IL CONTRATTO TRA TITOLARE E RESPONSABILE DEL TRATTAMENTO: UN CONCRETO INDICATORE DI UNA GOVERNANCE ROBUSTA

Giuseppe Alverone

INDICE DEGLI ARGOMENTI

La responsabilità generale del titolare del trattamento

Il ruolo privacy di "titolare del trattamento" nella versione in lingua inglese del GDPR" è definito **"controller"** i.e. **controllore.**

Questa particolare qualificazione fa ben comprendere l'effettiva sfera di responsabilità e di azione dell'entità protagonista nell'ecosistema privacy, che è chiamata ad avere la piena governance dei processi in cui girano i dati personali, i.e. il pieno "comando e controllo" dei trattamenti.

La conferma di questa considerazione si trova nel Considerando 74 del GDPR che, con assoluta chiarezza, stabilisce **la responsabilità generale** del titolare per qualsiasi trattamento di dati personali:

a. sia per quelli eseguiti direttamente, tramite il lavoro dei propri dipendenti *"autorizzati al trattamento";*
b. sia per quelli eseguiti *"per suo conto"* da entità esterne, che assumono il ruolo privacy di *"responsabili del trattamento"* (nella più pregnante versione inglese ***processor:processore***).

Una particolarità dell'ecosistema privacy è che questa **responsabilità generale** non può mai essere trasferita ad altre entità dal titolare ma potrà solo essere da questi governata e controllata.

La gestione della responsabilità della responsabilità generale da parte del titolare

Ci sono dei validi indicatori dai quali sia possibile indurre che un titolare sta gestendo correttamente la propria responsabilità generale?

Invero l'antica saggezza popolare aiuta ad orientarsi anche nella complessità che caratterizza i difficili momenti che stiamo vivendo. Un antico proverbio recita *"se vuoi scoprire i misteri della foresta, devi guardare la foglia, non l'albero"*. Applicando questo suggerimento ad un'analisi organizzativa, si può affermare che, ragionevolmente, un titolare ha il pieno comando e controllo dei trattamenti, laddove abbia posto costantemente la massima cura ed attenzione nel ripartire le necessarie operazioni di trattamento dei dati personali tra i lavoratori dipendenti ed i fornitori/appaltatori, attraverso:

a. accurate sessioni di formazione dei dipendenti, tutti formalmente autorizzati al trattamento con specifici atti di nomina;
b. la delega di alcuni trattamenti a fornitori/appaltatori, tutti vincolati con un contratto che sia strettamente aderente a tutte le indicazioni riportate nell'art. 28 del GDPR.

Il primo adempimento è facilmente realizzabile perché costituisce una forma di esercizio dell'autorità, propria del datore di lavoro, privato o pubblico.

La scelta dei responsabili del trattamento. e la successiva stipula del contratto necessario per vincolarli, è, invece, un'attività difficile e complessa che genera vulnerabilità.

Infatti l'estensione di una parte delle proprie attività di trattamento, attraverso l'affidamento ad entità esterne alla propria organizzazione, non sottoposte alla propria autorità, pone un problema di

sicurezza, anche alla luce della possibilità che hanno i responsabili, di far ricorso a sub-responsabili (seppur previa autorizzazione generale o specifica del titolare) che vanno così a formare una catena di responsabili/fornitori, i.e. la catena di approvvigionamento (la c.d. ***supplychain***).
Orbene, secondo un noto aforisma "la sicurezza di una catena è forte quanto il suo anello più debole". Quindi la "robustezza" di un complessivo sistema di trattamento di dati personali gestito da un determinato titolare è calibrato sui "punti di giunzione" dei flussi di trattamento più deboli, che sono appunto i contratti con i responsabili e sub-responsabili del trattamento.
La fondatezza di tale argomentazione è confermata dal fatto che la c.d. Direttiva NIS 2, approvata pochi giorni fa dal Parlamento Europeo, prevede l'obbligo di adottare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza della supplychain.

