NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY: GLI ADEMPIMENTI DI BASE

PAOLO FOTI

Sono pienamente operative le disposizioni del Regolamento (UE) 2016/679 in tema di trattamento dei dati personali che promuovono un'idea di privacy innovativa, incentrata sulla responsabilizzazione delle figure coinvolte nel processo di protezione dei dati e sono intese a semplificare gli adempimenti e a minimizzare eventuali dispersioni ed illecite esposizioni dei dati personali altrui. A queste norme non sfuggono i singoli liberi professionisti delle professioni tecniche che dovranno attenersi alle nuove regole. Nell'articolo sono illustrati gli adempimenti di base al fine di adeguarsi alle novità normative in materia.

Dallo scorso 25 maggio trova piena applicazione la nuova normativa in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che, come previsto dall'art. 99 "entrata in vigore e applicazione" dello stesso regolamento, è obbligatoria in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri abrogando contestualmente la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Il nuovo "Regolamento Europeo" ha modificato radicalmente l'approccio adottato finora per la regolamentazione della protezione dei dati personali, introducendo in modo espresso nel sistema legislativo di settore principi fino ad oggi lontani dal nostro ordinamento, basti pensare al concetto di "privacy by design" e "privacy by default" ed attribuendo, tra questi, un ruolo di centralità a quello così detto di "responsabilizzazione" sia del titolare che del responsabile del trattamento (accountability).

Partendo proprio dal concetto, di "accountability", volto ad una effettiva garanzia dell'interessato (qualsiasi informazione, ovvero "dato personale", riguardante una persona fisica identificata o

identificabile), in un'ottica di massima trasparenza (intesa come garanzia della completa accessibilità alle informazioni dei cittadini in quanto utenti di un servizio sia esso generico e/o specialistico), al "titolare del trattamento" è affidato l'incarico di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati. Questo significa che dovrà essere in grado, in qualsiasi momento, di garantire gli adempimenti agli obblighi previsti sia dalle norme a carattere cogente sia da regolamenti tecnici di riferimento (es. linee guida Garante delle Privacy) e l'efficacia della tutela predisposta, in un bilanciamento di discrezionalità di adempimenti e responsabilità per la verifica della loro efficacia, ivi compreso il riesame e l'aggiornamento costante di tutte le condizioni adottate.
Nello specifico sia il "Titolare" sia il "Responsabile del trattamento dei dati" dovranno predisporre un sistema che, sin dall'inizio dell'attività (processo di trattamento del dato personale), limiti possibili violazioni dei dati raccolti (privacy by design) e che quest'ultimo sia implementato di specifiche misure che garantiscano un idoneo trattamento dei dati, che dovrà essere personalizzato, a seconda delle finalità e del tipo di operazioni da porre in essere (privacy by default).

In buona sintesi, il Regolamento Europeo promuove una idea di privacy nuova e innovativa, incentrata sulla responsabilizzazione delle figure coinvolte a vario titolo nel processo di protezione dei dati personali, volta da un lato a semplificare gli adempimenti sul trattamento dei dati, dall'altro lato, a minimizzare eventuali dispersioni ed illecite esposizioni dei dati personali altrui.
A queste dinamiche non sfuggono anche i singoli liberi professionisti delle c.d. professioni tecniche o comunque organizzati in piccoli studi, i quali dovranno adeguarsi alle nuove regole in materia di trattamento dei dati personali.
Di seguito si riportano le novità più significative in relazione agli adempimenti necessari ai fini del rispetto della normativa, ricordando tuttavia che tali indicazioni hanno valore indicativo, limitandosi a delineare le regole basilari comuni previste nel Regolamento comunitario.
L'esistenza, in capo all'interessato, di una **serie di diritti** che dovrebbero permettergli di controllare e gestire consapevolmente il flusso dei propri dati e, in particolare: (i) diritto di **accesso** ai dati, (ii) il diritto di chiederne la **rettifica**, la **cancellazione**, o la **limitazione** del trattamento, (iii) il diritto di **opporsi** al trattamento, (iv) il diritto alla **portabilità** dei dati, (v) il diritto di **revocare il consenso** al trattamento, in qualsiasi momento e (vi) il diritto di **proporre reclamo** all'autorità di controllo: è infatti compito del titolare far conoscere all'interessato quali siano questi diritti e come procedere per esercitarli concretamente (oltre a predisporre delle procedure semplici ed efficaci per darvi esecuzione).

