono inflitte, **in funzione delle circostanze di ogni singolo** caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di **decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi**:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

Il regime sanzionatorio previsto dal GDPR

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

f) le categorie di dati personali interessate dalla violazione;

g) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

h) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

i) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;

j) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Il regime sanzionatorio previsto dal GDPR
Sanzioni § 4 art. 83

Paragrafo 4. art. 83

In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a **sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore**:

- a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli:
  - 8 Consenso dei minori in relazione alla società di servizi di informatica
  - 11 Trattamento che non richiede l'identificazione
  - 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
  - 26 Contitolari del trattamento
  - 27 Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione
  - 28 Responsabile del trattamento
  - 29 Trattamento sotto l'autorità del trattamento o del responsabile del trattamento
  - 30 Registri delle attività di trattamento
  - 31 Cooperazione con l'autorità di controllo
  - 32 Sicurezza del trattamento
  - 33 Notifica di una violazione dei dati personali all'autorità di controllo
  - 34 Comunicazione di una violazione dei dati personali dell'interessato
  - 35 Valutazione d'impatto sulla protezione dei dati
  - 36 Consultazione preventiva
  - 37 Designazione del responsabile della protezione dei dati (DPO)
  - 38 posizione del responsabile della protezione dei dati
  - 39, Compiti del responsabile della protezione dei dati
  - 42 Certificazione
  - 43 Organismi di certificazione
- b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;
- c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

Il regime sanzionatorio previsto dal GDPR
Sanzioni § 5 art. 83

In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a **sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore**:

a) I principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli:
   - 5 Principi applicabili al trattamento di dati personali
   - 6 Liceità del trattamento
   - 7 Condizioni per il consenso
   - 9 di dati

b) i diritti degli interessati a norma degli articoli da
   - 12 Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato
   - 13 Informazioni ida fornire qualora i dati personali siano raccolti presso l'interessato
   - 14 Informazioni da fornire qualora i dati personali non siano ottenuti dall'interessato
   - 15 Diritti d'accesso dell'interessato
   - 16 Diritto di rettifica
   - 17 Diritto alla cancellazione (Diritto all'oblio)
   - 18 Diritto di limitazione di trattamento
   - 19 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento
   - 20 Diritto alla portabilità dei dati
   - 21 Diritto di opposizione
   - 22 Processo decisionale automatizzato relativo alle persone fisiche compresa la profilazione

Il regime sanzionatorio previsto dal GDPR
Sanzioni § 5 art. 83 *(segue)*

In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a **sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:**

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli:
   - 44 Principio generale per il trasferimento
   - 45 Trasferimento sulla base di una decisione di adeguatezza
   - 46 trasferimento soggetto a garanzie adeguate
   - 47 norme vincolanti d'impresa
   - 48 Trasferimento o comunicazione non autorizzati dal Diritto dell'unione
   - 49 Deroghe in specifiche situazioni

c) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX (Disposizioni relative a specifiche situazioni di trattamento);

d) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

La responsabilità da illecito trattamento dei dati personali nel Regolamento Europeo

Il **Titolare** del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che **violi il presente regolamento.**

Il **Responsabile** del trattamento risponde per il danno causato dal trattamento solo se:

- **non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento**
- **ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento**.

La responsabilità da illecito trattamento dei dati personali nel Regolamento Europeo

Articolo 82 Diritto al risarcimento e responsabilità

Esonero della responsabilità (art. 82 co. 3)

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso **non gli è in alcun modo imputabile.**

Inversione dell'onore della prova: obbligo di dimostrare che l'evento dannoso non è imputabile o a carico del Titolare/responsabile

La responsabilità da illecito trattamento dei dati personali nel Regolamento Europeo

Articolo 82 Diritto al risarcimento e responsabilità

Responsabilità solidale

4. **Qualora più titolari del trattamento o responsabili del trattamento** oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, **responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.**

   (Compartecipazione attiva od omissiva all'evento di danno, apportatore delle conseguenze pregiudizievoli – importanza della ripartizione chiara delle istruzioni per il responsabile)

Azione di regresso

5. Qualora **un titolare del trattamento o un responsabile del trattamento abbia pagato**, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento **ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti** nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2. (quota di responsabilità)

   Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Il Professionista e la privacy..la “*pratica*”

Il Professionista e la privacy..la "*pratica*"

Il professionista, in relazione alla gestione della privacy, può rivestire un duplice ruolo:

A. Titolare del proprio studio professionale
B. Consulente per i clienti

Ne consegue che a seconda del ruolo rivestito assume una differente qualifica ai fini privacy con i conseguenti e correlati adempimenti da porre in essere.

