filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Guida II al Regolamento Privacy UE 2016/679: i principi generali del trattamento e l'accountability o responsabilizzazione

23 Maggio 2017
Marco Dettori, Iusgate

Introduzione

Il Regolamento (UE) 216/679 sulla "*Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*" ("Regolamento"), la cui applicazione è prevista a partire dal 25 maggio 2018 in tutti gli Stati Membri, **tra le novità introdotte rispetto alla Direttiva 95/46/CE** ("Direttiva"), include un importante istituto che si innesta tra i principi cardine applicabili al trattamento dei dati personali, come elencati all'articolo 5, Capo II del Regolamento: il **principio di responsabilizzazione** ("*accountability*").

Tale principio, non espressamente previsto dalla Direttiva, era stato oggetto di analisi specifica da parte del Gruppo di Lavoro *ex* articolo 29 ("Garante Europeo") nel parere n.3/2010, con il quale il Garante Europeo, in prospettiva futura, rivelava **la necessità che il trattamento dei dati personali all'interno dell'Unione Europea fosse ispirato e guidato da un generale principio di responsabilità**, inteso come motore di attuazione di tutti gli altri principi su cui si fonda la tutela dei dati personali.

Principio di responsabilizzazione

L'articolo 5, al paragrafo 1, elenca i principi applicabili al trattamento dei dati personali, riprendendo in parte quelli già enunciati nella Direttiva (liceità e correttezza) e specificando più nel dettaglio il contenuto di altri (trasparenza, minimizzazione, esattezza, limitazione di conservazione, integrità e riservatezza).

Il paragrafo 2 del medesimo articolo introduce il principio di responsabilizzazione, così espresso: "***il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo***".

La portata generale del principio rappresenta una delle chiavi di lettura dell'intero Regolamento. Per responsabilizzazione, infatti, deve intendersi **la presa di coscienza attiva, da parte dei titolari del trattamento, della necessità di una protezione dei dati personali degli interessati e della conseguente conformità del trattamento alla nuova disciplina**.

In sostanza, il principio di responsabilizzazione richiede **un diverso approccio applicativo delle disposizioni del Regolamento** rispetto alla Direttiva, "ribaltando" sui titolari del trattamento un **obbligo di autovalutazione** rispetto a

- trattamento effettuato,
- tipologia dei dati personali trattati,
- rischi derivanti da tale trattamento e, soprattutto,
- adeguatezza delle misure tecniche e organizzative predisposte affinché il trattamento sia conforme al Regolamento.

L'*accountability*, come sopra esposta, è allineata con i nuovi principi di protezione dei dati "fin dalla

progettazione" (*privacy by design*) e "per impostazione predefinita" (*privacy by default*), introdotti dall'articolo 25 del Regolamento.

La valutazione di conformità, infatti, deve essere effettuata dai titolari "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento*" (articolo 25, paragrafo 1). Altresì, il titolare deve valutare, scegliere e mettere 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*" (articolo 25, paragrafo 2).

L'ulteriore elemento che discende dal principio di responsabilizzazione – e che ha una rilevante conseguenza sul piano pratico – è riscontrabile nell'**obbligo di dimostrazione, gravante sul titolare del trattamento, di aver rispettato i principio generali di cui al paragrafo 1 dell'articolo 5 e di aver adottato misure tecniche e organizzative adeguate** (paragrafo 1, articolo 24).

È essenziale, pertanto, che la responsabilizzazione del titolare del trattamento debba essere intesa (oltre che come autovalutazione di conformità) anche come **acquisizione di evidenze probatorie finalizzate a comprovare che le disposizioni del Regolamento siano state rispettate** e, quindi, che il trattamento è ad esso conforme.

Strumenti operativi per l'attuazione del principio

Il Regolamento fornisce alcuni spunti operativi ai fini **dell'attuazione del principio di responsabilizzazione e della dimostrazione del rispetto del medesimo**. Tali indicazioni sono rivolte, in alcuni casi, agli Stati Membri (con un margine d'intervento conferito agli stessi mediante atti di normazione nazionale), in altri, direttamente ai titolari del trattamento (mediante l'adozione di particolari procedure di trattamento e il rispetto di specifici adempimenti).

