5 octubre 2020

GDPR: interrogativi sui concetti di titolare, responsabile e contitolare del trattamento

Milano, 5 ottobre 2020 – Dopo l'entrata in vigore del GDPR sono stati sollevati vari interrogativi in merito ai suoi effetti sui concetti di titolare, responsabile e contitolare del trattamento, in particolare per quanto riguarda la nozione di contitolarità del trattamento (di cui all'articolo 26 del GDPR, anche alla luce di alcune sentenze della CGUE), nonché gli obblighi dei responsabili del trattamento (fissati, in particolare, all'articolo 28 del RGPD) di cui al capo IV del GDPR.

Nel marzo 2019 il Comitato Europeo per la Protezione dei Dati (EDPB), insieme al suo segretariato, ha organizzato un evento pubblico con le parti interessate che ha segnalato chiaramente la necessità di orientamenti più pratici e ha consentito al Comitato di comprendere meglio le esigenze e le preoccupazioni in tale ambito.

Il 2 settembre 2020 l'EDPB ha adottato delle Linee Guida sui concetti di titolare, responsabile e contitolare del trattamento (Guidelines 07/2020 on the concepts of controller and processor in the GDPR) il cui testo è sottoposta a pubblica consultazione fino al prossimo 19 Ottobre.

Le nuove linee-guida si articolano in due sezioni principali: una prima sezione in cui sono illustrati i singoli concetti, e una seconda sezione contenente orientamenti dettagliati sulle principali conseguenze che ne derivano per i titolari e i responsabili del trattamento nonché per i contitolari del trattamento. Un diagramma di flusso fornisce ulteriori orientamenti pratici.

Più nel dettaglio:

- **Titolare del trattamento**, ex art 4.(7)GDPR 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 di dati personali.

L'individuazione del ruolo di titolare deve avvenire sulla base di un'analisi delle concrete attività svolte con riferimento al trattamento in uno specifico contesto, poco rileva la designazione formale. A tale riguardo riveste un ruolo particolarmente cruciale l'aspetto della determinazione dei mezzi: il potere decisionale del titolare con riferimento ai mezzi deve riferirsi agli aspetti fondamentali dei mezzi – quali la tipologia di dati personali trattati (quali dati devo trattare?), la durata del trattamento, le categorie di destinatari (chi ha accesso ai dati?) e le categorie di interessati – laddove la decisione delle questioni sia tecniche che organizzative "non essenziali" – (ad es. "quale hardware o software utilizzare?") – può anche essere delegata al responsabile.

Altro aspetto importante toccato dall'EDPB perché spesso fonte di equivoci è la precisazione che non è necessario che il titolare del trattamento abbia effettivamente accesso ai dati personali che vengono trattati per essere qualificato come titolare del trattamento.

ll potere decisionale su finalità e mezzi, infine, può derivare dalla legge o dedotte dalle circostanze concrete (possono derivare dalle competenze professionali con riferimento ad alcuni tipi di attività o devono essere determinate dai termini dedotti in contratto, valutando le concrete specifiche circostanze).

Esempi concreti di titolarità del trattamento: a) lo studio legale per quanto riguarda il trattamento dei dati svolto nell'ambito della rappresentanza legale del cliente; b) il contabile, quando fornisce servizi ai clienti sulla base di istruzioni molto generali (le linee guida danno l'esempio di un audit dettagliato), senza istruzioni dettagliate da parte del cliente; c) la banca nell'esercizio della propria attività tipica.

- L'art. 26 GDPR dispone che allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono **contitolari del trattamento**.

La qualifica di contitolare può sorgere quando più attori partecipano

congiuntamente nella determinazione di finalità e mezzi di una o più specifiche attività di trattamento, sia in seguito a una decisione comune presa da due o più soggetti oppure come risultato di decisioni convergenti, quando tali decisioni si completano a vicenda e sono necessarie per il trattamento in modo tale da avere un impatto tangibile sulla determinazione delle finalità e delle modalità del trattamento.

Le Linee Guida indicano un criterio importante da seguire per determinare la contitolarità, ovvero la verifica del fatto che senza la partecipazione di entrambe le parti il trattamento non sarebbe possibile: il trattamento da parte di ciascuna parte risulta, quindi, inscindibile, ovvero inestricabilmente legati.

La partecipazione congiunta deve avvenire sia con riferimento alla determinazione delle finalità che alla determinazione dei mezzi. Il fatto che una delle parti non ha accesso ai dati personali non è da sola sufficiente a escludere la contitolarità.

