

Tutela della riservatezza. Le ricadute dell'entrata in vigore del Regolamento 2016/679

La privacy 2.0 ridisegna l'organizzazione aziendale

Regole e sistemi interni da adeguare entro maggio 2018

PAGINA A CURA DI

Aldo Bottini
Paola Pucci

Il debutto, nel 2018, della nuova normativa europea sulla protezione dei dati personali impone alle aziende di cominciare ad adeguare policy e organizzazione interna, fin da ora, per arrivare preparate alla data del 25 maggio, quando sarà efficace in tutta l'Unione il Regolamento generale per la protezione dei dati (Gdpr, regolamento Ue 2016/679).

Da quella data, infatti, la normativa europea sostituirà integralmente quella interna attualmente in vigore; il Gdpr sostituirà il nostro Codice privacy (in vigore dal 2003) e la disciplina in materia di trattamento dei dati tra i vari Paesi membri sarà uniforme.

È facile intuire perché l'Unione abbia dedicato tempo e attenzione al tema della protezione dei dati: la tecnologia connota in modo profondo il mondo economico e imprenditoriale (i social media, la gig-economy) generando fatturati e valore che si appoggiano sulla gestione dei dati, più che sulla produzione o sui servizi. Non a caso si sente dire che questa è la quarta rivoluzione industriale, e i dati «il petrolio del nuovo millennio».

Rivendicando un ruolo centrale in questo contesto, l'Unione rivisita e innova una normativa e un concetto (la «privacy») entrato da tempo negli ordinamenti e nel lessico degli Stati ma in molti casi confinato in formule ripetitive, tutele evanescenti e, insomma, percepito più come requisito formale che

come diritto sostanziale (degli utenti) e rispettivo obbligo (dei titolari, degli incaricati e di chiunque si trovi a trattare un dato altrui).

La strada scelta dal legislatore europeo per raggiungere questo scopo è stata, in primo luogo, l'inasprimento del sistema sanzionatorio, con multe

IPERCORSI

Servirà una formazione specifica e documentabile dei dipendenti come già previsto per la sicurezza sul lavoro



Data protection regulation

● La *General data protection regulation* (in sigla Gdpr), il regolamento europeo 2016/679, adottato il 27 aprile 2016, diventerà efficace in tutta l'Unione europea, dopo due anni di transizione, il 25 maggio 2018 e sostituirà l'attuale normativa interna dei singoli Stati sulla protezione dei dati personali. Uscirà quindi di scena il Codice della privacy oggi applicato in Italia, contenuto nel Dlgs 196/2003. Il Regolamento europeo non necessita di norme nazionali di recepimento.

che possono arrivare nel massimo all'importo maggiore tra il 4% del fatturato mondiale di gruppo e 20 milioni di euro.

In secondo luogo, si è deciso di introdurre nuovi concetti e principi sconosciuti alla precedente legislazione, elaborando e specificando i concetti già presenti. Nascono nuove obbligazioni (la tenuta - obbligatoria per le aziende che impiegano più di 250 dipendenti, ma consigliata in ogni caso dal nostro Garante - del registro per le attività di trattamento), nuove procedure (come la notifica dei cosiddetti *data breach* o violazioni dei dati) e nuove figure (il Responsabile per la protezione dei dati) entrano nel nostro sistema, senza passare, considerata la natura del provvedimento, per un recepimento del legislatore nazionale. Il Gdpr sarà, da maggio 2018, la normativa europea per la tutela dei dati personali.

Nasce anche un nuovo vocabolario della privacy, con concetti e termini inediti (e anglofoni): la *privacy by design* e *by default*, ad esempio, che prevedono che ogni sistema di trattamento dei dati (con particolare riferimento ai sistemi elettronici) sia progettato sin dall'origine per il rispetto della normativa (non solo, quindi, usato in quel modo) e preveda specifiche tecniche che, per quanto possibile, impediscano in radice ogni violazione con impostazioni predefinite.

Il sistema, diversamente da quello precedente, è retto idealmente dal concetto di *accountability*, ossia, grosso mo-

do, responsabilizzazione: una sorta di clausola di chiusura per il sistema.

Non esiste più un catalogo di misure minime da adottare per la tutela dei dati, misure che, quindi, garantiscono il titolare da sanzioni e imprevisti. I titolari dovranno mettere in atto le misure tecniche e organizzative che di volta in volta siano adeguate, anche alla luce delle innovazioni tecnologiche, a garantire la tutela dei diritti degli interessati. Ogni titolare, dunque, sarà responsabile dei propri sistemi e della loro tenuta (a priori e a posteriori) di fronte a possibili violazioni o incidenti.

Una doppia rivoluzione copernicana: la privacy al centro dei processi aziendali; i diritti dell'utente al centro della disciplina della privacy.

Resta da chiedersi quali siano i processi aziendali che coinvolgono dati personali e chi siano gli utenti al centro delle nuove tutele. La risposta è semplice. Tutti i processi aziendali coinvolgono dati personali; gli utenti del sistema sono tutti i soggetti che, a ogni livello, hanno a che fare con le società: clienti, fornitori, visitatori del sito internet e, ovviamente, dipendenti.

Come già in materia di sicurezza sul lavoro, va prevista una formazione specifica ed efficace, che andrà anche debitamente documentata e inserita nei documenti e nei processi sulla privacy interni. La formazione andrà poi ripetuta e, soprattutto, aggiornata secondo i cambiamenti dell'attività e del tipo di dati trattati.

© RIPRODUZIONE RISERVATA