A titolo esemplificativo, i considerando 77 e 81 fanno riferimento ai **Codici di Condotta e ai sistemi di certificazione dei trattamenti come utili strumenti idonei a dimostrare la conformità del trattamento alle disposizioni del Regolamento** (e conseguentemente l'effettiva attuazione del principio di responsabilizzazione).

Inoltre, in ambito aziendale, vale la pena considerare **l'adozione di standard** per la valutazione dei rischi, la mappatura dei dati e dei trattamenti e, in generale, di sistemi di assessment aziendale che contribuiscano a costituire la compliance alla normativa privacy (a titolo esemplificativo si fa riferimento allo standard ISO 27001, 29134, 30001 e Linee Guida CNIL 2015).

Il considerando 82 prevede che il titolare del trattamento o il responsabile del trattamento "***per dimostrare che si conforma al presente regolamento*** – in attuazione del suddetto principio – *dovrebbe tenere* ***un registro delle attività di trattamento effettuate sotto la sua responsabilità***. ***Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione*** *affinché possano servire per monitorare detti trattamenti*".

Fatta salva l'obbligatorietà della tenuta del registro dei trattamenti soltanto per i titolari che soddisfino le condizioni di cui all'articolo 30 del Regolamento (si tratta di imprese o organizzazioni con più di 250 dipendenti e, comunque, dei titolari che effettuano trattamenti rischiosi per le libertà e i diritti degli interessati e dei trattamenti di particolari categorie di dati), in ogni caso, il citato considerando **caldeggia l'utilizzo di tale registro da parte di ogni titolare, al fine di dare attuazione efficace al principio di responsabilizzazione, soprattutto, in ordine alla capacità probatoria delle misure adottate**

.

Gli istituti del "*data breach*" – inteso come obbligo di comunicazione dell'avvenuta violazione di dati personali – e del *Data Privacy Officer* ("DPO") – come introduzione di una nuova figura professionale nelle strutture aziendali – seguono la logica del registro dei trattamenti. Pertanto, **nonostante l'applicazione obbligatoria di tali istituti sia prevista solo in alcune ipotesi tassative, in ogni caso, la relativa disciplina dovrebbe ispirare tutti i titolari dei trattamenti all'adozione di condotte "responsabili e coscienti"**, basate su una **valutazione preliminare** dei rischi derivanti dal trattamento e sull'adeguatezza delle misure da adottare e, in generale, su una forte consapevolezza dell'importanza della normativa sulla protezione dei dati personali.

Conclusioni

È evidente come la portata generale del principio di responsabilizzazione investa l'intera disciplina del Regolamento e, in alcuni casi, risulti strettamente connessa con specifici istituti.

Fermo restando il regime sanzionatorio del Regolamento, il principio di responsabilizzazione **dovrebbe guidare *ab origine* la condotta dei titolari del trattamento, i quali, avendo contezza dell'importanza dell'intera disciplina, devono orientare e conformare l'attività da cui dipende il trattamento di dati personali alle disposizioni del Regolamento, facendone propri i principi cardine**.

L'evoluzione normativa del Regolamento, rispetto alla precedente Direttiva, **prevede l'ingresso e il recepimento dei principi in materia di protezione dei dati personali all'interno delle strutture aziendali**.

Il tema della *data protection*, infatti, ha da sempre avuto un peso marginale (o inesistente) nelle articolazioni aziendali (soprattutto per quelle facenti capo alle piccole e medie imprese) e il principio di responsabilizzazione si pone in tal senso come principio-guida per tutti i titolari del trattamento, affinché **il tema della protezione dei dati personali entri a far parte a pieno titolo nell'organizzazione aziendale** , come in passato è accaduto per il recepimento della normativa sulla sicurezza sul lavoro.

TAG: *accountability, Guida Regolamento UE Privacy, principio di responsabilità, Regolamento privacy, sicurezza sul lavoro, GDPR, Diritto dell'Unione Europea, Diritto della concorrenza e della pubblicità, Diritto della privacy, Diritto delle nuove tecnologie e delle comunicazioni*

Avvertenza