Privacy

I registri delle attività di trattamento

di **Pietro Maria Mascolo, Vincenzo Colarocco**

I registri delle attività di trattamento si sostanziano in una tipica traduzione a livello pratico del più ampio principio di *accountability* che permea il Regolamento Europeo 679/16 per la protezione dei dati personali (GDPR o Regolamento).

Il detto principio, altresì noto come principio di *rendicontazione* o di *responsabilità*, impone al titolare del trattamento l'obbligo di dimostrare l'adozione di un processo complessivo di misure giuridiche, amministrative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi. In altri termini, si richiede al titolare un ampio margine di proattività, diviene fondamentale assumere delle scelte ponderate che si traducano nell'adozione di misure adeguate, efficaci ed in grado di dimostrare la conformità delle attività di trattamento con il GDPR.

È proprio il concetto di *dimostrazione di corretto adempimento* alla base della disciplina in materia di registri delle attività di trattamento. Tanto si può espressamente desumere sin dal Considerando 82 anteposto al fulcro normativo del Regolamento, a mente del quale *per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità*.

L'art. 30 del GDPR conferisce dignità prescrittiva al suesposto Considerando, prevedendo che tutti i titolari ed i responsabili del trattamento, con oltre 250 dipendenti, predispongano un **registro delle operazioni**. I contenuti sono indicati all'interno del medesimo articolo[1]. **Trattasi, quindi, non di un mero adempimento formale, bensì di una parte integrante di un sistema di corretta gestione dei dati personali, in quanto espressamente finalizzato a tenere sotto controllo il ciclo vitale del dato.**

Le informazioni contenute nel Registro sono da considerarsi come *minime*: il titolare può aggiungerne di ulteriori a seconda della propria realtà organizzativa e del tipo di attività svolta, come ad esempio il proprio *asset* immateriale.

La norma riporta, inoltre, una serie di specifici obblighi posti in capo al responsabile del trattamento e, ove applicabile, al suo rappresentante (cfr. art. 30, par. 2, GDPR).

Tuttavia è doveroso precisare come l'obbligo di redazione e adozione del registro non è generale, in quanto non compete *alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà*

dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a resti di cui all'articolo 10 (art. 30, paragrafo 5 del GDPR).

Ciò non esclude che, in determinate circostanze, anche nell'ipotesi in cui non sia obbligatorio adottare il registro dei trattamenti, sarebbe opportuno implementarlo, in quanto strumento utile per censire tutti i trattamenti operati (ad esempio con riferimento agli studi professionali in cui non vengono trattate categorie 'particolari' di dati). Tanto è stato ribadito anche dal *Working Party* 29 (WP29) con un recente parere dell'aprile del 2018 mediante il quale, pur ribadendo le circostanze di deroga dalla tenuta dei registri di cui all'art. 30, par. 5, GDPR, si ribadisce come tale attività costituisca uno strumento assai utile sia per supportare l'analisi delle implicazioni che derivano da ogni trattamento, sia per correttamente valutare il rischio che ne deriva ed implementare le misure di sicurezza da approntare; il tutto nel pieno rispetto del fondamentale principio dell'*accountability*.

In generale, il GDPR non prevede un'eccezione a seconda delle dimensioni dell'organizzazione del titolare e/o del responsabile, ad esempio per le piccole e medie imprese. L'approccio al rischio riflesso in una serie di obblighi del Regolamento non è adatto a questo tipo di eccezione. Per lo meno, sarebbe incoerente considerare che, in ogni caso, le dimensioni dell'organizzazione di un titolare o di un responsabile del trattamento si traducano in una mancanza di rischio o un basso rischio per i diritti e le libertà delle persone. Infatti, il Considerando 13 del GDPR rinvia per la nozione di micro, piccole e medie imprese alla raccomandazione 2003/361/CE della Commissione che, in allegato all'articolo 1, considera *impresa ogni entità, a prescindere dalla forma giuridica rivestita, che eserciti un'attività economica. In particolare sono considerate tali le entità che esercitano un'attività artigianale o altre attività a titolo individuale o familiare, le società di persone o le associazioni che esercitino un'attività economica*". L'articolo 2 della stessa raccomandazione precisa che *la categoria delle microimprese delle piccole imprese e delle medie imprese (PMI) è costituita da imprese che occupano meno di 250 persone.*

Per quanto specificamente attiene alle modalità operative mediante le quali predisporre il registro, si evidenzia anzitutto come la compilazione dello stesso possa essere fatta con una pluralità di strumenti: dal semplice foglio di carta ad un file *Excel*, sino all'adozione di un *software* dedicato (cd. "tool"). Come già sottolineato in precedenza, le informazioni da inserire nel Registro non sono identiche a seconda che il trattamento sia eseguito dal titolare o da un responsabile, sussistono, ad ogni modo, dei denominatori comuni che riguarderanno le finalità per le quali i dati vengono trattati (come ad esempio, per gestione dei servizi di marketing, ecc.), le categorie di interessati coinvolti nel trattamento dei dati (dipendenti, utenti, lavoratori autonomi, ecc.), i destinatari dei dati (Paesi terzi, Extra UE, Organizzazioni internazionali, ecc.), il periodo di conservazione dei dati, ecc..

Sempre con riferimento all'aspetto 'pratico' dell'argomento in esame, risulta infine doveroso segnalare che il Garante Privacy Italiano ha di recente pubblicato delle interessanti 'FAQ' espressamente focalizzate sul tema dei registri delle attività di trattamento. Si rinvengono

interessanti informazioni circa aspetti essenziali della disciplina (su tutte, una serie di chiarimenti circa le figure tenute alla compilazione dei registri; le informazioni essenziali da riportare negli stessi; le relative modalità di prescrizione e conservazione) e, inoltre, si possono rinvenire dei "**Modelli di registro semplificato delle attività di trattamento**" (sia del titolare che del responsabile) utilizzabili dalle PMI.

[1] Più specificamente, il registro, in formato scritto o elettronico, dovrà essere munito delle seguenti informazioni: *i) il nome e i dati di contatto del titolare del trattamento; ii) i dati identificati, se presenti, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; iii) le finalità del trattamento; iv) una descrizione delle categorie di interessati; v) una descrizione delle categorie di dati personali; vi) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; vii) se applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; viii) i termini ultimi previsti per la cancellazione delle diverse categorie di dati; ix) una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1, ovvero:*

1. *la pseudonimizzazione e la cifratura dei dati personali;*
2. *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
3. *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*
4. *una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*