MPSLAW

Privacy e trattamento dei dati personali nelle Aziende Sanitarie

Avv. Juri Monducci

studio legale associato

www.mpslaw.it

1

MPSLAW

CHI SONO

Partner fondatore di *MPSLAW – STUDIO LEGALE ASSOCIATO*.
Professore a contratto all'Università di Bologna.
Dottore di ricerca in Diritto dell'Informatica all' Università di Bologna.
Dottore di ricerca in Bioetica all'Università di Bologna.
Assegnista di Ricerca all'Università a Bologna.

DPO dell'Azienda Unità Sanitaria Locale di Ferrara.
DPO dell'Azienda Ospedaliero – Universitaria di Ferrara.

studio legale associato

www.mpslaw.it

2

MPSLAW

Un po' di storia:
dal diritto alla riservatezza al diritto alla protezione dei dati

- 1890: Harward Law Review: ***the right to be let alone*.**
- Cass., 27 maggio 1975, n. 2129 (Caso «Soraya»): **diritto alla riservatezza** come diritto alla segretezza delle proprie vicende personali;
- Rodotà S., *Privacy e costruzione della sfera privata*, 1991: **diritto alla protezione dei dati personali** quale «diritto alla circolazione controllata o alla interruzione del flusso delle informazioni»

MPSLAW

Un po' di storia del diritto alla protezione dei dati:
dalla Direttiva 95/46/CE al Regolamento UE 2016/679

- La Direttiva UE 95/46/CE ha consentito l'approvazione della legge 675/96, entrata in vigore il 07/05/1997, poi abrogata a decorrere dal 1/1/2004.
- Il Codice in materia di protezione dei dati personali (d.lgs. 196/03) è un Testo Unico. Entra in vigore il 1/1/2004.
- Il Regolamento sulla protezione dati (RGPD o GDPR), entrato in vigore nell'anno 2016, è divenuto definitivamente efficacie il 25/05/18.
- Il d.lgs. 101/2018, entrato in vigore il 19/09/2018, «armonizza» l'ordinamento giuridico italiano al predetto Regolamento UE

MPSLAW

Il Regolamento UE sulla privacy

- Il Regolamento sulla protezione dati (RGPD o GDPR), entrato in vigore nell'anno 2016, è divenuto definitivamente efficacie il 25/05/18.
- Il Regolamento individua un quadro ben preciso in termini di compliance per la protezione dati in Europa, basandosi sul principio di **responsabilizzazione**.
- Al centro di tale quadro giuridico è stato collocato il *data protection officer* (DPO) - responsabile della protezione dei dati (RPD), che entrambe le Aziende Sanitarie di Ferrara hanno nominato nella persona dell'avv. Juri Monducci.

MPSLAW

Il trattamento dei dati personali

- *Trattamento dei dati*: ogni operazione o complesso di operazioni che viene effettuata con dati personali, dalla raccolta alla distruzione.
- *Dato personale*: ogni informazione relativa ad una persona individuata o individuabile.
- *Dato particolare* (ex *dato sensibile*): ogni dato personale idoneo a rivelare l'origine **razziale ed etnica**, le **convinzioni religiose** o **filosofiche**, l'adesione a partiti e sindacati, la **vita e l'orientamento sessuale**, lo **stato di salute**, i dati biometrici, i dati genetici e i dati giudiziari.
- *Titolare del trattamento*: la persona fisica o giuridica alla quale competono le decisioni relative su finalità e alle modalità del trattamento (es: Azienda USL di Ferrara, Azienda Ospedaliera di Ferrara) .
- *Interessato*: ogni persona fisica alla quale si riferiscono i dati personali.

MPSLAW

Il responsabile del trattamento

Il responsabile del trattamento è la persona **fisica o giuridica che effettua trattamenti per conto del titolare**

- scelto tra soggetti competenti;
- in forma scritta con atto contrattuale;
- con predeterminazione analitica dei compiti e con specificazione delle istruzioni.

In caso di esternalizzazione del servizio la designazione del RESPONSABILE è obbligatoria.

MPSLAW

L' «autorizzato» al trattamento

Il titolare e il responsabile dovrebbero trattare *personalmente* i dati, non potendo comunicarli a terzi senza il consenso.

Affinché dipendenti o collaboratori possano procedere al trattamento, è necessario *autorizzarli* (art. 29 del Reg.):

- l'autorizzazione deve provenire dal titolare o dal responsabile **che sia dotato di potere «gerarchico» su chi viene autorizzato**;
- il titolare o il responsabile devono «formare» chiunque designino al trattamento.

