Il governo della filiera dei responsabili del trattamento rientra nell'accountability del titolare

Quando a trattare i dati del Titolare è un terzo soggetto è necessario controllare in maniera efficace l'attività del Responsabile Esterno

Nell'ambito di un trattamento di dati personali ci troviamo di fronte a quella che possiamo definire una "filiera dei partner" ogni qual volta le varie attività di trattamento di dati vengono effettuate da vari "soggetti privacy". Questa filiera, costituita dall'insieme di soggetti che si relazionano tra loro e che compiono varie attività nell'ambito di un trattamento di dati personali, può essere semplice o anche complessa e stratificata, a seconda di quante titolarità privacy si interpongono nella gestione di un determinato trattamento di dati e a seconda dei particolari rapporti tra essi.

Il Garante privacy con un provvedimento di fine 2022 ha sanzionato una società per essersi dimostrata incapace di controllare efficacemente la filiera dei partner che effettuavano attività di trattamento (in questo caso, per scopi di marketing) per conto della società stessa.

Il GDPR definisce i diversi ruoli dei soggetti che intervengono a vario titolo nella gestione di un trattamento: partendo dal soggetto privacy "protagonista" e sempre presente quando siamo di fronte ad un trattamento di dati, vale a dire il titolare del trattamento (articolo 4), possono poi interporsi responsabili e sub-responsabili del trattamento (articolo 28), contitolari del trattamento (articolo 26) e, infine, autorizzati al trattamento (articolo 4).

Responsabile del trattamento - In particolare, il responsabile del trattamento rappresenta quel soggetto che tratta i dati personali "per conto" del titolare in relazione a taluni trattamenti specificatamente individuati nel contratto (o altro atto giuridico a norma del diritto dell'Ue) che disciplina i rapporti tra titolare e responsabile del trattamento. L'articolo 28, GDPR prevede che il titolare del trattamento «ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato».

Il Considerando n. 81 al GDPR aggiunge che le "garanzie sufficienti" che devono presentare i responsabili del trattamento vanno letti in termini di conoscenza specialistica, affidabilità e risorse, elementi necessari in vista della messa in atto di misure tecniche e organizzative in grado di soddisfare il rispetto della normativa privacy, anche in relazione alla sicurezza del trattamento.

Anche l'Europea Data Protection Board (EDPB) con le **Linee guida n. 7/2020 adottate il 7 luglio 2021** sui concetti di titolare e responsabile del trattamento evidenzia l'essenzialità del processo di selezione dei responsabili e la necessaria contrattualizzazione del rapporto tra i due soggetti.

Il contratto deve vincolare il responsabile al titolare e specificare la materia disciplinata, la durata, la natura e la finalità del trattamento,

il tipo di dati personali oggetto del trattamento e le categorie di interessati coinvolti, gli obblighi e i diritti del titolare del trattamento.

Il contratto deve indicare che il responsabile:

- Tratti i dati personali soltanto su istruzione documentata del titolare;
- Garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza (per esempio con nomine a incaricato, ad amministratore di sistema, ad addetto alla videosorveglianza ecc.)
- Adotti tutte le misure tecniche e organizzative richieste dall'articolo 32, GDPR, vale a dire pseudonimizzazione, cifratura, capacità di assicurare riservatezza, integrità, disponibilità, resilienza, ripristino dei dati, procedura di test ed efficacia delle misure adottate, risk assessment (per perdita, distruzione, modifica, divulgazione);
- Tenendo conto della natura del trattamento, assista il titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (in questo contesto può essere importante avere un risk e privacy impact assessment per dimostrare di aver adottato misure tecniche ed organizzative adeguate);
- Assista il titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, GDPR (quindi in relazione alle notifiche di data breach, alle comunicazioni di data breach agli interessati coinvolti, redazione della DPIA) tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile;
- Su scelta del titolare, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati (in partica, il titolare deve comunicare al responsabile la propria politica di data retention e cancellazione);
- Metta a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto dei propri obblighi e consenta le attività di audit, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato (pertanto il titolare ha il dovere di verificare con audit periodici le "credenziali" del responsabile del trattamento e, di converso, il responsabile ha l'obbligo di consentire l'effettuazione degli audit).

Verifiche ex ante e periodiche sul responsabile del trattamento - In generale, il titolare del trattamento è tenuto a dimostrare, in virtù del principio di accountability, di governare la filiera dei partner di trattamento.

La domanda cruciale è: come lo dimostra concretamente? La dimostrazione del corretto governo della filiera dei partner/fornitori (che poi saranno nominati "responsabili del trattamento") si esplica in momenti diversi.

Infatti, l'attività di verifica su tali soggetti va fatta sia ex ante, vale a dire dal momento della selezione del responsabile del trattamento, sia ex post considerando i controlli periodici effettuati sottoforma di audit sulla gestione dei dati effettuata dal responsabile stesso, che temporalmente vanno svolti lungo tutto il rapporto contrattuale.

Quindi, per verificare fin da subito se il responsabile può essere un soggetto che garantisce un trattamento dei dati compliance privacy, il titolare del trattamento deve procedere con la valutazione, caso per caso, del risk assessment del responsabile/fornitore fin dalla fase della selezione.

