18 newsletter
ottobre 2017

Novità legislativa

PRIVACY - REGOLAMENTO UE 679/2016

Cambia l'approccio del legislatore: necessario un adeguamento che tenga conto della specifica realtà di ciascuna impresa. Il termine ultimo di adeguamento alla nuova normativa (non prorogabile) scade il 25.5.2018

Il legislatore europeo, consapevole della complessità delle attività da porre in essere per dar corso all'adeguamento normativo, aveva fissato in due anni il termine ultimo per concludere dette attività. Ormai mancano poco più di sette mesi alla scadenza del termine e la stragrande maggioranza delle imprese non ha ancora preso atto della portata della nuova normativa e delle conseguenze che posso derivare dal mancato adeguamento.
A differenza che nel passato, le conseguenze del mancato adeguamento sono infatti estremamente gravi: **sanzioni amministrative (da 10 a 20 milioni di euro o dal 2% al 4% del fatturato)**. Permangono poi le **responsabilità civili e penali** in capo ai soggetti cui è riconducibile l'inadempimento degli obblighi normativi.
Inoltre, trattandosi di normativa che riguarda direttamente l'adeguatezza degli assetti organizzativi e amministrativi dell'impresa, il mancato rispetto della stessa comporterà una **responsabilità in capo agli organi di amministrazione e di controllo** delle società inadempienti.
SLM, in partnership con qualificati advisors, offre un'attività di consulenza atta a garantire un puntuale adeguamento alla nuova realtà normativa, consentendo di prevenire le gravi conseguenze che possono derivare dalla non adeguatezza del modello organizzativo Privacy e IT.

La normativa italiana in materia di protezione dei dati personali attualmente vigente è contenuta nel **D.lgs. 196/2003 (cd. Codice Privacy)**, che ha recepito la Direttiva 46 del 1995 e la Direttiva 58 del 2002 in materia di comunicazioni elettroniche.
Con l'entrata in vigore (il 24.05.16) e la piena applicazione (dal 25.05.18) del Regolamento UE 679/2016 (d'ora in poi **Regolamento**), che riguarda la protezione dei dati personali delle sole persone fisiche, sarà automaticamente abrogata la Direttiva 46/1995 e, di conseguenza, le norme che l'hanno recepita in Italia non potranno più trovare applicazione laddove in contrasto con quanto sancito dal Regolamento. Inoltre, anche nel caso in cui le norme del Codice Privacy non siano manifestamente in contrasto con il Regolamento (ad esempio laddove siano maggiormente dettagliate) occorrerà valutare caso per caso se le prime rispettino i nuovi principi dettati dal legislatore europeo.

STUDIO LEGALE MARCHIONNI & ASSOCIATI

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

Un esempio è quello delle **norme relative alle misure minime di sicurezza** disciplinate in maniera molto precisa ed analitica dall'Allegato B del Codice Privacy. Il Regolamento in proposito si basa sul "nuovo" principio dell'*accountability,* ossia sul principio della "responsabilizzazione" del titolare (e responsabile) del trattamento nel valutare, determinare e mettere in atto non già misure minime di sicurezza predeterminate, ma **misure che siano adeguate al caso concreto, ossia alla specifica realtà aziendale**. Non è quindi più la legge a indicare quali siano le misure minime da rispettare, ma spetta al titolare (e responsabile) del trattamento l'obbligo di individuare ed adottare, in considerazione dei rischi concretamente individuati, le specifiche misure e procedure, adeguate alla propria realtà aziendale, atte a garantire gli obiettivi indicati dalla normativa (cd. approccio basato sul rischio).
Da qui la necessità per il titolare (e il responsabile) del trattamento di effettuare innanzitutto un'adeguata "analisi dei rischi", informatici e non, volta a valutare se le misure attualmente adottate possano ritenersi adeguate al caso concreto (in particolare tenendo conto dei rischi di distruzione, perdita, modifica, accesso accidentale o illegale, divulgazione non autorizzata dei dati personali trasmessi, conservati o comunque trattati con mezzi informatici o meno, nonché dei rischi di illecito trattamento).
Si tratta quindi di pianificare ed adottare tutte le misure adeguate alla specifica realtà aziendale per garantire una protezione dei dati fin dalla progettazione dei sistemi di raccolta e trattamento dei dati (cd. ***privacy by design***) e per garantire che siano trattati solo quei dati personali necessari per ogni specifica finalità del trattamento (cd. ***privacy by default***).
Taluni obblighi ed adempimenti previsti dalla nuova normativa comunitaria sono già contemplati dalla legislazione italiana vigente, ma, se fino ad oggi il mancato rispetto della normativa poteva avere conseguenze non particolarmente impattanti (le sanzioni amministrative più gravi previste dal Codice sono pari al massimo ad 60.000 euro), con la definitiva entrata in vigore del Regolamento, **le sanzioni pecuniarie potranno ammontare sino a 10 milioni di euro** (o sino al 2% del fatturato se superiore) per le tipologie di violazioni "meno gravi" **o sino a 20 milioni di euro** (o sino al 4% del fatturato se superiore) per altre tipologie di violazioni (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), e pertanto sono tali da mettere in taluni casi a repentaglio la stessa sopravvivenza dell'impresa, **coinvolgendo altresì personalmente i membri degli organi di amministrazione e di controllo.** Parallelamente, le relative **sanzioni penali** continueranno invece ad essere previste ed applicate dal legislatore italiano.

