GDPR: compliance, responsabilità e sanzioni

Da **Stefano Castelnuovo** - 18/01/2018

Tutto quello che c'è da sapere sulla regolamentazione che entrerà in vigore il 25 maggio. La tua azienda è pronta?

La Farnesina, Università Bicocca, UniCredit, Saint Gobain, Sogei, Deloitte, Yahoo e Uber. Cosa accomuna tutte queste aziende? Hanno tutte subìto una violazione e la perdita dei dati a causa di un attacco informatico. A queste realtà purtroppo però se ne aggiungono altre centinaia di migliaia, appartenenti ad ogni settore, nazione, sia pubbliche che private e di qualunque dimensione (basti pensare che nel 2017 il 47% delle PMI sono state attaccate). La sicurezza informatica sta pertanto velocemente diventando una vera problematica di business per le aziende che, oltre a subire ingenti danni economici e la perdita di reputazione, vedono inoltre compromessi tutti i dati da loro posseduti, sia interni che di clienti, ma anche di terze parti, con gravi conseguenze per il proseguo dell'attività.

Al fine di garantire una maggior sicurezza delle informazioni, l'Unione Europea ha introdotto nel 2016 il GDPR, normativa alla quale le imprese devono adeguarsi entro 2 anni, con scadenza ultima il 25 maggio 2018, senza proroga alcuna.

"*Il trattamento dei dati è lecito, il loro utilizzo deve però essere protetto, autorizzato e con il consenso espresso dell'interessato*" ha dichiarato l'avvocato Giovanna Ianni, in occasione dell'evento "GDPR: un dato di fatto, un fatto di dati", organizzato ieri a Milano da BBTech e Risk Solver, nato con l'obiettivo di approfondire le tematiche legate alla nuova regolamentazione.

GDPR

Il General Data Protection Regulation si basa essenzialmente su 3 pilastri:

1) Principio di Accountability o di responsabilizzazione: i dati devono essere trattati sotto la responsabilità del Titolare, che deve dimostrare per ciascuna operazione di aver agito in conformità alle disposizioni del GDPR. Al contrario di come avveniva in passato infatti, si passa ad un approccio proattivo e non più reattivo, con focus su obblighi e comportamenti che prevengano in modo effettivo il possibile evento di danno.

2) Privacy by Design: si intende la necessità di prevedere già in fase di progettazione dei sistemi informatici e applicativi, di sistemi che tengano costantemente sotto controllo i rischi che il trattamento può comportare per la tutela degli interessati

3) Privacy by Default: tutte le volte in cui un soggetto cede i propri dati ad un terzo, deve sempre esistere una procedura interna che preveda e disciplini le modalità di acquisizione, trattamento, protezione e modalità di diffusione.

GDPR vs Regolamento Italiano

Il GDPR prevede che ogni Nazione emetta una legge di coordinamento (entro il 21 maggio 2018) tra il Regolamento Europeo e le normative nazionali vigenti, soprattutto in riferimento alle materie sulle quali gli Stati Membri hanno competenza legislativa esclusiva (es. penale), con anche l'obiettivo di evitare che vi siano contrasti tra le due legislazioni. La suddetta legge di coordinamento non è però ancora stata emessa, ma solo dei provvedimenti intermedi. Il rischio è quindi che ci siano in essere leggi contrastanti in vigore.

Quali aziende devono essere compliance al GDPR?

Si devono adeguare alla normativa tutte le imprese, le organizzazioni e le Pubbliche Amministrazioni presenti negli stati membri dell'Unione Europea (indipendentemente dal fatto che il trattamento sia effettuato in UE), ma anche società extra UE che offrono servizi o prodotti a persone fisiche nel territorio dell'UE o che semplicemente monitorano il comportamento di soggetti all'interno dell'Unione.

Quali dati sono soggetti al GDPR?

L'introduzione della normativa non fa più riferimento a quelli che si chiamavano fino a poco tempo fa "dati sensibili", ma a qualunque informazione riguardante una persona fisica

identificata o identificabile, direttamente o indirettamente (non solo nome e cognome, ma anche indirizzi IP, cookies, dati di geolocalizzazione, dati bancari, ecc.) e trattabili con mezzi automatizzati e non**.**

Esistono pero delle esclusioni per le quali il trattamento è libero: informazioni anonime, quelle utilizzate per scopi personali o domestiche, quelle rientranti nella politica estera, nella sicurezza comune, nella sicurezza pubblica e giustizia, oltre che quelle aventi finalità esterne al diritto UE.

Chi può trattare i dati personali?

Il Titolare del trattamento, ossia qualsiasi persona fisica o giuridica, Autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali. Il titolare può a sua volta nominare un Responsabile del trattamento che tratta le informazioni per conto del Titolare e anche un Autorizzato al trattamento, cioè chiunque agisca sotto l'autorità del Titolare o del Responsabile del trattamento, che sia da lui istruito e abbia accesso ai dati personali oggetto del trattamento.

Trasferimento dei dati all'estero. È possibile?

Il GDPR vieta il trasferimento verso Paesi situati al di fuori dell'UE o organizzazioni internazionali se effettuato in assenza di adeguati standard di tutela. Al contrario, invece, è permesso in caso di presenza di adeguate garanzie come clausole contrattuali tra titolari autorizzate dal Garante, accordi e provvedimenti vincolanti tra autorità pubbliche amministrative e giudiziarie, clausole tipo adottate dal Garante, adesione a codici di condotta e/o meccanismi di certificazione.
E' inoltre permesso il trasferimento oltre UE in caso di decisioni di adeguatezza della Commissione UE (es. «*Privacy Shield EU/USA*», Svizzera, Argentina, Australia, Canada, ecc.), norme vincolanti di impresa (*Binding Corporate Rules* – «*BCR*») e casi in deroga (consenso informato dell'Interessato, necessità per esecuzione adempimenti contrattuali e precontrattuali, interesse pubblico, diritto di difesa, interessi vitali, dati tratti da registro pubblico, ecc.)