Sarebbe utile utilizzare una check-list oppure un questionario da far compilare alla società fornitrice in modo da verificare vari aspetti, che vertono, per esempio:

- Sulla verifica di un corretto "assetto privacy" (presenza, per esempio, dei seguenti documenti: registro dei trattamenti di dati personali, informative privacy, accordi, procedure per la gestione dei data breach o per la gestione dell'esercizio dei diritti degli interessati, policy di data retention);
- Sull'eventuale nomina di un DPO;
- Sulla presenza di misure tecniche ed organizzative e adeguate;
- Sulla verifica della presenza di un approccio privacy by design e by default;
- Sulla verifica di eventuali trasferimenti dati extra-Ue.

Naturalmente sarebbe molto efficace poter effettuare tali verifiche parallelamente all'analisi dell'impianto, se esistente, del Modello 231 e/o all'analisi degli asset concernenti gli obblighi antiriciclaggio.

Dopo tale fase di selezione, se il titolare del trattamento considera idoneo il fornitore sulla base del suo assetto, delle sue comprovate competenze ed esperienze, della sua affidabilità e delle risorse che mette a disposizione dovrebbe innanzitutto documentare tale decisione per poi procedere con la stipula dell'accordo ai sensi dell'articolo 28, GDPR, disciplinante tutti gli elementi sopra descritti.

Poi, come detto, durante il rapporto contrattuale il titolare del trattamento dovrà effettuare un'analisi periodica sull'attività del responsabile del trattamento nominato attraverso degli specifici audit.

Caso sanzionato dal Garante privacy - Il provvedimento sanzionatorio emanato dal Garante privacy anticipato in premessa (di cui al Registro dei provvedimenti n. 349 del 20 ottobre 2022) ci ha dato lo spunto per approfondire fin qui la tematica della filiera dei partner di trattamento e per la sua corretta governance.

La vicenda ha avuto origine dalla segnalazione di un cittadino che ha lamentato la ricezione, via e-mail, di una comunicazione indesiderata proveniente da un indirizzo di posta non direttamente ricollegabile alla società con cui l'interessato aveva avuto dei rapporti (di seguito anche "società X"), ma avente ad oggetto la promozione di prodotti offerti dalla società X stessa.

In realtà, infatti, la mail proveniva da una società di marketing che svolgeva l'attività di promozione dei prodotti della società X, la quale era la committente l'attività promozionale stessa, che, lato privacy, si configurava quale titolare del trattamento. A quest'ultimo riguardo, con riferimento ai ruoli privacy, l'Autorità di controllo nel provvedimento in commento ha ricordato sia le Linee guida dell'EDPB n. 7/2020 sia alcuni suoi provvedimenti dove ha più volte affermato che il committente di una campagna promozionale, indipendentemente dalla materiale raccolta dei dati, deve ritenersi titolare del trattamento avendo in concreto determinato, nella ricorrente prassi relativa a tale settore, le decisioni in ordine alle finalità e ai mezzi essenziali del trattamento stesso.

Il reclamante aveva avanzato una formale richiesta di chiarimenti sul trattamento dei propri dati personali alla società incaricata all'attività di marketing, la quale avrebbe dovuto essere stata nominata responsabile del trattamento ai sensi dell'articolo 28 GDPR dalla società X committente l'attività promozionale (nella fattispecie, la nomina non era stata effettuata).La società di marketing non riscontrava l'interessato, pertanto quest'ultimo inviava un reclamo al Garante privacy dichiarando di non aver mai conferito il consenso alla ricezione della comunicazione promozionale e lamentando il mancato riscontro alla richiesta di esercizio dei diritti di cui agli articoli 15, 17 e 21, GDPR.

L'Autorità di controllo chiedeva informazioni alla società titolare del trattamento, la quale dichiarava la propria estraneità in relazione alla condotta lamentata nel reclamo, precisando che i dati dell'interessato sono risultati presenti nelle liste di contatti di un'altra società di cui la società si avvaleva per la gestione dell'attività di marketing.

La società X sanzionata, ha sottolineato il Garante privacy nel provvedimento in esame, non è stata in grado di comprovare l'adozione di adeguate misure tecniche e organizzative, come richiesto dagli articoli 5, par. 2, e 24 del GDPR, norme che inquadrano le competenze del titolare in un'ottica di responsabilizzazione (accountability) finalizzata a comprovare gli adempimenti effettuati in materia di protezione dei dati personali.

In particolare, il Garante ha considerato il riscontro fornito dalla società indicativo dell'incapacità di controllare efficacemente la filiera dei partner che effettuano attività promozionale a suo vantaggio. Di conseguenza, è stata contestata alla società X la violazione degli articoli 5, par. 2, e 24, GDPR, nonché degli articoli 12, 15, 17 e 21, GDPR, non essendo stata riscontrata, nei termini richiesti, l'istanza di esercizio dei diritti formulata dall'interessato, oltre che la violazione dell'art. 6, par. 1, lett. a), GDPR e dell'articolo 130 del

Codice privacy, in ragione dell'invio all'interessato reclamante di una e-mail promozionale in assenza di un consenso libero, specifico, documentato ed inequivocabile.

Fonte: Il Sole 24 Ore (di Elisa Chizzola)