Oggetto: Regolamento UE 2016/679 Vademecum degli adempimenti a carico dei biologi Titolari di laboratori di analisi.

Come ormai noto, il 25 maggio 2018 entrerà in vigore la nuova normativa in materia di protezione dati personali. Premesso che nel caso di esercizio della professione in forma societaria, o comunque associata, titolare del trattamento (e destinatario di obblighi e sanzioni) è la Società, in persona del legale rappresentante pro tempore, con il presente vademecum si vuole fornire al biologo Titolare di un laboratorio di analisi, un quadro generale degli adempimenti imposti.

Revisione dei moduli per l'informativa / consenso

Il nuovo regolamento introduce elementi ulteriori rispetto a quelli previsti dall'art. 13 del D. Lgs 196/03, ed in particolare, alla informativa già in uso nella struttura andranno aggiunti:

a) L'eventuale intenzione del Titolare di trasferire i dati al di fuori dell'Unione Europea;
b) Il periodo di conservazione dei dati, o, se non è possibile, i criteri utilizzati per determinare tale periodo;
c) L'esistenza del diritto dell'interessato alla portabilità dei dati (l'esistenza di altri diritti dell'interessato quali quello di richiedere l'accesso, la rettifica, la cancellazione o la limitazione erano già previsti dal d. Lgs 196/03);
d) L'esistenza del diritto dell'interessato di revocare il consenso in qualunque momento;
e) Il diritto dell'interessato di proporre reclamo all'Autorità Garante;
f) L'esistenza di un processo decisionale automatizzato (qualora sia utilizzato nella struttura).

Revisione dei moduli per la nomina del Responsabile esterno

Tutte le volte che i dati dell'interessato vengono comunicati al di fuori della Struttura (ad esempio al Commercialista per la tenuta della contabilità), è necessario predisporre un formale atto di nomina a Responsabile del Trattamento del soggetto esterno. Tale nomina, secondo quanto previsto dall'art.28 del Regolamento, deve contenere:

a) Durata, natura e finalità del Trattamento, il tipo di dati oggetto di trasferimento e le categorie di interessati:

L'impegno del Responsabile a:

b) Trattare i dati, esclusivamente per le finalità connesse all'esecuzione del contratto, e su istruzioni documentate del Titolare;

c) Garantire che i soggetti autorizzati dal Responsabile stesso a compiere operazioni di trattamento sui dati, siano vincolati alla riservatezza;
d) Adottare all'interno della propria struttura, le misure di sicurezza di cui all'art.32 del Regolamento UE 2016/679;
e) Non nominare sub responsabili se non su espressa autorizzazione scritta del Titolare;
f) Predisporre misure tecniche ed organizzative adeguate per consentire al Titolare di assolvere il proprio obbligo di dare seguito nei tempi previsti ad eventuali richieste per l'esercizio dei diritti degli interessati;
g) Assistere il Titolare nel garantire il rispetto degli obblighi in materia di sicurezza del trattamento e di eventuale consultazione preventiva ai sensi dell'art. 36 del Regolamento;
h) Cancellare o fornire copia del dati al Titolare, alla conclusione del rapporto;
i) Mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare l'adempimento degli obblighi di cui alla presente nomina ed a consentire, se del caso collaborandovi, le attività di revisione, comprese le ispezioni predisposte da Titolare o da un oggetto da questi delegato.

Analisi dei Rischi

Il Titolare deve analizzare, ed essere in grado di documentare, di avere svolto una analisi dei rischi che incombono sui dati.

In particolare i rischi da prendere in considerazione sono:

a) Distruzione;
b) Perdita;
c) Modifica;
d) Divulgazione non autorizzata;
e) Accesso accidentale o illegale

Ciascun Titolare, analizzato il contesto, il grado di rischio ed i costi di attuazione dovrà attuare misure tecniche ed organizzative tali da ridurre al minimo i rischi indicati.

E' ritenuta misura idonea, ad esempio, la pseudonimizzazione del dato che consiste nel rendere il dato riferibile ad uno specifico interessato solo attraverso l'utilizzo di informazioni aggiuntive, conservate in luogo diverso.

Per il resto andrà effettuato un controllo relativo all'adeguamento degli strumenti informatici utilizzato per il trattamento dei dati (pc, server, hard disk, software, ecc).

Registro dei Trattamenti

Il Titolare deve tenere un registro delle operazioni di trattamento in cui vengano indicati:

a) Nome e dati di contatto del Titolare;

b) Finalità del trattamento;
c) Le categorie di interessati e e categorie di dati personali oggetto del trattamento;
d) Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e) I termini previsti per la cancellazione dei dati;
f) Una descrizione delle misure di sicurezza adottare all'interno dello Studio;

Notifica delle violazioni

Il Titolare dovrà notificare all'autorità di controllo le violazioni di dati personali di cui venga a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

A questo proposito si precisa che tra i menzionati rischi rientra, tra gli altri, "la perdita di riservatezza dei dati personali protetti da segreto professionale".

Se la probabilità di tale rischio è elevata, tale comunicazione andrà inviata anche ai pazienti, sempre "senza ingiustificato ritardo", a meno che i dati non siano stati cifrati, o il titolare si sia adoperato per scongiurare il rischio elevato o la comunicazione richiederebbe sforzi sproporzionati.

Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, Il Garante raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione al Garante stesso in caso di accertamenti.

Nomina del Responsabile Protezione Dati (DPO)

Il Legale rappresentante di un laboratorio di analisi, così come chiarito dal Garante Privacy italiano, è tenuto alla nomina di un Responsabile Protezione Dati, ai sensi dell'Art. 37 del Regolamento.

Si tratta di una soggetto (dipendente o consulente esterno) con una comprovata conoscenza del Regolamento e del settore specifico al quale viene demandato il compito di:

a) informare e fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento;
b) sorvegliare l'osservanza del regolamento, nonché delle politiche del titolare del trattamento, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con il Garante e fungere da punto di contatto per questioni connesse al trattamento

Formazione

Dal momento che la formazione del personale assume un ruolo fondamentale, il Titolare dovrà predisporre un piano di formazione annuale che coinvolga tutti i soggetti che a vario titolo vengono coinvolti nel trattamento.

Valutazione di impatto sulla protezione dati.

Si deve ritenere applicabile ai Titolari di laboratori di analisi l'obbligo di redigere un documento (anche informatico) che contenga:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
b) una valutazione della necessità e proporzionalità del trattamento;
c) una valutazione dei rischi per i diritti e per le libertà dell'interessato;
d) le misure previste per:
    a. affrontare i rischi
    b. dimostrare la conformità con il regolamento

Per facilitare tale compito, è stato rilasciato dall'Autorità Garante francese un software di libero utilizzo (tradotto in italiano) e scaricabile al seguente link:
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Avv. Mario Ponari