Il Professionista e la privacy..la "*pratica*"

Qualche spunto di riflessione sul ruolo del commercialista in ambito privacy può essere tratto dalla nota del 22 gennaio 2019 emessa dalla stessa Autorità in risposta a un quesito posto il 24 settembre 2018 dal Consiglio Nazionale dei Consulenti del Lavoro, proprio in ordine **alla duplice identificazione dello stesso quale Titolare autonomo o Responsabile del trattamento.**

Nella nota a chiarimento il Garante ha affermato che, in via preliminare, occorre distinguere il segmento di attività in cui il Consulente del Lavoro tratta i dati dei propri dipendenti ovvero dei propri clienti nella sua qualità di professionista, dalla diversa attività per la quale il medesimo soggetto tratta i dati dei dipendenti del proprio cliente.

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9080970

Il Professionista e la privacy..la "*pratica*"

Dunque i consulenti del lavoro sono "**titolari**" quando trattano, in piena autonomia e indipendenza, i dati dei propri dipendenti oppure dei propri clienti quando siano persone fisiche, come ad esempio i liberi professionisti determinando puntualmente le finalità e i mezzi del trattamento. Sono, viceversa, "**responsabili**" quando trattano i dati dei dipendenti dei loro clienti sulla base dell'incarico ricevuto, che contiene anche le istruzioni sui trattamenti da effettuare. E' il caso, ad esempio, dei consulenti che curano per conto di datori di lavoro la predisposizione delle buste paga, le pratiche relative all'assunzione e al fine rapporto, o quelle previdenziali e assistenziali, trattando una pluralità di dati personali, anche sensibili, dei lavoratori.

Si tratta di informazioni raccolte e utilizzate dai datori di lavoro in base al contratto e a norme di legge e di regolamento (come quelle in materia di lavoro, previdenza e assistenza sociale), e che vengono gestite dai consulenti cui sono esternalizzati i servizi sulla base delle discipline di settore e delle regole deontologiche pertinenti. Ed è sul contratto di affidamento dell'incarico e di designazione a responsabile del trattamento da parte del cliente che si basa la legittimità dei trattamenti realizzati dal consulente.

Il Garante ha chiarito infine che ai consulenti, pur in qualità di "responsabili" del trattamento, viene riconosciuto un apprezzabile margine di autonomia e correlativa responsabilità anche con riguardo alla individuazione e predisposizione di idonee misure di sicurezza, sia tecniche che organizzative, a tutela dei dati personali trattati.

Il Professionista e la privacy..la "*pratica*"

La figura del Consulente *privacy* per l'assistenza ai soggetti obbligati come individuato dal DOCUMENTO DI RICERCA dell'ODEC del 30 NOVEMBRE 2022

L'avvento del GDPR ha imposto all'attenzione degli operatori economico-giuridici una nuova figura professionale, quella del ***consulente privacy*** *("data protection specialist", o anche "privacy officer").*

L'importanza strategica di tale figura è evidente alla luce della necessità delle aziende di adeguarsi correttamente alla normativa in commento, garantendo la tutela dei diritti e della dignità nel trattamento dei dati personali dei soggetti interessati e, al contempo, la libera circolazione dei dati per legittimo interesse di business.

In effetti il consulente privacy sembra essere una figura necessaria all'interno di qualsiasi azienda, dal momento che l'adeguamento al GDPR implica, da un lato, una conoscenza approfondita della particolare branca del diritto rivolta alla protezione dei dati personali e, dall'altro, l'adozione di procedure di risk assessment finalizzate alla individuazione delle misure di sicurezza più appropriate da adottare.

Rispetto al DPO, il consulente privacy si pone quale interlocutore qualificato per conto dell'azienda, fermo restando che gli adempimenti privacy devono essere espletati esclusivamente dai soggetti individuati dal GDPR (titolare, eventuale contitolare e responsabile del trattamento).

Il Professionista e la privacy..la "*pratica*"

TIPOLOGIA ADEMPIMENTO	SI/NO	NOTE
INFORMATIVA	si	Utilizzo di un linguaggio semplice e chiaro e il trattamento dei dati personali deve essere corretto e trasparente
CONSENSO	Si/no	a) Non è richiesto il consenso per le finalità che sono attinenti al conseguimento della prestazione d'opera intellettuale richiesta. b) Il consenso è richiesto per il conseguimento di finalità ulteriori e diverse rispetto alla prestazione richiesta (vedi marketing, profilazione, etc..) c) Stabilire procedure ben definite per il rilascio del consenso e per la revoca dello stesso, per il diritto di accesso ai propri dati, cancellazione e oblio, rettifica, limitazione. d) Lo studio garantisce di rispondere a queste richieste in un tempo ragionevole.(entro 1 mese)
REGISTRO TRATTAMENTO	Si	La norma prevede che il registro venga redatto solo per aziende il cui numero di dipendenti sia di 250; è ipotizzabile quindi l'uso del registro dei trattamenti sicuramente per studi associati; è a discrezione del singolo PROFESSIONISTA redigere o meno il registro.(CONSIGLIATO PER ADEMPIMENTO ACCOUNTABILITY). Vedasi le indicazioni fornite dal Garante della Privacy il quale ne suggerisce l'adozione.
DPIA	Si	Art.35 Gdpr, quando un tipo di trattamento, allorché prevede l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto,le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare prima di procedere al trattamento effettua una valutazione d'impatto. Tale rischio risulta essere presente soprattutto quando siamo dinanzi a dati giudiziari, minori, incapaci, origini razziali, credo religioso,appartenenza sindacale, etc.. QUINDI RISULTA FORTEMENTE CONSIGLIATO Ci sono dei parametri definiti per la valutazione del rischio? Quali sono le misure tecniche volte a prevenire ogni categoria di rischio?
NOMINA DPO	Si/no	Il gdpr regola tale nomina per le aziende con 250 dipendenti; tale figura potrebbe essere d'aiuto nell'applicazione di tale normativa, oltre ad essere utile nel dimostrare l'accountability del titolare.
CONTRATTI RESPONSABILI DEL TRATTAMENTO	Si/No	Ai sensi dell'art.28 Gdpr, la nomina di un responsabile del Trattamento avviene per contratto o da altro atto giuridico. Tale nomina risulta obbligatoria solo qualora il trattamento debba essere fatto per conto del Titolare

