REGOLAMENTO EU 679/2016

RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI E CHE ABROGA LA DIRETTIVA 95/46/CE (REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI)

Nota introduttiva

Il presente testo è stato redatto utilizzando la versione italiana del Regolamento Europeo 679/2016, meglio noto in lingua anglosassone come GDPR - General Data Protection Regulation.

Pertanto, a beneficio del lettore, si ricorda che la denominazione delle figure chiave disciplinate dal suddetto Regolamento sono state tradotte, nella versione italiana della normativa, come segue:

- *Controller:* Titolare del Trattamento
- *Processor:* Responsabile del Trattamento
- *Data Protection Officer (DPO):* Responsabile della Protezione dei Dati (RPD)

1. Oggetto del Regolamento

Il regolamento EU 679/2016 è il nuovo regolamento europeo sul trattamento dei dati personali: esso disciplina il trattamento e la protezione dei dati personali ad opera di enti privati o pubblici.

2. Ambito territoriale di applicazione

Il regolamento EU 679/2016 è direttamente applicabile in ciascuno degli Stati membri dell'Unione Europea.

3. Norme applicabili

Il regolamento EU 679/2016 è vincolante ed obbligatorio in ogni sua parte: non è possibile per nessuno degli Stati membri derogare a quanto stabilito dal regolamento.

4. Entrata in vigore del Regolamento

Il regolamento EU 679/2016 entrerà in vigore dal giorno 25 Maggio 2018.

5. Applicabilità del Regolamento agli studi medici ed odontoiatrici.

Poiché sia gli studi medici che quelli odontoiatrici, nello svolgimento dell'attività professionale, trattano i dati personali dei propri pazienti, essi sono tenuti al rispetto di quanto prescritto dal regolamento EU 679/2016. A titolo esemplificativo e non esaustivo: adeguamento della modulistica di raccolta dati, misure di sicurezza e protezione dei dati, misure di controllo d'accesso ai dati, tenuta del registro delle attività,

eventuale nomina di un Responsabile del Trattamento dei Dati, eventuale nomina di un Responsabile della Protezione dei Dati.

6. La nuova figura introdotta dal Regolamento EU 679/2016: il Responsabile della Protezione dei Dati

Il Responsabile della Protezione dei Dati è una nuova figura introdotta dal Regolamento EU 679/2016. Tale figura, ove prevista, deve essere nominata dal Titolare e dal Responsabile del Trattamento.

7. Soggetti obbligati alla nomina di un Responsabile della Protezione dei Dati

In accordo a quanto prescritto dal regolamento EU 679/2016 la nomina del Responsabile della Protezione dei Dati è obbligatoria per tutte le autorità pubbliche e per tutti coloro i quali esercitano attività che richiedono per loro natura il monitoraggio regolare e sistematico degli interessati su larga scala, così come per tutti coloro i quali esercitano attività comportanti il trattamento su larga scala di particolari categorie di dati, tra i quali anche i dati sanitari.

Tuttavia il regolamento EU 679/2016 non fornisce una definizione precisa del concetto di *larga scala,* ma si limita ad esemplificare, nei *Considerando,* alcuni casi nei quali il trattamento non dovrebbe essere ritenuto su larga scale: in particolare, il *Considerando 91,* suggerisce che: " […] 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 […]. Se ne evince che negli studi medici ed odontoiatrici ove sia presente un singolo titolare non sia da ritenersi obbligatoria la nomina di un Responsabile della Protezione dei Dati.

E' d'uopo tuttavia sottolineare che, in attesa di un intervento chiarificatore ad opere del Garante della Protezione dei Dati e/o del Legislatore sul predetto punto, la parte restante del Regolamento EU 679/2016 rimane pacificamente applicabile.

Infine è bene ricordare che, anche ove non sia obbligatorio procedere alla nomina di un Responsabile della Protezione dei Dati, è comunque possibile optare per la stessa.