La sussistenza di una contitolarità non implica necessariamente una responsabilità uguale tra i soggetti coinvolti. I contitolari determinano e concordano in modo trasparente le rispettive responsabilità in merito al rispetto degli obblighi previsti dal GDPR: l'esercizio dei diritti degli interessati e gli obblighi di fornire informazioni, ai sensi degli articoli 13 e 14, il rispetto dei principi generali di protezione dei dati, le basi giuridiche, le misure di sicurezza, gli obblighi di notifica in caso di data breach, la valutazione dell'impatto, il ricorso a responsabili del trattamento, i trasferimenti dei dati in paesi terzi e le comunicazioni con gli interessati e le autorità di controllo.

In assenza di prescrizioni sulla forma di tale accordo nel GDPR l'EDPB raccomanda che sia stipulato un contratto o altro atto giuridico vincolante secondo il diritto degli Stati membri.

Come disciplina l'art. 26 GDPR, indipendentemente dalle disposizioni dell'accordo di contitolarità, l'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento, non essendo tale accordo vincolante per l'interessato, così come non risulta vincolante nei confronti dell'Autorità di controllo.

Esempi pratici di contitolarità: a) l'agenzia di viaggi, la compagnia aerea e l'hotel che decidessero di creare una piattaforma online comune per perseguire i loro fini congiuntamente ad es. per gestire i servizi di prenotazione e, condividendo i dati dei clienti, effettuare attività integrate di marketing; b) le società che lancino sul mercato un prodotto co-branded e un evento per promuovere questo prodotto, condividendo i dati dei rispettivi clienti e prospects e definendo la lista degli invitati all'evento.

- **Responsabile** per l'art. 4 (8) GDPR) è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Per qualificare un soggetto "responsabile" devono sussistere due requisiti essenziali: deve essere un soggetto distinto dal titolare del trattamento; deve trattare i dati personali per conto di quest'ultimo (nell'interesse del titolare). Le linee guida ribadiscono che il responsabile del trattamento non deve trattare i dati personali se non su istruzione documentata del titolare del trattamento. Sul contenuto delle istruzioni del titolare sussiste un margine di discrezionalità, consentendo al responsabile del trattamento di scegliere i mezzi tecnici e organizzativi maggiormente idonei.

L'art. 28 GDPR impone al titolare di ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, tali da soddisfare i requisiti del Regolamento. Le Linee Guida individuano tra i parametri che devono guidare questa valutazioni la considerazione delle conoscenze specifiche da parte del fornitore (ad es. con riguardo alle misure tecniche e alla gestione dei data breach), l'affidabilità del fornitore, le sue risorse e l'eventuale aderenza a codici di condotta e meccanismi di certificazione.

Il rapporto tra titolare e responsabile deve essere regolato da un contratto o da un atto che abbia potere di vincolare le parti secondo la normativa dello Stato Membro e che deve essere provato per iscritto.

I responsabili possono scegliere di negoziare il testo oppure di utilizzare clausole contrattuali standard, ciò che rileva è che includano gli elementi richiesti dall'art. 28 GDPR, ma evitando di riportare pedissequamente il dettato normativo, quanto

piuttosto includendo informazioni specifiche e concrete su come i requisiti richiesti dall'art. 28 sono rispettati, nonché il livello di sicurezza richiesto per lo specifico trattamento di dati personali oggetto del contratto. A tale riguardo le Linee Guida chiariscono un aspetto rilevante, sgomberando il campo da dubbi. Ai fini della qualificazione dei rispettivi ruoli non ha importanza se il testo di accordo è predisposto da una o dall'altra parte: la prassi conferma, infatti, che in molti casi i fornitori di servizi, responsabili del trattamento, stabiliscono servizi e contratti standard da far firmare ai titolari. A tale proposito l'EDPB specifica che il fatto che il contratto e le sue condizioni generali siano preparate dal fornitore di servizi invece che dal titolare, in primo luogo, non basta in sé per far concludere che il fornitore di servizi debba essere considerato come un titolare, e in secondo luogo, comporta che il titolare, nella misura in cui ha liberamente accettato le clausole contrattuali, ne assuma di conseguenza la piena responsabilità. Analogamente, lo squilibrio fra il potere contrattuale di un piccolo titolare del trattamento rispetto a un grosso fornitore di servizi non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla protezione dei dati.

Un responsabile del trattamento viola il GDPR se va oltre le istruzioni del titolare del trattamento e inizia a determinare le proprie finalità e le proprie modalità di trattamento; in questo caso il responsabile del trattamento sarà considerato a o propria volta un titolare del trattamento.

Esempio tipico di responsabile la figura del cloud provider.