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

(art. 5 - Regolamento "UE" 2016/679)

Ai sensi dell'art. 5 del Regolamento i dati debbono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato e le finalità dovranno essere ben determinate, esplicite e legittime.
Questo impone al titolare del trattamento di fornire all'interessato una informativa chiara, semplice e facilmente accessibile che gli permetta di controllare i propri dati, quali: eventuali trasferimenti all'estero dei dati (a tal fine si raccomanda di prestare particolare attenzione a titolo esemplificativo alla localizzazione di server, servizi in hosting, cloud, ecc.), il diritto di accesso, rettifica, cancellazione e/o diritto all'oblio, portabilità, limitazione del trattamento ed opposizione.

LICEITÀ DEL TRATTAMENTO E CONSENSO
(art. 6 - Regolamento "UE" 2016/679)

Ogni trattamento dovrà trovare fondamento all'interno di una adeguata base giuridica, come ad esempio l'esecuzione di un contratto, l'adempimento ad un obbligo legale, l'esecuzione di un compito di interesse pubblico, il perseguimento di un legittimo interesse, etc.
Come naturale che sia, condizione fondamentale della liceità del trattamento è il consenso da parte dell'interessato.

CONDIZIONI PER IL CONSENSO
(art. 7 - Regolamento "UE" 2016/679)

Il consenso da parte dell'interessato dovrà essere prestato in maniera chiara, semplice e in forma comprensibile e facilmente accessibile.
A tal proposito è obbligo ricordare che il nuovo regolamento non prevede obbligatoriamente la forma scritta, ma tuttavia per completezza di informazione è giusto ricordare che in capo al titolare del trattamento, sempre ai sensi dello stesso articolo, vige l'obbligo di "dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali" ed è evidentemente raccomandabile l'opportunità di provvedere all'acquisizione del consenso in forma scritta.
Tuttavia è giusto ricordare che esistono delle eccezioni, come ad esempio il trattamento di "dati particolari" di cui all'art. 9 (*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*) e il trattamento automatizzato ivi compresa la "profilazione" (*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*).

REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO
(art. 30 - Regolamento "UE" 2016/679)

Il "registro dei trattamenti" è uno strumento fondamentale ai fini sia della mappatura dei dati raccolti e degli strumenti impiegati per il trattamento dei dati e la loro protezione sia per il monitoraggio degli adempimenti e della garanzia dei diritti previsti dal Regolamento Europeo.
Tuttavia questo non è obbligatorio per il titolare del trattamento che occupi meno di 250 dipendenti a patto che il trattamento possa presentare un rischio per i diritti e le libertà degli interessati, non sia occasionale o includa le categorie particolari di cui all'articolo 9, condanne penali o reati riconducibili all'articolo 10.
Inoltre, i titolari che debbano iniziare un trattamento molto rischioso per i diritti e le libertà delle persone fisiche, per le caratteristiche del trattamento o degli strumenti adottati per esso (ad esempio novità tecnologiche, finalità, natura dei dati), sono tenuti ai sensi dell'art. 35 anche alla "valutazione d'impatto del trattamento dei dati" e, laddove ne risulti un rischio elevato, sempre il titolare è tenuto a consultare preventivamente l'organo di controllo competente.
La pseudonimizzazione è una tecnica che consiste nel conservare i dati in una forma che impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive.

SICUREZZA DEI DATI PERSONALI
(art. 32 - Regolamento "UE" 2016/679)

Tenendo conto delle specifiche caratteristiche del trattamento e dei connessi profili di rischio per i diritti e le libertà delle persone fisiche, il titolare del trattamento dei dati mette in essere misure tecniche e organizzative (privacy by design e privacy be default) adatte a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: 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.*
Inoltre, il titolare e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a "dati personali" non tratti tali dati se non preventivamente autorizzato ed istruito in tal senso.

RESPONSABILI ESTERNI E DPO
(artt. 28 e 37 - Regolamento "UE" 2016/679)

Qualora un trattamento debba essere effettuato per conto del titolare, quest'ultimo ricorre unicamente a "responsabili esterni" che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, che garantiscano le tutele dei diritti dell'interessato.
Per quanto riguarda invece la nomina della figura del "Data Protection Officer" in sigla D.P.O. (Responsabile della Protezione dei Dati) all'interno dell'organizzazione, il titolare ed il responsabile la designano ogniqualvolta: 1. *il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; 2. le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; 3. le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.*
La norma non prevede requisiti particolari per rivestire il ruolo di DPO, salvo qualità professionali, conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e capacità di assolvere i compiti di cui all'art. 39 del medesimo Regolamento Europeo.

NOTIFICA DI VIOLAZIONE (DATA BREACH)
(artt. 33 e 34 - Regolamento "UE" 2016/679)

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Qualora la violazione dei dati personali presenti anche un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica, con un linguaggio semplice e chiaro, la violazione all'interessato senza ingiustificato ritardo.