Cliens

Privacy

IL NUOVO REGOLAMENTO PRIVACY

Vademecum

a cura di Giuseppe Vaciago e Stefano Ricci

MVLTA PAVCIS AG

GIUFFRÈ EDITORE

Cliens
Privacy

IL NUOVO REGOLAMENTO PRIVACY

A chi si rivolge

Il Nuovo Regolamento si applica a tutti i soggetti (anche extra UE) che offrono servizi a cittadini UE.

Principio di ***accountability***

Il titolare del trattamento deve rispettare la normativa e deve essere in grado di dimostrarlo:

- **responsabilizzazione**, attuare proattivamente misure efficaci
- **rendicontazione**, darne dimostrazione

Approccio basato sul **rischio**

Il titolare del trattamento deve condurre una ***gap analysis*** e, nei casi di trattamento a maggiore impatto sui diritti e le libertà degli interessati, condurre un vero e proprio *privacy impact assessment.*

Trasparenza e legittimità del trattamento di dati personali

Obbligo di rendere l'**informativa** e di valutare la **base legale** del trattamento.

I diritti degli interessati

Obbligo di dare riscontro **entro un mese in forma scritta.**
Diritto di accesso, limitazione, cancellazione (oblio), portabilità.

Attraverso l'adesione a **codici deontologici** ovvero l'adesione a **schemi di certificazione** il responsabile può dimostrare le "garanzie sufficienti" di cui all'art. 28, paragrafi 1 e 4.

Per quanto concerne i **codici deontologici**, il Garante sta valutando quelli attualmente vigenti per alcune tipologie di trattamento nell'ottica dei requisiti fissati nel regolamento (art. 40).

Per quanto concerne **gli schemi di certificazione** occorrerà attendere anche l'intervento del legislatore nazionale che dovrà stabilire alcune modalità di accreditamento dei soggetti certificatori.

LA MAPPA DEI SOGGETTI CHE ACCEDONO AI DATI - I

Titolare (art. 24) - Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. Deve adottare policy adeguate in materia di protezione dei dati personali. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Con-titolare (art. 26) - In caso di condivisione in ordine a finalità e modalità del trattamento, il Regolamento impone ai titolari di definire con uno specifico atto il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente.

Rappresentante (art. 27) - Il titolare o il responsabile non stabilito nell'Ue dovrà designare un rappresentante in Italia.

Responsabile (art. 28) - Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento 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. L'accordo per il trattamento dei dati personali deve contenere l'indicazione della natura, durata e finalità del trattamento o dei trattamenti assegnati, e le categorie di dati oggetto di trattamento, oltre le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare.

Cliens
Privacy

LA MAPPA DEI SOGGETTI CHE ACCEDONO AI DATI - II

Sub-responsabile (sub art. 28) - Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile

Amministratore di sistema - Figura non prevista espressamente dal Regolamento.

Soggetti autorizzati (art. 29) - 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. Pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex art. 30 Codice Privacy), il Regolamento non ne esclude la presenza facendo genericamente riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile».

Data Protection Officer - Il titolare del trattamento deve nominarlo obbligatoriamente se è (i) un soggetto pubblico; (ii) se è un soggetto pubblico o privato che come attività principale svolge attività implicanti monitoraggio regolare e sistematico di interessati su larga scala; (ii) se è un soggetto pubblico o privato che come attività principale svolge attività implicanti trattamenti di dati particolari (ex sensibili) e/o dati giudiziari su larga scala.

LARGA SCALA: cosa riguarda

- Numero degli interessati
- Quantità dei dati
- Durata e permanenza del trattamento
- Ambito geografico

Il trattamento di dati personali **NON** dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati (Considerando 91).

Cliens
Privacy

LA MAPPA DELLE ATTIVITÀ
REGISTRO DEL TRATTAMENTO

La tenuta del registro dei trattamenti è prevista dall'articolo 30 del GDPR, ed è considerata indice di una corretta gestione dei trattamenti. tale registro che può essere in formato telematico dovrà essere messo a disposizione dell'Autorità Garante qualora lo richieda e permette di:

- tenere traccia delle operazioni di trattamento effettuate all'interno del singolo Studio professionale;
- censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un efficace «ciclo di gestione» dei dati personali.

Cosa deve contenere il registro del trattamento dati

- Il nome e i dati di contatto del titolare del trattamento e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- Le finalità del trattamento;
- La descrizione delle categorie di interessati e delle categorie di dati personali;
- Le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
- Se presenti, i trasferimenti di dati personali verso paesi terzi e la loro identificazione;
- I termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative.

Obbligatorietà

Nel caso in cui lo Studio professionale **superi i 250 dipendenti** o, pur avendo un numero inferiore di addetti, effettui un tipo di trattamento che possa presentare un **rischio per i diritti e le libertà dell'interessato**, quando questo trattamento non sia occasionale o includa il trattamento delle **categorie particolari di dati.**

Gli Studi professionali trattando dati giudiziaria rientrano in tale obbligo. Inoltre, il Garante per la Protezione dei dati personali si è recentemente espresso consigliando espressamente la tenuta del registro anche per i soggetti giuridici che non rientrassero in tale categoria.

Cliens
Privacy

MISURE DI SICUREZZA

Secondo quanto previsto dall'art. 32 del GDPR, il titolare e il responsabile del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio, **devono adottare le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**.

Esiste un elenco di tali misure di sicurezza che il titolare o il responsabile del trattamento devono adottare?

No. L'art. 32 del GDPR elenca una lista aperta e non esaustiva di misure che dovrebbero comprendere:

- la **pseudonimizzazione** e la **cifratura** dei dati personali;
- la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;
- la capacità di **ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per **testare**, **verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

Ciò vuol dire, in concreto, che spetta, sulla base del principio dell'*accountability*, al titolare del trattamento stabilire quali siano le misure adeguate. L'elenco previsto nel disciplinare tecnico dell'allegato B del Codice della Privacy può essere un punto di riferimento, ma non è più un obbligo di legge.
Per questa ragione è consigliabile che il titolare di uno Studio Professionale faccia svolgere con regolarità un *risk assesment* sulle misure tecnico informatiche ad un consulente informatico esperto in *cybersecurity*.

DATA BREACH

In caso di violazione dei dati personali a seguito di attacco informatico o anche alterazione del dato, il titolare del trattamento notifica tale violazione all'Autorità Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Cosa deve contenere la notifica?

- Descrivere la **natura della violazione dei dati personali** compresi, ove possibile, le categorie e il numero approssimativo di interessati colpiti, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- Comunicare il **nome e i dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto;
- Descrivere le **probabili conseguenze della violazione dei dati personali**;
- Descrivere le **misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per **porre rimedio alla violazione** dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Comunicazione all'interessato

Va sempre comunicato il ***data breach*** agli interessati i cui dati personali sono stati violati tranne se:

a) il titolare del trattamento **ha messo in atto le misure tecniche e organizzative adeguate di protezione** e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento **ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati**;

c) **detta comunicazione richiederebbe sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

NOTE