La Privacy by Design nel regolamento europeo UE 2016/679

Privacy e "cura" dei dati in sanità

Filippo Lorè

Università degli Studi di Bari

Corrispondenza a:
Dott. Filippo Lorè
Docente a contratto
Università degli Studi di Bari
e-mail: Filippo.lore@yahoo.it


Filippo Lorè

Per il mondo sanitario, e non solo, il 25 maggio 2018 ha rappresentato un cambiamento radicale nel modo di intendere la protezione dei dati personali (1).

Se fino a qualche anno fa la privacy veniva considerata marginalmente nelle attività principali delle strutture sanitarie, questo atteggiamento sta mutando sino a sovvertire il punto di vista degli attori principali. Questo lo si deve ad una nuova consapevolezza acquisita dall'interessato (o assistito), dal cambiamento culturale che ha coinvolto il mondo sanitario e, non in ultimo, dall'aspetto deterrente della sanzione prevista dal legislatore europeo.

Come detto, il principio della Privacy by Design (2) (e della Privacy by Default) rappresenta un elemento di assoluta novità. Al titolare del trattamento è demandato un atteggiamento responsabile e proattivo nei confronti dei "nuovi" dettami normativi, valutando, di caso in caso, le misure che dovranno essere predisposte per garantire pieno rispetto dei diritti e delle libertà delle persone fisiche.

Una volta definito l'aspetto formale della Privacy By Design, passiamo ad analizzare brevemente l'aspetto sostanziale.

Una delle priorità per il titolare del trattamento è la definizione e la stesura dell'organigramma privacy: è necessario individuare gli attori principali impegnati nelle operazioni di trattamento.

Il titolare è 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 dei dati personali. La vecchia disciplina del Codice in materia di protezione dei dati personali prevedeva la figura del responsabile del trattamento all'art. 29 e dell'incaricato al trattamento dei dati personali all'art. 30 dello stesso D.Lgs n.196/2003.

La previsione di queste ultime due figure sembra venir meno con il Regolamento europeo, ma il principio di accountability, espressamente introdotto dal legislatore all'art. 24, prevede che "*…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*". Tale disposizione implica che il titolare può ancora definire compiti e responsabilità derivanti dalle operazioni di trattamento, nominando (gli ex responsabili ai sensi del Codice privacy) attraverso un atto di designazione, per iscritto, a referente (o delegato) al trattamento. Anche per quanto riguarda l'incaricato, il Regolamento, attraverso un'attenta interpretazione riconosce tale figura agli artt. 4, n.10, 29 e 32, par. 4, specificando che chiunque agisca sotto l'autorità del titolare non può trattare dati se non è istruito in tal senso dallo stesso.

All'interno dell'organizzazione sanitaria, accanto alle figure sopra richiamate, il titolare del trattamento non può prescindere dalla nomina dell'amministratore di sistema (disciplinata nel Provvedimento del Garante privacy del 27/11/2008). Sono questi "*esperti chiamati a svolgere delicate funzioni che richiedono concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione…* " (3).

L'art. 28 del Regolamento UE 2016/679, poi, prevede la figura del Responsabile del trattamento, soggetto esterno all'ambito aziendale che tratta, in forza di un accordo, convenzione, contratto o altro atto giuridico, dati personali per conto del titolare del trattamento. La nomina del responsabile del trattamento (esterno), avviene specificando al meglio le istruzioni alle quali soggetti giuridici esterni al titolare del trattamento dovranno attenersi.

Proseguendo con l'analisi pratica delle misure di Privacy by Design, il titolare, con l'ausilio del Responsabile per la protezione dei dati personali, deve procedere alla mappatura dei trattamenti effettuati nelle varie aree operative al fine di redigere e tenere aggiornato il Registro delle operazioni di trattamento, espressamente previsto all'art. 30 del Regolamento UE 2016/679. Questo adempimento riveste assoluto rilievo, poiché consente di "fotografare" lo stato dell'arte della struttura sanitaria sotto il profilo della tutela dei dati personali e, in sede ispettiva, funge quale strumento probatorio.

In ogni attività rilevante sotto il profilo della tutela dei dati personali, strategico è il ruolo del Responsabile per la protezione dei dati personali che assume la veste di "piccolo garante" per i diritti e le libertà delle persone fisiche (come specificato negli articoli curati dallo scrivente nella presente rubrica).

Una volta definite le prime attività, nel prossimo numero si approfondiranno ulteriori aspetti legati al principio della Privacy by Design in una struttura sanitaria.

BIBLIOGRAFIA

1. Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali
2. Privacy by Design" numero aprile/giugno della rivista Privacy news
3. Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale" di F. Modafferi