talleri law

Lugano, 17 giugno 2018
68|16 RT/mp

A CHI DI COMPETENZA

GDPR (General Data Protection Regulation)

ATTENZIONE: il presente documento non costituisce un parere legale. Esso intende sensibilizzare al tema della protezione dei dati alla luce del Regolamento europeo in materia.

*** *** ***

Il GDPR, o meglio il "General Data Protection Regulation", è un regolamento dell'Unione europea entrato di fatto in vigore dal 25 maggio 2018. Esso è stato pubblicato sulla Gazzetta ufficiale dell'Unione Europea già due anni orsono, anche se ciò non ha permesso di giungere alla data dell'entrata in forza della norma con una percentuale importante di aziende, anche in Europa, adeguatamente preparate. Questo elemento lascia intendere che le Autorità amministrative competenti (i diversi garanti della privacy degli Stati Europei), in questa prima fase faranno verosimilmente capo a misure meno incisive di quelle che il Regolamento consente (fra gli altri la multa per i casi più gravi fino a Euro 20 milioni oppure il 4% del fatturato globale della società responsabile della violazione). Ci si può aspettare quindi che all'inizio le autorità di vigilanza intervengano con ammonimenti o raccomandazioni. Questo non significa sottovalutare la norma, che comunque consente all'interessato di agire in giudizio contro il titolare o il responsabile del trattamento, che avessero violato i propri obblighi.

Scopo del GDPR è quello di proteggere i dati personali delle persone fisiche e quindi non si applica ai dati personali delle persone giuridiche. Non si applica neppure ai dati personali gestiti in un contesto privato (se a titolo non professionale utilizzo un social network non sarò tenuto ad adempiere i compiti del GDPR).

Avv. Rocco Talleri
Iscritto al registro cantonale degli avvocati

Talleri Law
Studio legale

Crocicchio Cortogna 2
P.O. Box 6544
CH - 6901 Lugano

Tel. +41 91 921 45 47
Fax +41 91 921 45 49

info@talleri.ch
talleri.ch

L'attività di fiduciario svolta ai sensi della LFid implica la gestione, da parte dei fiduciari e delle fiduciarie, di importanti volumi di dati sensibili, spesso anche di persone fisiche.

Nonostante il Regolamento europeo non sia, a differenza degli Stati membri dell'EU, una norma direttamente applicabile alla Svizzera, nel nostro Paese, come nel resto del mondo all'infuori dell'EU, il GDPR torna applicabile in virtù dell'art. 3 GDPR che recita:

1. Il presente regolamento si applica ***al trattamento dei dati personali*** *effettuato nell'ambito delle attività di uno* ***stabilimento da parte di un titolare del trattamento*** *o di un responsabile del trattamento* ***nell'Unione****, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.*

2. Il presente regolamento si applica ***al trattamento dei dati personali di interessati che si trovano nell'Unione****, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*
a) ***l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione****, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure*

b) ***il monitoraggio del loro comportamento*** *nella misura in cui tale comportamento ha luogo all'interno dell'Unione.*

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Quindi, semplificando, se:

- avete uno stabilimento d'impresa nell'EU,
- trattate dati di cittadini residenti nell'EU nell'ambito di offerte di beni e servizi a tali cittadini,
- monitorate il loro comportamento tramite una piattaforma web o dei servizi online, oppure
- contrattualmente torna applicabile il diritto dell'EU ad alcuni Vostri contratti

la Vostra attività ricadrà sotto il GDPR.

In ogni caso, a prescindere dal GDPR, si tenga conto che la revisione totale della Legge federale sulla protezione dei dati, che dovrebbe entrare in vigore a breve, imporrà comunque l'adozione di misure importanti per la tutela dei dati personali; si consiglia pertanto di valutare un adeguamento della struttura.

