Regolamento europeo privacy: gli adempimenti per le aziende

Valentina Frediani - Avvocato - Founder e CEO Colin & Partners

Per le aziende si avvicina il momento in cui dovranno applicare il nuovo Regolamento europeo in materia di protezione dei dati personali, in vigore dal 24 maggio 2016. Titolari e responsabili della privacy dovranno, infatti, predisporre un idoneo sistema di gestione delle attività nel rispetto dei nuovi principi introdotti. Mappatura degli strumenti ICT, contrattualistica ad elevato standard di sicurezza e Privacy Impact Assessment per alcune tipologie di trattamento dati: queste alcune delle direttrici di azione per le imprese.

Il 2016 ha dato concretezza ai tentativi europei di uniformare la normativa in materia di protezione dei dati personali, con l'intento di assicurare la centralità degli interessati europei i cui dati sono trattati. Dopo un lento percorso normativo, iniziato nel 2012, le istituzioni comunitarie hanno raggiunto un accordo finalizzando il testo definitivo del Regolamento Europeo (GDPR), entrato in vigore il 24 maggio 2016.

Consulta il dossier Nuovo regolamento privacy

Il nuovo assetto ha confermato in massima parte gli obblighi già introdotti a carico dei titolari e dei responsabili del trattamento dalla Direttiva 95/46/CE, ma si è fatto portatore di interessanti novità. Per adeguarsi ad esse gli stakeholders avranno tempo fino al 25 maggio 2018, data di sostanziale applicazione della neonata normativa. E non potranno che conformarsi alle disposizioni richieste, tenuto conto della rinnovata competenza sanzionatoria attribuita, dal Regolamento, alle Autorità Garanti. Queste ultime potranno sanzionare fino al 4% del fatturato mondiale annuo dell'azienda o della capogruppo, qualora si tratti di una compagine più strutturata.

Il cambio di prospettiva richiesto porterà necessariamente le aziende, destinatarie dei nuovi obblighi, a stabilire un sistema di gestione del quale la tutela del dato personale diventerà il perno attorno al quale costruire ed implementare processi e procedure aziendali.

Quali sono i macro temi sui quali le aziende dovranno intervenire?

La mappatura degli strumenti ICT

Le aziende coinvolte dovranno affrontare l'analisi degli strumenti aziendali che comportano trattamento di dati personali ed evidenziare eventuali non conformità ai principi introdotti. Tali strumenti, come sistemi biometrici, di videosorveglianza, CRM, ecc., dovranno essere capaci di gestire livelli differenziati di data retention, piuttosto che anonimizzazione e pseudonimizzazione dei dati personali. Tale analisi coinvolgerà principalmente l'area ICT, quale parte tecnicamente competente per assistere le aziende in tale percorso.

Non dimentichiamo come il Regolamento abbia ufficializzato il rispetto dei principi di privacy by design e by default che impongono ai titolari del trattamento di porre in atto misure tecniche organizzative adeguate al fine di garantire - ed essere in grado di dimostrare sin dall'origine - che ogni trattamento dati sia conforme al quadro normativo.

La contrattualistica

Le aziende non potranno prescindere dal predisporre efficienti contratti a disciplina delle

attività di trattamento dei dati. Sarà assolutamente indefettibile predisporre modelli contrattuali che impongano elevati standard di sicurezza a presidio dei dati personali trattati da terze parti - a seguito di esternalizzazione di servizi - nonché le responsabilità ripartite con i providers coinvolti. Basti pensare ad attività di manutenzione ed assistenza informatica in outsourcing, contratti di hosting o prestazione di servizi in modalità SaaS (Software as a Service). Il trattamento dei dati di cui sono titolati le aziende, da parte dei fornitori e subfornitori, implica necessariamente il disciplinarne gli aspetti tecnici e legali in ordine a data breach, misure di sicurezza, rapporti di contitolarità.

Trasferimenti dei dati all'estero

Il Regolamento europeo ha confermato il divieto di trasferimento di dati personali verso Paesi non appartenenti all'UE, se non in presenza di idonee garanzie. Oltre alle decisioni della

Commissione europea, chiamata a valutare quando un Paese non UE garantisce un livello di protezione opportuno, i trasferimenti verso paesi terzi sono subordinati all'adozione di particolari strumenti: clausole contrattuali standard e norme vincolanti di impresa, qualora si tratti di una multinazionale. Infine, lo scorso 12 luglio 2016, la Commissione Europea ha confermato l'adeguatezza del cosiddetto Privacy Shield che legittima i trasferimenti di dati personali diretti verso azienda situate in USA. Lo scudo UE-Usa per la privacy si fonda su un sistema di autocertificazione in base al quale l'organizzazione statunitense si impegna a rispettare un insieme di principi in materia di privacy.

Privacy Impact Assessment per alcune tipologie di trattamento dati

In alcuni casi sarà obbligatorio per le aziende redigere anche un Privacy Impact Assessment. Il PIA rappresenta una valutazione concreta da effettuarsi per determinate tipologie di trattamento dati (ad esempio: profilazione o videosorveglianza) volta a definire rischi e misure tecniche di sicurezza adottate in relazione a detti trattamenti. Tale documento dovrà anche individuare i soggetti coinvolti nella definizione del trattamento e le funzioni aziendali da rendere partecipi, qualora ne venga modificato l'assetto (comparto IT, Marketing, HR). Tale valutazione dovrà essere preventiva rispetto all'inizio del trattamento e rappresenta - di fatto - la messa in pratica dei principi di privacy by design e by default suindicati.

Data Protection Officer

Altro inserimento nella GDPR riguarda la figura del Data Protection Officer, che non risulta una completa novità nel panorama giuridico europeo, essendo stata in realtà prevista fin dalla Direttiva 95/46/CE.

Tra i requisiti del DPO il Regolamento ha introdotto quello dell'indipendenza rispetto alle posizioni apicali, tale che egli risponda direttamente al Titolare (ossia al legale rappresentante dell'azienda). Tra i compiti a questi demandati, vi sono attività atte ad informare e consigliare il titolare, o il responsabile, in merito agli obblighi derivanti dal Regolamento, per quanto attiene alle misure e procedure tecniche e organizzative, funzioni di vigilanza sull'attuazione e sull'applicazione delle politiche inerenti alla protezione dei dati personali, compiti di controllo a che le violazioni dei dati personali siano documentate, notificate e comunicate, ed infine funzioni di cooperazione con l'Autorità di controllo.