PRIVACY SHIELD NON IN LINEA CON IL GDPR QUALI EFFETTI PER LE IMPRESE?

La sentenza della Corte di Giustizia dell'Unione Europea che dichiara non adeguata la protezione offerta dal regime di scudo UE-USA per il trattamento dei dati all'estero, porta a riflettere sulla necessità di una revisione del sistema aziendale di compliance al GDPR

di **Paola Gobbi**

Sono passati più di due anni dalla corsa finale delle aziende all'adeguamento del proprio sistema privacy alle regole innovative del GDPR di privacy by design e by default e di accountability. A fronte dei recenti interventi a livello comunitario e dei rapidi, quanto inaspettati, mutamenti del contesto operativo e organizzativo aziendale occorre chiedersi se è opportuno prevedere dei correttivi o degli adeguamenti. La risposta non può che essere positiva: sì, in applicazione delle previsioni del GDPR di continua manutenzione dell'impianto privacy, che non è un sistema statico bensì dinamico, bisogna prendere atto dell'intervenuto mutamento e rimodulare il progetto iniziale.

Un primo forte segnale di questa esigenza di revisione deriva dalla sentenza della Corte di Giustizia dell'Unione Europea (causa C-311/18 adottata il 23 luglio 2020) che - dichiarando non adeguato lo scudo UE-USA per il trasferimento all'estero dei dati - impone di riflettere se nelle informative inviate ai dipendenti, clienti, fornitori vi è una corretta previsione sul punto, preso atto che l'ipotesi di trasferimento e trattamento dei dati all'estero non è particolarmente remota: basti pensare ai sistemi back-up e conservazione dati in cloud oppure agli accentramenti dei trattamenti in paesi extra UE in caso di soggetti internazionali e multinazionali. Analoghe spinte arrivano anche da un contesto più domestico e dalla normativa nazionale per la gestione dell'emergenza Covid-19. Il continuo e prorogato ricorso allo smart working, di pari passo con un accresciuto utilizzo della tecnologia da remoto e della necessità per le aziende - e non solo - di tutelarsi da accessi non autorizzati e/o utilizzi abusivi portano alla conseguente necessità di una implementazione delle misure di difesa dei sistemi informativi aziendali, di una rimodulazione delle potenzialità di controllo rispetto a un corretto e diligente utilizzo dello strumento, e alla adozione di tutte le misure di sicurezza per un trattamento sia legittimo che sicuro rispetto a possibili data breach. Tale esigenza trova conferma anche nel recente messaggio del Garante che ha fornito indicazioni su come difendersi in tempo di Covid-19 dall'altrettanto aggressivo virus, anche se virtuale, ransomware o su come proteggersi dai tentativi di phishing. Un "accountable" datore di lavoro e titolare del trattamento dei dati, allora, dovrà riesaminare il proprio progetto/sistema di privacy e predisporre tutte quelle misure volte a difendere e proteggere i propri dati anche qualora vi siano nuove modalità di trattamento quali appunto lo smart working. Il lavoratore dovrà però essere informato di tali misure e implementazioni, del loro funzionamento, delle finalità del trattamento dei dati così raccolti e della modalità di trattamento.

Si torna, pertanto, al punto di partenza: l'informativa dovrà essere revisionata e aggiornata, al passo con il mutevole contesto mondiale. Senza una corretta e completa informativa, infatti, nessun trattamento potrà essere legittimo.

Avv. **Paola Gobbi** partner
UNIOLEX Stucchi & Partners - www.uniolex.com