Impatti del Regolamento Privacy sullo sviluppo software

Il Nuovo Regolamento Europeo sulla Privacy (GDPR), emanato lo scorso maggio ed in vigore entro fine maggio 2018, pone nuove questioni relativamente all'impiego di programmi software per l'elaborazione di dati personali, in particolare se si tratta anche di dati c.d. "sensibili" secondo la vecchia definizione del D. Lgs 196/2003.

Infatti il nuovo Regolamento Europeo sulla privacy ("Regolamento UE 2016/679 del Parlamento europeo") impone alle organizzazioni che intendono effettuare trattamenti di dati personali di "progettare" il sistema in modo tale che sia conforme fin da subito (**Privacy by design**) alle regole della privacy, spostando la responsabilità del corretto trattamento tramite strumenti informatici idonei sul titolare e sul responsabile del trattamento, quando identificato.

Nella pratica una organizzazione, prima di impiegare un applicativo software per trattare dati personali dovrà verificare che esso sia conforme ai requisiti stabiliti dal Regolamento UE 679/2016, ovvero che presenti caratteristiche di sicurezza adeguate per mantenere protetti i dati personali, compresa l'eventuale pseudonomizzazione dei dati personali, quando necessaria, e la cifratura dei dati stessi.

Il Regolamento parla anche di "certificazione" della privacy, che può riferirsi ad un singolo o ad un insieme di trattamenti effettuati da un programma software, oppure da tutti i trattamenti effettuati da una organizzazione. In quest'ultimo caso siamo molto vicini alla certificazione del sistema di gestione ISO 27001, anche se in realtà il GDPR intende qualcosa di differente. Al proposito è stato approvato da ACCREDIA lo schema proprietario ISDP©10003:2015 (conformità alle norme vigenti EU in tema di trattamenti dei dati personali)che conente di certificare un prodotto, processo o servizio relativamente alla gestione dei dati personali, quindi anche un applicativo software che tratta dati personali.

Lo schema di certificazione ISDP 10003:2015 risponde ai requisiti di cui agli art. 42 e 43 del Regolamento 679/2016 ed è applicabile a tutte le tipologie di organizzazioni soggette alle norme vigenti in tema di tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati. Lo schema di certificazione specifica ai "Titolari" e "Responsabili" del trattamento, soggetti ai vincoli normativi vigenti nel territorio dell'EU, i requisiti necessari per la corretta valutazione della conformità alle norme stesse.

Per maggiori informazioni su questo schema di certificazione si veda la pagina del sito Inveo
http://www.in-veo.com/servizi/certificazioni-inveo/isdp-10003-2015-data-protection.

Ricordiamo anche che all'art 25, coma 2 il Regolamento sancisce che:

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. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Rappresenta **la c.d. Privacy by default**: devono essere trattati "per default" solo i dati necessari a perseguire le finalità del trattamento posto in essere dal responsabile dello stesso, ovvero non devono essere trattati dati in eccesso senza che una persona fisica autorizzata lo consenta.

La certificazione introdotta all'Art. 42 può servire a dimostrare l'adozione di misure tecniche ed organizzative adeguate.

L'impatto di queste regole sugli **applicativi software** utilizzati per trattare anche dati personali è notevole: una organizzazione di qualsiasi dimensione che adotta un sistema informatico gestionale che tratta dati personali non in modo conforme al Regolamento UE 679/2016 di fatto rischia di essere sanzionata perché non ha adottato misure di sicurezza adeguate. Le responsabilità ricadono, in questo caso, sul titolare del trattamento e sul responsabile del trattamento, ove presente.

Dunque prima di adottare un nuovo software che gestisce archivi contenenti dati personali (a maggior ragione se vengono gestiti dati sanitari o altri dati c.d. "sensibili") titolari e responsabili del trattamento devono valutarne la **conformità alla normativa sulla privacy** e questo può essere al di fuori delle competenze di chi decide l'acquisto di un applicativo software (responsabili EDP, Direttori Generali, ecc.), soprattutto nelle piccole e medie imprese o nelle strutture sanitarie di modeste dimensioni (es. Cliniche ed ambulatori privati).

La casistica di software che ricadono in questa sfera è vastissima, si va dai comuni ERP che trattano anche dati del personale, ai software per la gestione delle paghe, ai programmi per la gestione delle *fidelity card*, ai software impiegati in strutture sanitarie o quelli utilizzati dagli studi legali.

Oggi molti applicativi, magari obsoleti, non permettono di implementare misure di sicurezza adeguate (password di lunghezza adeguata, password di complessità minima variate periodicamente, password trasmesse via internet con connessioni crittografate, gestione utenti, raccolta di dati minimi indispensabili, gestione dei

consensi, procedure di backup, ecc.) e in futuro il loro impiego diverrà non conforme alla normativa sulla privacy, ovvero non saranno più commercializzabili.

Da un lato i progettisti e gli sviluppatori di applicativi software dovranno considerare fra i requisiti di progetto anche quelli relativi alla normativa privacy, dall'altro le organizzazioni che adotteranno applicativi software (o che già li stanno utilizzando) saranno responsabili della loro eventuale non conformità al Regolamento Privacy. Sicuramente una certificazione di tali applicativi o un assessment indipendente potrà sollevare il titolare del trattameto dalle rsponsabilità (cfr. principio dell'*accountability)* connesse all'adozione di un software che non tratta i dati in conformità al GDPR.