DATA BREACH

Una delle tematiche affrontate dal GDPR riguarda il Data Breach, definito come qualsiasi attività che comporti la distruzione, perdita, modifica, divulgazione non autorizzata o

l'accesso ai dati personali trasmessi, conservati o comunque trattati. Le aziende, entro 72 ore dalla venuta a conoscenza della violazione subita (eventuali ritardi devono essere giustificati) devono comunicare all'Authority la natura della violazione, le possibili conseguenze, le misure adottate per rimediare o ridurre l'impatto del danno subito, ma anche fornire il nome e i dati di contatto del DPO.

Qualora sussistesse un rischio elevato per i diritti e le libertà della persona fisica i cui dati sono compromessi, la comunicazione dovrà avvenire anche agli interessati con le stesse modalità fornite all'Autorità. Esistono però alcuni casi per i quali la notifica all'interessato non è necessaria, ossia quando i dati non sono stati compromessi a seguito della violazione, se sono state adottate misure successive atte a scongiurare il sopraggiungere un rischio elevato dei diritti dell'interessato o qualora l'invio della comunicazione richieda sforzi sproporzionati.

Responsabilità

Sono passibili della responsabilità e quindi tenuti al risarcimento soltanto **il titolare del trattamento ed il responsabile** incaricato: mentre il titolare deve risarcire qualsiasi danno abbia cagionato in virtù della violazione del Regolamento nel trattamento dei dati, il responsabile risponde solo se non ha adempiuto agli obblighi a lui specificatamente diretti o ha agito in modo difforme o contrario alle istruzioni del titolare.

SANZIONI

Il GDPR prevede sanzioni pecuniarie e penali a seconda della gravità della violazione e delle strategie messe in atto dall'azienda per minimizzare il rischio di perdita dei dati.

Sanzioni Pecuniarie

Sono stabilite multe fino a 10 milioni di euro o fino al 2% del fatturato mondiale annuo dell'azienda dell'esercizio precedente, se superiore alla predetta cifra, qualora non vegano adottati accorgimenti strutturali e formali, come ad esempio non essere conformi al privacy by design/ by default, non aver assegnato ruoli specifici nel trattamento dei dati così come del DPO, non aver realizzato i registri delle attività di trattamento o il non aver comunicato la violazione del Data Breach all'Autority e all'interessato.

Le sanzioni salgono a 20 milioni di euro, o per le imprese, fino al **4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore alla predetta cifra, qualora si attestino violazioni ai principi e alle norme che provocano dei danni sugli interessati.

Come si può notare le sanzioni predisposte sono graduali e definiscono un tetto massimo al quale le multe possono arrivare poiché spetterà all'organo competente stabilirne l'esatto ammontare. Sarà infatti valutata la natura, gravità e durata della violazione, se vi è responsabilità dolosa o colposa, quali sono state le misure adottate per limitare il danno, il grado di cooperazione con l'Authority e la tempestività o meno della notifica della violazione, ma anche quali dati sono stati sottratti, il rispetto di precedenti ammonimenti, provvedimenti, ingiunzioni ed altre circostanze aggravanti o attenuanti (benefici finanziari, perdite evitate, ecc.). Anche le organizzazioni no profit e di volontariato, ad esempio, sono soggette a sanzioni, le cui multe saranno appunto valutate dall'Authority, consapevole della loro particolare struttura.

Sanzioni Penali

Il GDPR prevede anche sanzioni penali (che saranno stabilite da una normativa non ancora esistente, ma che dovrà essere introdotta entro il 21 maggio 2018) qualora si accertasse il trattamento illecito dei dati, la falsità nelle dichiarazioni e notificazioni al Garante, oltre che l'inosservanza di misure di sicurezza e dei provvedimenti del Garante.

Oltre le Sanzioni

Secondo l'articolo 58, le autorità possono avvalersi inoltre di una serie di poteri correttivi come la possibilità di limitare o addirittura vietare un trattamento dei dati da parte dell'azienda. Tutto ciò potrebbe portare l'organizzazione ad interrompere l'erogazione di un servizio o un'attività, a danno dei clienti che potrebbero richiedere un risarcimento. Si potrebbe pertanto in casi estremi ad arrivare a compromettere l'esistenza stessa dell'azienda.

Il DATA PROTECTION OFFICER (DPO)

Anche se già obbligatoriamente presente in alcune nazioni europee, il GDPR ha introdotto la figura del DPO in tutti i membri dell'Unione. Si tratta di un soggetto indipendente (interno o esterno alle organizzazioni e un gruppo di imprese o soggetti pubblici può nominare un unico DPO) il cui compito è quello di osservare, valutare e organizzare la gestione e protezione del trattamento di dati personali in conformità alla legge. La sua nomina deve essere obbligatoria per tutti le amministrazioni ed enti pubblici (tranne le autorità giudiziarie), per i soggetti la cui attività principale consiste in trattamenti che richiedono il controllo regolare e sistematico degli interessati e per tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici. AL fine di riuscire nel proprio compito, il