Violazioni. Le contromisure per chi non si allinea

Sanzione massima fino a 20 milioni o al 4% del fatturato

Uno dei cardini del nuovo Regolamento generale per la Protezione dei dati europeo è il sistema sanzionatorio; o meglio, l'entità delle sanzioni che costituiscono, di per sé, motivo di potenziale preoccupazione per qualunque imprenditore. Vale la pena di ripetere gli importi massimi delle multe per violazione delle norme a tutela della privacy: 20 milioni di euro o il 4% del fatturato mondiale di gruppo.

Ma non è solo l'importo a rilevare, analizzando il Gdpr e il suo possibile impatto sull'attività delle aziende italiane ed europee in generale. Va notato, come punto di partenza, che il Regolamento è generale: il suo campo di applicazione comprende ogni trattamento dei dati che ha a che fare con l'Unione europea, una sorta di extra-territorialità sui generis. Chiarito questo, a partire dal mese di maggio 2018 il punto di entrata per un ricorso, una segnalazione o un procedimento nei confronti di un titolare di dati potrà essere, indifferentemente di fronte a violazioni, rischi e contestazioni. Ogni soggetto dovrà dotarsi di un sistema (e di una organizzazione) capace di rispondere in tempo reale a ogni tipo di crisi: dalla più banale (la richiesta di accesso ai propri dati da parte di un soggetto) alla più rilevante (un allarme per furto o sparizione di dati sensibili). Le fattispecie (e le conseguenti responsabilità) non mancano: ogni violazione o perdita di dati (*data breach*) va notificata al Garante entro 72 ore dall'accaduto. I titolari devono essere in grado di restituire a chi lo richiede immediatamente e in forma accessibile tutti i dati detenuti (diritto all'oblio e alla cancellazione); il solo modo di gestire profili di responsabilità efficacemente sarà dimostrare la bontà e la tenuta dei propri sistemi. La privacy sarà (come la sicurezza sul lavoro o i modelli 231) una materia per la quale non si potrà piangere sul latte versato.

LE RESPONSABILITÀ
Ogni perdita di dati va comunicata al Garante entro 72 ore e l'accesso agli interessati va sempre consentito

Del resto, le sanzioni non si limitano a multe o a raccomandazioni: nel nuovo sistema Gdpr le Autorità garanti hanno potere di raccomandazione, verifica e addirittura divieto per i trattamenti illeciti o non in linea con le prescrizioni. Per alcune attività, si tratta di un potere che può paralizzare la produzione e i profitti per periodi anche rilevanti.

Il legislatore europeo è serissimo, quando si parla di pri-

mente, ogni autorità garante sul territorio dell'Unione, il che comporta (per i soggetti che operano, in qualunque modo, su scala transnazionale) una effettiva necessità di prassi e regole uniformi e agili.

Il terzo punto, assai rilevante, è il tempo. Le regole del Gdpr, da quelle generali e di principio a quelle specifiche e prescrittive, impongono ai titolari processi e procedure che consentano reazioni e azioni immediate

vacy, trattamento dei dati e diritti connessi. A ottobre del 2015, poco più di sei mesi prima che il Gdpr fosse pubblicato, la Corte di Giustizia Ue ha dichiarato invalido l'accordo cosiddetto di *safe harbour* (porto sicuro) tra Europa e Usa, rendendo invalido ogni scambio di dati basato sull'accordo; un segno, a posteriori, dell'estrema serietà con cui la privacy è vissuta dalle istituzioni dell'Unione.