Il Professionista e la privacy..la "*pratica*"

DESIGNATI	Si/No	Designati tramite nomina ad hoc
DATA BREACH	Si	Ai sensi dell'art.33 del Gdpr, una eventuale violazione dei dati personali deve essere notificata dal Titolare del Trattamento all''Autorità Garante entro 72 ore dalla venuta conoscenza, senza ingiustificato ritardo, salvo che tale violazione non presenti rischi per i diritti e le libertà delle persone fisiche. Quali sono le misure di sicurezza volte a prevenire eventuali data breach? Vengono poste delle misure informatiche e fisiche al fine di evitare data breach? (password personali non accessibili ad altri, da inserire nei rispettivi pc per poter accedere alle informazioni riservate, pseudonimizzazione dei faldoni cartacei; porre in essere tutte le misure tali da far si che i clienti non possano entrare in contatto direttamente o indirettamente con eventuali nominativi di altri clienti. Ricevere i clienti in orari separati. Il personale dipendente viene formato per prevenire eventuali violazioni? Come e dove avviene la conservazione dei fascicoli personali dei relativi clienti. Dove avviene la conservazione e l'utilizzo delle penne usb, e chi ne dispone.
TRATTAMENTO DATI ALL'ESTERO	Si	Ai sensi dell'art.44 del Gdpr è possibile il trasferimento dei dati trattati all'estero, soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni del presente capo e le altre disposizioni del presente Regolamento.
MISURE TECNICHE ED ORGANIZZATIVE	Si	Ai sensi dell'art.32 del Gdpr il Titolare del Trattamento e il Responsabile del Trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte e dei costi di attuazione. Le misure tecniche ed organizzative devono essere tali da consentire un adeguato livello di tutela e sono: a) garanzia di riservatezza, integrità,disponibilità, b) pseudonimizzazione e cifratura dei dati personali c) capacità di ripristinare tempestivamente la disponibilità e l' accesso ai dati personali in caso di incidente fisico o tecnico d) attraverso periodici penetrations test verificare il livello di affidabilità dei propri sistemi di sicurezza e) aderire ad un codice di condotta, se presente, relativo alla propria categoria professionale.
MONITARE I RISCHI ON LINE	Si	**SERVIZI CLOUD** PER CONSERVARE E CONDIVIDERE I DATI.L'UTILIZZO DEVE ESSERE INDICATO NELL'INFORMATIVA E CHIARIRE SE VI E' UN TRASFERIEMNTO DI DATI ALL'ESTERO. COLUI CHE SI OCCUPA DELLA GESTIONE DEL SERVIZIO VIENE INDIVIDUATO QYUALE RESPONSABILE ESTERNO **SITO WEB.** PREDISPORRE COOKIE POLICY, INFORMATIVA E CONSENSO , INSERIRE TALE ATTIVITA' NEL REGISTRO DEI TRATTAMENTI.

Il Professionista e la privacy..la "*pratica*"

Tipologia di trattamento

1. Contabilità dello studio
1. Contabilità Clienti e Fornitori
1. Selezione del personale
1. Gestione dei dipendenti/collaboratori dello Studio
1. Gestione adempimenti sicurezza e salute sui luoghi di lavoro e sorveglianza sanitaria
1. Formazione del personale
1. Dichiarazione dei redditi persone fisiche
1. Consulenza finanziaria società di persone e ditte individuali e professionisti
1. Attività di Sindaco/Revisione
1. Obblighi di adeguata verifica della clientela
1. Consulenza in materia tributaria
1. Invio newsletter
1. Gestione IT studio
1. Sito internet studio
1. Invii telematici delle dichiarazioni fiscali
1. Elaborazione dati contabili per conto dei clienti
1. Elaborazioni paghe per conto clienti
1. Trattamento dati quale membro di un ODV

Ruolo del professionista

TITOLARE DEL TRATTAMENTO

RESPONSABILE DEL TRATTAMENTO

AUTORIZZATO AL TRATTAMENTO