L'autorizzazione non amplia le attribuzioni del dipendente ma gli attribuisce il potere di svolgere le mansioni affidategli.

N.B.: è obbligatoria la FORMAZIONE PERIODICA.

MPSLAW

Il *Data Protection Officer*/Responsabile della Protezione dati

Il DPO **deve** essere designato quando il titolare del trattamento è una pubblica amministrazione o quando le attività principali del titolare consistono nel trattamento su «larga scala» di dati particolari (es. «sanitari»). Le due Aziende Sanitaria Ferraresi hanno designato l'avv. Juri Monducci.

MPSLAW

Il *Data Protection Officer*/Responsabile della Protezione dati

Il DPO ha le seguenti funzioni:

- informare e fornire consulenza al **titolare** e ai **dipendenti** sugli obblighi privacy;
- sorvegliare l'osservanza delle norme sulla privacy, sulle relative politiche del titolare, compresa l'attribuzione delle responsabilità, la formazione, i controlli;
- fornire pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- cooperare e fungere da punto di contatto con il **Garante Privacy**;
- contatto diretto da parte dei singoli interessati, che possono contattarlo bypassando il titolare e/o il responsabile del trattamento.

Il DPO è contattabile da ciascun dipendente dell'Azienda Sanitaria, con vincolo di segretezza rispetto a quanto gli viene comunicato

MPSLAW

SOS PRIVACY

Il DPO presta servizio presso la Direzione Generale delle Aziende, è contattabile attraverso i seguenti contatti email
dpo@ausl.fe.it - dpo@ospfe.it

Per eventuali urgente il DPO è contattabile direttamente dal vertice aziendale.
Al DPO possono essere inviate comunicazioni istituzionali attraverso il sistema di gestione documentale delle Aziende (BABEL)

MPSLAW

Correttezza e pertinenza del trattamento

L'art. 5 del Reg. UE impone al titolare di trattare i dati:

1. in modo lecito, secondo correttezza, trasparente «nei confronti dell'interessato»;
2. per scopi determinati, espliciti e legittimi;
3. in altre operazioni solo per ragioni compatibili con gli scopi originari (è compatibile la finalità di archivio pubblico, di ricerca scientifica, storica o statistica);
4. esatti e, se necessario, aggiornati;
5. adeguati, pertinenti, completi e limitati, quindi non eccedenti le finalità per le quali sono raccolti e successivamente trattati;
6. in forma identificativa solo per il tempo necessario al perseguimento di detti scopi;
7. in modo tale da garantire adeguata sicurezza.

I dati trattati in violazione non possono essere *utilizzati,* obbliga al risarcimento dei danni subiti dall'interessato, anche morali, e comporta una sanzione amministrativa fino a **20 milioni di euro**.

MPSLAW

L'informativa

Il titolare (o chi per esso), deve fornire alla persona che fornisce i dati le seguenti informazioni:

–finalità, modalità e base giuridica del trattamento;

–durata del trattamento e natura del conferimento dei dati (obbligatoria o facoltativa) e conseguenze in caso di rifiuto;

–i soggetti (ad es., Ministro della Sanità) o le categorie di soggetti (ad es., enti locali) ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati;

–i diritti dell'interessato e la possibilità di proporre reclamo al Garante;

–gli estremi identificativi e i contatti del titolare, i dati di contatto del DPO.

L'informativa viene fornita a mezzo **cartellonistica**, è stata inserita nei fogli di prenotazione, deve essere consegnata in caso di ricovero e comunque viene fornita nella documentazione che viene consegnata agli interessati

MPSLAW

Il consenso

Il trattamento dei dati per finalità di diagnosi e cura, nonché il trattamento dei dati per finalità amministrative di natura pubblicistica **prescinde** dal consenso dell'interessato.

Il consenso è comunque necessario:

- per il trattamento dei dati genetici
- per il trattamento per finalità di ricerca e sperimentazione

MPSLAW

(segue) l'informativa e il consenso: sanzioni

L'omessa informativa comporta l'irrogazione di una sanzione fino a 20 milioni di euro

L'omesso consenso (quando necessario, quindi in caso di ricerca e di trattamento dei dati genetici) comporta l'irrogazione di una sanzione fino a 20 milioni di euro.