Le garanzie sufficienti
In tale quadro, al fine di presidiare i dati personali ed irrobustire la governance di tutti i processi aziendali, appare utile seguire le indicazioni fissate dal Considerando 81 del GDPR, secondo il quale un titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento, dovrebbe ricorrere unicamente ad operatori che presentino ***garanzie sufficienti***, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del GDPR, anche per la sicurezza del trattamento.
Quindi le aziende e le P.A. che agiscono come titolari del trattamento dovrebbero scegliere, sempre e soltanto, responsabili del trattamento che siano in grado di consentire o facilitare la gestione della responsabilità generale dei trattamenti.
Un modo efficace per poter individuare responsabili del trattamento appropriati consiste nel raccogliere i suggerimenti e seguire le raccomandazioni dei Garanti Europei.

I suggerimenti e le raccomandazioni dei Garanti Europei
I Garanti Europei, riuniti nel gruppo di lavoro WP 29 hanno chiarito[1] che una valutazione d'impatto sulla protezione dei dati (la c.d. DPIA) - funzionale, secondo il Considerando 84 del GDPR, a potenziare la compliance dei trattamenti - può essere utile anche per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico, e,g. un dispositivo hardware software che probabilmente verrà utilizzato da titolari del trattamento distinti, per svolgere tipologie diverse di trattamento. Resta comunque impregiudicato l'obbligo di ogni titolare che acquisti detto prodotto di eseguire la propria DPIA.
Questa possibilità rappresenta quindi un riferimento prezioso per i produttori i quali possono;

- rendere così più "desiderabili" i loro prodotti sul mercato;
- dimostrare concretamente di offrire garanzie sufficienti per svolgere le funzioni di "responsabile del trattamento".

Ancora, i Garanti Europei, riuniti nel Comitato Europeo della Protezione dei Dati, hanno evidenziato[2] che la capacità di un responsabile di ottenere una certificazione per il trattamento rappresenta un valore aggiunto per il titolare al momento in cui dovrà scegliere tra i diversi software, hardware, servizi e/o sistemi di trattamento forniti dagli stessi responsabili del trattamento.
Pertanto, i responsabili del trattamento dovrebbero sforzarsi di dimostrare che il rispetto del principio di "privacy by design" è parte integrante del ciclo di vita dello sviluppo della soluzione da loro venduta.

[1] Nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati" Wp248 rev. 01, par.III, A.
[2] Al punto delle Linee Guida EDPB 4/2019, sull'articolo 25 "Protezione dei dati fin dalla progettazione e per impostazione predefinita".

La possibilità di far certificare un trattamento può quindi certamente costituire un vantaggio competitivo per i responsabili del trattamento che in questo modo potranno anche facilmente vantare il possesso di "garanzie sufficienti".
Gli stessi Garanti Europei aggiungono che, in assenza di certificazione, i titolari del trattamento:

- dovrebbero cercare di avere altre garanzie in merito alla conformità ai principi di protezione dei dati da parte dei responsabili del trattamento;
- non dovrebbero mai scegliere produttori o responsabili che non offrano sistemi in grado di consentire o facilitare l'adempimento degli obblighi posti dal GDPR in capo ai titolari stessi, poiché saranno sempre, inevitabilmente, questi ultimi a rispondere dell'eventuale mancata attuazione.

Particolari indicazioni per le Pubbliche Amministrazioni

Le Pubbliche Amministrazioni che, quali titolari, hanno necessità di affidare parte dei loro trattamenti a responsabili del trattamento, devono seguire ben precise procedure, per assicurare il rispetto dei principi di trasparenza, concorrenza e meritocrazia nell'assegnazione del relativo appalto.
Quindi l'applicazione dei citati suggerimenti e raccomandazioni dei Garanti Europei va realizzata prodromicamente, in fase di predisposizione del capitolato di appalto.
E' quindi in quella sede che vanno precisati i criteri di scelta e le garanzie richieste ai fornitori/responsabili del trattamento.
Per questo motivo è auspicabile che ogni Pubblica Amministrazione che deve predisporre un capitolato per affidare un particolare trattamento ad un responsabile del trattamento, coinvolga tempestivamente il proprio DPO per avviare la procedura di appalto nel pieno rispetto dei principi di protezione dei dati personali.
Sempre nel momento in cui viene predisposto il capitolato per l'affidamento di un trattamento ad un responsabile è anche consigliabile il ricorso ai modelli di "Clausole Contrattuali Tipo" che la Commissione UE ha recentemente adottato con la Decisione di Esecuzione 2021/915 del 4 giugno 2021.