Privacy / tre questioni chiave del Regolamento sulla protezione dei dati personali (GDPR) per i fornitori di software

di Marco Perini
FGA, Studio Legale Ferraro Giove e Associati

I fornitori di applicativi informatici sono Responsabili esterni del trattamento: questo a condizione che intervengano sui dati per conto del cliente, dovendo pertanto predisporre tutte le misure di sicurezza da osservare nella conservazione delle informazioni e nei trattamenti demandati.

Nella corsa all'adeguamento alla normativa sulla protezione dei dati personali (il cosiddetto GDPR n. 2016/679), che ha contraddistinto gli ultimi due anni, era previsto che i fornitori di software avrebbero svolto un ruolo strategico**: le loro piattaforme intervengono nel trattamento dei dati, rispetto ai quali hanno rilevanza misure di compliance e di sicurezza che necessitano specifiche implementazioni all'interno dei software**, ad esempio per minimizzare l'accesso alle informazioni da parte di operatori con ruoli diversi. Molti trattamenti sono automatizzati, spesso avvengono on line, con memorizzazione dei dati su cloud che si trovano presso fornitori esterni e che sono pertanto Responsabili delle operazioni sui dati che compiono per conto dei clienti. La corretta individuazione di queste attività è dunque uno dei temi che l'applicazione del Regolamento ha proposto e propone quotidianamente alle imprese e alle pubbliche amministrazioni, ma sul quale non vi è una piena consapevolezza.

A questa, si aggiungono altre questioni chiave, anch'esse forse finora sottovalutate. In questa sede ci soffermiamo su tre in particolare.

1. L'identificazione dei ruoli. Il registro dei trattamenti assume una evidenza strategica anche per l'esatta individuazione dei ruoli che di volta in volta si rivestono nella gestione dei dati personali. Questa riflessione viene avvalorata anche dalla recente risposta del Garante per la Privacy (newsletter n 449 del 7 febbraio scorso) al quesito sottoposto dal Consiglio Nazionale dei Consulenti del Lavoro.
I **ruoli presi in considerazione dal GDPR (Titolare, Contitolare, Responsabile, Incaricato) possono cambiare nel tempo, nelle diverse fasi di trattamento dei dati** a seconda di cosa si va a fare concretamente con quei dati. Per il trattamento di dati dei clienti, ad esempio, una azienda potrà essere in un primo momento responsabile ed in un secondo momento titolare, mentre per altri tipi di dati potrà essere contitolare. Il diverso ruolo dell'azienda emerge, ovviamente, nella fase di compilazione del **registro dei trattamenti**, che costituisce un vero e proprio percorso di analisi ed indagine finalizzato anche a questo scopo e premessa per le conseguenti attività da svolgere.

2. I rapporti tra Titolari e Responsabili.

Attualmente la più comune criticità che si sta consumando è nei rapporti tra i Titolari e i Responsabili.

L’art. 28 del Regolamento UE 2016/679, infatti, richiama la necessità di un contratto vincolato, che leghi il responsabile del trattamento al titolare.

La norma riguarda tendenzialmente tutti rapporti di fornitura di servizi, per effetto dei quali il fornitore tratta dati personali per conto del fruitore del servizio (p.e. dei suoi clienti e/o dei dipendenti).

L’ottica di sistema del Regolamento è assolutamente ineccepibile: i dati sono affidati al titolare, questo deve informare l’interessato di cosa andrà a fare con quei dati e se sceglie di usare un outsourcer ne risponde insieme con il diretto autore dell’infrazione. Quindi serve un contratto.

Ma proprio sul fronte del contratto stanno emergendo pericolose criticità, costituite, da un lato, dallo squilibrio nei rapporti di forza tra le parti e, dall’altro, dal fatto che il Responsabile dovrebbe comunicare al Titolare (che dovrebbe pretenderlo) le misure di sicurezza che intende applicare al trattamento demandatogli.

In merito al primo aspetto si stanno polarizzando due tendenze assolutamente opposte: il fornitore responsabile “debole” farà qualunque sforzo per mantenere il rapporto con il suo potente cliente titolare, sottoscrivendo qualunque contratto gli venga sottoposto, mentre il cliente titolare “debole” dovrà accettare, nella migliore delle ipotesi, un contratto vincolato da un potente fornitore responsabile, anche se non adeguato a quanto prescrive la legge. Mentre nella maggior parte dei casi dovrà accettare di non stipulare proprio nessuna appendice integrativa, a dispetto di quanto il Regolamento prescrive. D’altra parte alcuni Titolari si sono limitati ad inviare ai Responsabili mere richieste unilaterali di adeguamento a prescrizioni impartite ex art. 28 GDPR, senza considerare il chiaro dettato normativo e la necessità di dover **acquisire certezze in termini di accountability.**

3. Il rapporto con i fornitori di software gestionali.

Altro argomento critico è costituito dalle evidenti necessità di cooperazione dei fornitori di software gestionali, il cui compito è appunto “gestire” dati, ma che sempre più spesso risultano non essere stati adeguati tempestivamente alla normativa vigente, rendendo di fatto impossibile alle società utilizzatrici essere a norma.

In quest’ultimo caso il GDPR non ha previsto direttamente obblighi in tal senso, ma le relazioni attinenti ai sopramenzionati tre punti sono **governate dai doveri di correttezza e di buona fede stabiliti dagli art.li 1175 e 1375 c.c.** , derivandone una serie di obblighi di collaborazione che –al di là del contratto in essere - si sostanziano, tra gli altri, nell'obbligo di informare circa ogni questione che sia rilevante per la controparte, nell'obbligo di solidarietà e nell'obbligo di protezione e cioè di evitare che l'altra parte subisca pregiudizi.

A cura dell’Avv. Marco Perini
Managing Partner
Supervisore del Dipartimento di Compliance