AIFI
Associazione Italiana del Private Equity, Venture Capital e Private Debt

fieldfisher

Commissione Tax&Legal, Approfondimenti, marzo 2018

A cura di Francesca Gravili e Imma Ciarletta (Fieldfisher)

Il nuovo Regolamento europeo in materia di protezione dei dati personali: le principali novità per i gestori di private equity

La Commissione UE ha proposto una riforma della disciplina europea relativa alla protezione dei dati con l'introduzione del General Data Protection Regulation – GDPR (Regulation EU 2016/679), di seguito il «Regolamento o GDPR».

Si ricorda che la legislazione europea in materia di protezione dei dati personali è entrata in vigore nel 1995, attraverso l'attuazione della relativa Direttiva, in modo differente negli Stati membri, comportando incongruenze, complessità, incertezze giuridiche e costi amministrativi.

Il nuovo Regolamento ha l'obiettivo di fornire chiarezza e coerenza alle regole da applicare, ripristinando la fiducia dei consumatori e permettendo alle imprese di cogliere appieno le opportunità del Mercato unico digitale.

Il Regolamento è direttamente applicabile e vincolante in tutti gli stati membri dell'Unione Europea ed è obbligatorio per tutte le aziende che trattano dati personali, anche solo dei propri dipendenti (es. aziende che non svolgono attività di marketing e/o che non trattano dati dei consumatori finali).

Domanda: cosa cambierà con il Regolamento?

Risposta: il Regolamento mira a rafforzare i diritti dei singoli e a garantire un'applicazione più rigorosa delle regole. Queste sono elaborate per far sì che le informazioni personali siano protette - a prescindere da dove vengano inviate, elaborate e conservate - anche al di fuori dell'UE, come spesso accade su Internet.

Domanda: quando entreranno in vigore le disposizioni del Regolamento?

Risposta: le disposizioni diverranno direttamente applicabili in tutti gli stati membri dell'UE a partire da maggio 2018.

Domanda: quali sono i principali doveri e le conseguenze per le imprese?

Risposta: il GDPR promuove la responsabilizzazione (accountability) dei Titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Di seguito si riportano le linee guida del Regolamento:

Responsabilità: alle Società sarà richiesto di adottare adeguate misure tecniche e organizzative - da rivedere e aggiornare ove necessario - per garantire ed essere in grado di dimostrare che il trattamento viene effettuato conformemente al Regolamento.

Estensione dell'ambito di applicazione: le imprese extracomunitarie saranno soggette al Regolamento se i) offrono beni e servizi a cittadini UE; ii) monitorano il comportamento di cittadini UE ("targeting").

Protezione dei dati by design e by default: ai Titolari del trattamento sarà richiesto di attuare la protezione dei dati by design e by default fin dalla progettazione delle attività di business (ad esempio, quando si creano nuovi prodotti, servizi o altre attività di elaborazione dei dati).

Data Protection Officer (DPO): le realtà, pubbliche o che tratteranno dati più "a rischio", dovranno nominare un Responsabile della protezione dei dati (Data Protection Officer), comunicandolo all'Autorità Nazionale di Controllo. Il Data Protection Officer potrà essere interno e/o esterno all'organizzazione del Titolare del trattamento ma dovrà essere dotato di particolari poteri sì da assicurare la conformità delle aziende al GDPR.

Nuovi obblighi per il responsabile del trattamento: il Regolamento introduce obblighi di *compliance* diretti per il responsabile del trattamento (questi obblighi includono: responsabilizzazione, notificazione della violazione dei dati, sicurezza dei dati). Ciò avrà un impatto sia sui Titolari che sui responsabili, dovendo negoziare tale aspetto nei futuri accordi e rivedere anche i contratti già esistenti.

Cittadini più garantiti: il GDPR introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, introducendo il diritto alla «portabilità» dei propri dati personali per trasferirli da un Titolare del trattamento ad un altro. Inoltre, grazie all'introduzione del cosiddetto «diritto all'oblio», gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del Titolare del trattamento qualora ricorrano alcune condizioni previste dal Regolamento.

Data Breach: il Titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (*data breach*) all'Autorità Nazionale di Controllo. Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il Titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

Sanzioni: in caso di inosservanza delle regole sono previste sanzioni, anche elevate. Sono soggette a sanzioni amministrative fino a 10 milioni di euro, o in caso di un'impresa, fino al 2% del fatturato totale annuo mondiale dell'esercizio precedente, se superiore, le violazioni degli obblighi generali previsti dal Regolamento. Sono applicabili sanzioni amministrative fino a 20 milioni di euro, o in caso di un'impresa, fino al 4% del fatturato totale annuo mondiale dell'esercizio precedente, se superiore, per le violazioni in materia di principi base del trattamento, condizioni per il consenso, diritti degli interessati, trasferimento di dati personali all'estero, mancata ottemperanza a un ordine o a una limitazione temporanea o definitiva del trattamento disposti dall'autorità di vigilanza.