N.B. la sanzione viene inflitta all'Azienda, ma **permane la responsabilità contabile del dipendente che ha agito con dolo o colpa grave**

MPSLAW

I diritti dell'interessato

Gli artt. 15 ss. del Reg UE consentono all'interessato l'esercizio:

- del diritto di «accesso» (al trattamento, ai dati e alle relative informazioni);
- del diritto di «intervento» (cancellazione e/o modifica dei dati, nonché blocco del trattamento o di singole operazioni);
- del diritto di «opposizione» (per motivi legittimi).

Il riscontro all'esercizio dei suddetti «diritti» deve essere garantito entro 30 giorni dalla ricezione della richiesta.

Eventuali richieste, laddove di non semplice soluzione, devono pertanto essere trasmesse alla D.G. e/o all'indirizzo email del DPO entro 5 giorni dalla sua ricezione (da annotare per iscritto, previa identificazione dell'interessato e dei suoi contatti telefonici, anagrafici e, nel caso, telematici)

MPSLAW

(segue) i diritti dell'interessato: sanzioni

L'omessa ottemperanza alla richiesta dell'interessato comporta l'irrogazione di una sanzione amministrativa fino a 20 milioni di euro

MPSLAW

Le misure adeguate di sicurezza

L'Azienda è tenuta a «mettere in atto» misure tecniche e organizzative finalizzate a garantire un livello di sicurezza adeguato al rischio

Tali misure, se del caso, devono comprendere, tra le altre:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

MPSLAW

Le misure organizzative

Le misure «organizzative» sono determinate dall'Azienda, in accordo col DPO, e sono, tra le altre:

- la «distanza di cortesia», che impedisce a chi attende di udire i dati comunicati allo sportello;
- soluzioni che, in caso di prestazioni precedute da un periodo di attesa, prevedano un ordine di precedenza e di chiamata che prescinda dalla individuazione nominativa dei pazienti;
- soluzioni che prevengano, durante colloqui, l´indebita conoscenza da terzi di dati sanitari;
- cautele che evitino che le prestazioni sanitarie, ivi compresa l´eventuale documentazione di anamnesi, avvengano in situazioni di promiscuità
- nell'identificazione, se possibile certa, dell'interlocutore telefonico, ad es. chiedendogli informazioni che sono presumibilmente solo a sua conoscenza e/o nella sua disponibilità;
- nell'evitare di lasciare la password per l'accesso al sistema e/o agli applicativi in luogo facilmente reperibile (sotto la tastiera, attaccato al monitor, nel primo cassetto);
- l'accorgimento di gettare carte contenenti dati particolare previa **distruzione fisica (es. trita-documenti)**.

MPSLAW

Le misure informatiche

Le misure di sicurezza di tipo informatico sono determinate dall'Azienda (in particolare dall'ICT), in accordo con il DPO, e sono, almeno, le seguenti:

- l'utilizzo di un sistema di login+password **personali** per l'accesso alla rete;
- l'implementazione di requisiti «sicuri» della password (alfanumerica, almeno 8 caratteri, obbligo di modifica trimestrale, blocco della postazione lavoro, ecc….);
- l'installazione di antivirus ad aggiornamento automatico e di un firewall;
- l'installazione di un sistema di backup
- Il divieto di utilizzare, per trasmettere dati sanitari, la posta elettronica;
- Il divieto di utilizzare, per comunicazioni aziendali, la posta elettronica personale (non aziendale)

MPSLAW

Il c.d. DATA BREACH

La potenziale violazione della privacy degli interessati deve essere notificata al Garante entro 72 ore e comunicata ai singoli interessati.

In caso di potenziale violazione **(es. attacco hacker, attacco virus, smarrimento e/o furto di pc, smarrimento e/o furto di chiavetta, furto o apertura di cassaforte, se tali supporti contenevano dati personali, smarrimento di una cartella clinca)** è necessario darne immediato avviso (entro 6 ore) al DPO che provvederà ad inoltrare un modulo da compilare e a dare indicazioni su come procedere.

MPSLAW

(segue) misure di sicurezza: le sanzioni

La violazione delle misure di sicurezza comporta l'irrogazione di una sanzione amministrativa fino a 20 milioni di euro e responsabilità CIVILE (l'interessato può chiedere il risarcimento del danno).

In ogni caso di violazione della normativa privacy il Garante può disporre il blocco del trattamento.

MPSLAW

Avv. Juri Monducci

dpo@ausl.fe.it
dpo@ospfe.it

Skype contact: juri.monducci