8. Principali funzioni del Responsabile della Protezione dei Dati

I compiti principali del Responsabile della Protezione dei Dati sono:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento;
- sorvegliare l'osservanza dello stesso e delle altre disposizioni di legge relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e cooperare con l'autorità di controllo; fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

In sintesi, i compiti del Responsabile della Protezione dei Dati riguardano da un lato coadiuvare il titolare ed il responsabile del trattamento nell'applicazione di quanto prescritto dal regolamento EU 679/2016, e dall'altro fungere da raccordo tra essi e l'autorità preposta al controllo.

9. Compiti specifici riguardanti la sicurezza del Responsabile della Protezione dei Dati

Per quanto concerne l'adeguamento ed il costante aggiornamento di quanto prescritto dal regolamento EU 679/2016, i principali compiti spettanti al Responsabile della Protezione dei Dati sono:

- effettuare in via preliminare una valutazione del rischio volta ad individuare le problematiche relative alla gestione ed alla sicurezza dei dati personali detenuti dal titolare del trattamento;
- individuare ed indicare quali soluzioni adottare per adeguare la struttura agli standard di sicurezza richiesti dal regolamento EU 679/2016. A titolo esemplificativo e non esaustivo: pseudonimizzazione, crittografia, controllo degli accessi, minimizzazione dei dati, integrità dei dati, copie di sicurezza;
- individuare ed indicare al titolare quali soluzioni adottare per consentire agli interessati l'esercizio dei diritti connessi ai propri dati;
- redigere e aggiornare periodicamente il registro delle attività di trattamento, ove il titolare e/o il responsabile ritengano di delegare tale compito;
- pianificare controlli ed interventi regolari per rilevare tempestivamente problematiche emergenti ed aiutare il titolare ad individuare interventi appropriati per porvi rimedio: il compito del Responsabile della Protezione dei Dati Personali è dunque un compito destinato a protrarsi nel tempo, si tratta infatti di un controllo periodico, continuo e sistematico su specifiche attività o vulnerabilità, alle quali il titolare del trattamento dovrà porre rimedio in accordo a quanto suggerito dal Responsabile della Protezione dei Dati.

10. Responsabile della Protezione dei Dati: interno o esterno?

Il regolamento EU 679/2016 prevede che: "Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi".

Pertanto il Regolamento consente di nominare un Responsabile della Protezione dei Dati sia interno, affidando tale incarico ad una persona già presente nella struttura, sia esterno, avvalendosi di un terzo.

11. Qualifiche professionali del Responsabile della Protezione dei Dati

Il regolamento EU 679/2016 non indica i requisiti formali necessari per ricoprire il ruolo di Responsabile della Protezione dei Dati, si limita soltanto ad indicare che deve le avere qualità professionali adeguate al compito da svolgere.

12. Titolare del Trattamento

Il regolamento EU 679/2016 definisce all'art. 4, punto 7) il Titolare del Trattamento come: " la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri,

determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".

Pertanto Il Titolare del Trattamento è colui il quale decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali, compreso l'obbligo di notifica al Garante nei casi previsti. Tra questi obblighi è importante ricordare che il titolare del trattamento deve porre in essere misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato.

In sostanza il Titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati.

13. Contitolari del Trattamento

È possibile che coesistano più Titolari del Trattamento che decidono congiuntamente di trattare i dati per una finalità comune: gli interessati possono, in tal caso, rivolgersi indifferentemente ad uno qualsiasi dei contitolari per l'esercizio dei propri diritti.

Nel caso vi sia una situazione di contitolarità del trattamento il Regolamento stabilisce che essi debbano determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento stesso: Il contenuto essenziale di tale accordo deve essere messo a disposizione dell'interessato.

14. Responsabile del Trattamento

Il Regolamento EU 679/2016 definisce all'art. 4, punto 8) il Responsabile del Trattamento come: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

Si tratta quindi di quel soggetto al quale viene affidato, da parte del titolare, il trattamento dei dati personali.

