COSTANTINO & partners
DIRITTO DEL LAVORO, SINDACALE E DELLA PREVIDENZA SOCIALE

Le principali novità del Regolamento Europeo per la Protezione dei dati Personali

Dal prossimo 25 maggio il vigente Codice della Privacy verrà integralmente sostituito dal Regolamento Europeo per la Protezione dei Dati Personali n. 2016/679, essendo quest'ultimo un provvedimento normativo immediatamente applicabile nell'ordinamento degli stati membri.
Il Regolamento introduce rilevanti novità in merito ai diritti derivanti dal trattamento dei dati personali ed introduce nuove figure a garanzia dell'effettiva tutela della privacy, che incidono (anche) sulla formulazione dell'informativa per l'acquisizione del consenso da parte degli interessati.
Senza dubbio la più rilevante è rappresentata dall'istituzione della figura del "Responsabile per la protezione dei dati personali" (denominato anche DPO, acronimo di Data Protection Officer), la cui finalità è quella di assolvere – a fianco del Titolare e del Responsabile del trattamento dei dati – alle funzioni di supporto e controllo, nonché a quelle consultive, formative e informative.
Al riguardo, il Garante della Privacy, in risposta alle Faq del 26 marzo 2018, ha fugato ogni dubbio sulla nomina del DPO da parte delle strutture sanitarie private, avendo espressamente specificato che sono obbligate in tal senso anche le "società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione".
Tale figura deve possedere un'approfondita conoscenza della normativa e della prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano tale specifico settore, affinché sia in grado di offrire la consulenza necessaria per progettare, verificare e mantenere un corretto sistema organizzato di gestione dei dati personali.
Inoltre, il DPO deve essere in grado di agire in piena indipendenza ed autonomia, senza ricevere istruzioni da alcuno e con il potere di riferire direttamente ai vertici aziendali.
Atteso che (allo stato) non esistono attestazioni formali sul possesso delle suddette conoscenze né iscrizioni ad appositi albi professionali, in ambito privato l'incarico di DPO può essere conferito (anche) ad un dipendente del Titolare o del Responsabile dei dati, in assenza di conflitto di interessi.
In proposito, il Garante della Privacy, sempre in risposta alle citate Faq del 26 marzo 2018, ha specificato che risulta preferibile evitare di assegnare il ruolo di responsabile della protezione dei dati personali a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di organismi aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (come la direzione risorse umane, la direzione marketing, la direzione finanziaria, ecc.), suggerendo di valutare la possibilità, in assenza di conflitti di interesse e in base al contesto di riferimento, di riservare tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale), ammettendo, inoltre, la possibilità di attribuire tali funzioni anche ad un soggetto esterno che, peraltro, potrà essere anche una persona giuridica.

Il Regolamento consente, inoltre, che le imprese appartenenti al medesimo gruppo (costituito da un'impresa controllante e da imprese da questa controllate), possano designare un unico responsabile della protezione dei dati personali, purché lo stesso possa facilmente raggiungere ciascuno stabilimento, nonché sia in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.
Secondo quanto raccomandato dal Gruppo di Lavoro "Articolo 29" (organismo consultivo ed indipendente istituito in materia di privacy) è opportuno che il nominativo e i dati di contatto del DPO siano comunicati ai dipendenti mediante la pubblicazione sul sito internet del datore di lavoro, sull'intranet aziendale e, in ogni caso, in seno all'informativa sul trattamento dei dati personali.
Altre rilevanti novità del Regolamento europeo, riguardano il riconoscimento di nuovi diritti, non compresi nell'attuale Codice della Privacy, che dovranno essere necessariamente elencati, ai sensi di quanto disposto dall'art. 13 del Regolamento, in seno alla nuova informativa da fornire al destinatario del trattamento dei dati.
La normativa europea prevede, in particolare, il diritto dell'interessato ad essere informato circa il periodo di trattamento e conservazione dei suoi, che dovrà risultare specifico e determinato, o predeterminabile secondo altri criteri.
In proposito, è ragionevole sostenere che, nell'ambito del rapporto di lavoro, il suddetto arco temporale possa coincidere con la durata del rapporto lavorativo nonché con il successivo termine quinquennale, previsto dal D.M. del 9 luglio 2008 per la tenuta della documentazione del lavoratore.
Gli ulteriori nuovi diritti espressamente riconosciuti dalla suddetta normativa europea sono rappresentati dalla possibilità di chiedere al titolare del trattamento di accedere ai propri dati personali, nonché di pretendere la rettifica o la cancellazione degli stessi, di limitarne o opporsi al trattamento e di godere della portabilità degli stessi.
In ordine a quest'ultima facoltà, l'art. 20 del Regolamento, riconosce il diritto dell'interessato di ricevere "in un formato strutturato, di uso comune e leggibile da dispositivo", i dati personali forniti ad un titolare e di trasmetterli ad un altro titolare "senza impedimenti", ove ciò sia tecnicamente possibile.
Conseguentemente, l'interessato potrà effettivamente godere di tale diritto unicamente se "il trattamento sia effettuato con mezzi automatizzati" (ossia qualora i dati siano memorizzati su supporti informatici), non potendosi ovviamente realizzare nel caso in cui le informazioni vengano conservati in archivi o registri cartacei.
L'informativa deve altresì contenere l'indicazione dell'eventuale adozione di un processo automatizzato di dati personali, compresa la c.d. profilazione, termine con il quale si intende l'utilizzo di tali dati 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.
Sul punto, con riferimento alla possibilità di controllare il rendimento professionale tramite gli strumenti "utilizzati dal lavoratore per rendere la prestazione lavorativa" (come, ad esempio, computer e telefonino aziendale), anche sotto la vigenza della nuova normativa europea, si

rammenta (come peraltro evincibile dalla recente newsletter n. 439 del 29 marzo 2018 del Garante della Privacy) che sarà necessario mettere a conoscenza quest'ultimi tale eventualità, tramite l'adozione e la pubblicazione di una policy aziendale sul corretto uso di internet e degli strumenti informatici.

Infine si segnala un'altra rilevante novità imposta dal Regolamento europeo, rappresentata dall'obbligo per le imprese con più di 250 dipendenti di tenere un registro delle attività di trattamento dei dati.

Tale registro, ai sensi dell'art. 30 del citato Regolamento, deve contenere: il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; le finalità del trattamento; una descrizione delle categorie di interessati e delle categorie di dati personali; le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale; ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati, nonché una descrizione generale delle misure di sicurezza tecniche e organizzative per la cancellazione degli stessi.

In merito alle misure di sicurezza, l'art. 31 del Regolamento prevede espressamente che il Titolare del trattamento "deve garantire un livello di sicurezza adeguato al rischio", lasciando a quest'ultimo un ampio margine di discrezionalità nell'adozione degli strumenti utili per la suddetta finalità protettiva, sebbene all'art. 32 vi sia un'elencazione dei suggerimenti sulle possibili misure che potrebbero essere adottate per tale scopo.

In conclusione si rammenta che la disciplina europea sulla privacy, sebbene immediatamente applicabile, potrebbe essere ulteriormente integrata dalla disciplina nazionale, mediante il riconoscimento di ulteriori diritti (o il potenziamento di quelli esistenti) volti a garantire l'effettiva tutela della riservatezza dei dati personali e sensibili.