Per valutare l'esposizione al Regolamento appare utile una verifica della struttura societaria della fiduciaria. Dopodiché, prima di poter intervenire, occorre conoscere nel dettaglio quali tipi di dati vengono raccolti, da chi e come vengono gestiti, dove vengono conservati e per quali finalità. Questo tenendo conto anche dell'organizzazione interna dell'attività. In questo modo posso rendermi conto in quale maniera vengono effettivamente trattati i dati personali all'interno della struttura. Per poter intervenire occorre avere un quadro documentato della situazione, ciò che implica quindi l'allestimento di un rapporto. Le prime misure che si possono prendere sono quelle di avere un inventario dei dati, che permetta di verificare se i dati personali sono gestiti con il consenso dell'interessato, se sono aggiornati, se sono corretti, se sono necessari allo scopo per il quale sono stati raccolti e se quindi rispecchiano i diritti dell'interessato. Nella misura in cui si dovesse disporre di newsletter o di sistemi automatizzati di comunicazione, occorrerà verificare che se i destinatari sono residenti nell'EU, abbiano acconsentito espressamente all'uso dei loro dati anche a fini di marketing.

L'attività di adeguamento al GDPR implica la conoscenza in azienda dal titolare/CEO fino a tutti i dipendenti dell'importanza di una corretta gestione dei dati. È quindi importante sensibilizzare tutti i collaboratori e le collaboratrici, facendo in modo di evitare l'accesso ai dati sensibili a coloro che non ne hanno bisogno per svolgere il mandato conferito dal cliente/interessato.

Sarà inoltre opportuno valutare l'adeguamento dei mandati ricevuti da cittadini residenti nell'EU.

Qualora si disponesse di servizi esternalizzati (outsourcing), siano essi legati al cloud computing o a servizi di fatturazione o spedizione, si consiglia di far verificare tali contratti e soprattutto di prevedere che i vari prestatori di servizio (che il GDPR definisce "responsabili del trattamento"), garantiscano a loro volta il rispetto della normativa.

Non vi è una formula generica per essere adeguatamente preparati al GDPR, ogni caso necessita di una valutazione specifica. I punti di seguito riassunti, che riprendono quanto qui esposto, vogliono essere, come indicato, lo stimolo a

analizzare e a prendere coscienza dell'importanza dei dati personali. Spesso le aziende e la dirigenza non conoscono nel dettaglio alcune dinamiche interne, ciò che poi rende più complesso intervenire. Questo è quindi un invito a svolgere, da parte dei titolari, rispettivamente del CDA, delle fiduciarie, un'accurata analisi della propria attività.

I. ANALISI STRUTTURA FIDUCIARIA

1. Presente solo in CH o anche in EU?
2. Gestione dati personali solo in CH o anche in EU?

II. ANALISI DATI

1. Quali dati gestisco? Di chi?
2. Come vengono elaborati? Da chi? Per quale motivo?
3. Dove si trovano i dati?
4. Chi ha accesso ai dati?
5. Come sono protetti?

III. ANALISI ORGANIZZAZIONE

1. Organigramma
2. Verifica contratti con i dipendenti e i collaboratori
3. Compiti e competenze
4. Accesso ai dati
5. Struttura sistema informatico (dove si trovano i dati? come sono protetti? Ci sono sistemi di controllo? ecc);
6. Outsourcing (contratti servizi IT, cloud, prestazioni, ecc);
7. Sito internet, a chi mi rivolgo? Raccolgo informazioni sugli utenti? Offro servizi? Ecc.

IV. ALLESTIMENTO DI UN RAPPORTO

1. Allestire un rapporto con le indicazioni sopra riportate.

V. MISURE INIZIALI

1. Allestire un inventario dei dati (tipologia, scopo, ubicazione, diritti d'accesso) e verificare che i dati siano attuali, corretti, adeguati allo scopo per cui sono stati raccolti.
2. Sensibilizzare i collaboratori e prevedere eventuali adeguamenti dei contratti.
3. Per i cittadini residenti nell'EU si consiglia di chiedere sistematicamente il consenso all'utilizzo dei dati raccolti, prevedere una dichiarazione sul trattamento dati, con il diritto all'accesso, alla rettifica, alla cancellazione (dopo il periodo legale che ne impone la conservazione).
4. Verifica e adeguamento contratti coi fornitori di servizi che trattano o hanno accesso ai dati personali dei clienti (fornitori di servizi IT, servizi di fatturazione, spedizione, stampa, trasporto, ecc.)
5. Adeguamento misure di sicurezza (prevedere controllo d'accesso ai dati, possibilità di tracciare /impedire l'accesso, sistemi di trasmissione sicuri, misure di backup adeguate sia contro l'accesso non autorizzato (mediante codifica) e la distruzione).

Cordiali saluti

Avv. Rocco Talleri