È opportuno sottolineare come, nel caso il Titolare del Trattamento decida di avvalersi di un Responsabile del Trattamento, sia necessario provvedere a regolare il loro rapporto tramite un contratto o un altro atto giuridico. Tale atto o contratto dovrà contenere almeno le indicazioni prescritte dall'art 28, paragrafo 3 del Regolamento EU 679/2016.

15. Rapporto tra il Titolare del Trattamento ed il Responsabile della Protezione dei Dati

Il regolamento EU 679/2016 specifica chiaramente che la responsabilità per eventuali violazioni della normativa sulla protezione dei dati personali incombe esclusivamente sul Titolare del Trattamento ed eventualmente sul Responsabile del Trattamento: il Responsabile della Protezione dei Dati infatti, fatte

salve le ipotesi di eventuali illeciti contrattuali e/o extracontrattuali ad egli addebitabili nei confronti del Titolare del Trattamento, non risponde riguardo la violazione di quanto prescritto dal Regolamento.

16. Registri delle attività di trattamento

Il regolamento EU 679/2016 obbliga il Titolare ed il Responsabile di un trattamento sui dati alla tenuta del relativo registro delle attività di trattamento svolte. Tale documento deve contenere:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del Regolamento EU 679/2016, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

In sintesi si tratta di un registro dove vengono descritte le attività svolte sui dati personali, i soggetti autorizzati a svolgerle, le finalità e la tipologia di trattamento, il tempo di conservazione, le misure di sicurezza adottate e ogni altra informazione utile riguardo il trattamento effettuato.

L'obbligo di tenuta del registro incombe sia sul titolare che sul responsabile: tuttavia tale attività, come detto in precedenza, può essere delegata al Responsabile della Protezione dei Dati, ove si sia provveduto a nominarne uno.

17. Vademecum degli adempimenti minimi per i professionisti medici ed odontoiatri.

Il regolamento EU 679/2016 si applica integralmente agli studi medici ed odontoiatrici, i quali dovranno provvedere, come minimo e con urgenza:

1- a disciplinare con atto o contratto i rapporti tra più Titolari in caso di contitolarità del trattamento;
2- alla nomina di un Responsabile del Trattamento dei Dati ove necessario;
3- alla nomina di un Responsabile della Protezione dei Dati ove lo studio presenti più di un titolare, nel caso invece l'attività sia svolta dal singolo professionista tale nomina è facoltativa;
4- a comunicare al Garante per la Protezione dei Dati Personali il nominativo del Responsabile della Protezione dei Dati;
5- ad adeguare la propria struttura alla misure di sicurezza prescritte dal Regolamento EU 679/2016;

6- ad adeguare la propria struttura ai principi contenuti nel regolamento, in particolare quello di *privacy by design* e *by default;*
7- ad aggiornare la propria modulistica, in particolare l'informativa al trattamento dei dati e, ove previsto, il consenso al trattamento dei dati, a quanto prescritto dal regolamento;
8- a redigere e mantenere aggiornato il registro o i registri delle attività di trattamento;
9- a garantire agli interessati l'effettiva possibilità di esercitare i diritti connessi ai dati detenuti dal titolare.

18. Link utili

Per l'espletamento dei predetti obblighi ed il reperimento della correlata modulistica, nonché per la consultazione delle eventuali linee guida e dei relativi aggiornamenti e si consiglia di consultare periodicamente il sito internet del Garante per la Protezione dei Dati Personali, disponibile al link: http://www.garanteprivacy.it

19. Aggiornamenti e documenti utili

L'Ordine provvederà a mantenere informati i propri iscritti riguardo gli adempimenti connessi al regolamento EU 679/2016, fornendo quando possibile guide applicative, pareri del Garante per la Protezione dei Dati Personali, modelli e modulistica aggiornata ed ogni altro strumento che possa risultare utile all'adempimento di quanto prescritto dal predetto regolamento.