***

Il Regolamento, oltre ad aver ribadito alcuni Principi Generali già presenti nel nostro Codice (**trasparenza**: l'interessato deve essere sempre informato sui propri diritti di accesso, di rettifica, di limitazione di trattamento, di opposizione, di tutela; **liceità**: il trattamento deve essere basato, alternativamente, sul consenso dell'interessato, sull'adempimento di obblighi contrattuali, su interessi vitali della persona interessata o di terzi, su obblighi di legge cui è soggetto il titolare, sull'interesse pubblico o sull'esercizio di pubblici poteri, sull'interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati; **proporzionalità**: il trattamento deve essere limitato ai soli dati indispensabili per le specifiche finalità perseguite; conservazione dei dati per un tempo limitato allo scopo; **sicurezza**), ha introdotto anche rilevanti novità**:**
- **obbligo di procedere ad una "valutazione di impatto"** (che costituisce parte integrante dell'approccio *Privacy by Design*) e che deve contenere almeno (i) una descrizione dei trat-

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

tamenti previsti e delle finalità del trattamento; (ii) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; (iii) una valutazione dei rischi per i diritti e le libertà degli interessati; iv) le misure previste per affrontare i rischi; in particolare, tale obbligo sussiste allorquando il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone, ad esempio in caso di utilizzo di sistemi di videosorveglianza, di geolocalizzazione e di profilazione degli utenti;

- **obbligo di nominare un responsabile esterno o co-titolare in tutti i casi di outsourcing**, ossia laddove sia affidata l'esecuzione di determinati servizi a terzi che, in quanto tali, trattino i dati personali in nome e per conto o nell'interesse del titolare (il che è più che frequente, come ad esempio nei casi di esternalizzazione del servizio di elaborazione delle paghe, di imbustamento e consegna di corrispondenza, di archiviazione/conservazione sostitutiva dei documenti aziendali, di gestione dati e sistemi informatici, di sistemi di videosorveglianza, di noleggio mezzi dotati di scatola nera), nonché di **contrattualizzare il relativo rapporto**: il che significa che occorrerà concludere per iscritto o revisionare (laddove già esistenti) i contratti con ciascun "fornitore" di tali servizi, nominando quest'ultimo (che non potrà rifiutare) responsabile (esterno) del trattamento;
- **obbligo di contrattualizzare per iscritto il rapporto tra eventuali contitolari del trattamento** (ossia quando siano due o più soggetti a determinare congiuntamente le finalità ed i mezzi del trattamento - come ad esempio nel caso di associazioni professionali o società articolate in direzioni generali o in sedi decentrate o periferiche, dotate di poteri decisionali del tutto autonomi circa i trattamenti che si effettuano nel loro ambito);
- **introduzione della figura del DPO** (*Data Protection Officer* o **responsabile della Protezione dei dati**), che avrà una funzione di consulenza e controllo, nonché di coordinamento con il Garante e potrà essere un dipendente particolarmente competente in materia, ma preferibilmente un professionista esperto in *diritto privacy* (tenuto conto della indipendenza che deve caratterizzare tale funzione); il DPO deve essere nominato **obbligatoriamente** in determinati casi, ossia quando le attività principali del titolare consistano in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali (sostanzialmente quelli che nel codice vigente sono definiti "dati sensibili");
- **introduzione di eventuali meccanismi di certificazione** (approvati da appositi organismi qualificati e riconosciuti) e possibilità di aderire a **Codici di condotta approvati dal Garante** (eventualmente elaborati dalle associazioni di categoria cui i titolari sono iscritti), che assumono rilevanza anche (ma non solo) in caso di trasferimenti di dati verso paesi terzi (extra UE). In proposito, salvo specifici casi tassativamente previsti, il trasferimento dei dati verso paesi terzi è legittimo solo se sussiste una decisione della Commissione europea sull'adeguatezza del paese terzo o se effettuato sulla base di clausole contrattuali o di norme vincolanti d'impresa adottate/approvate dalla Commissione o sulla base della predetta certificazione e dell'adesione a un Codice di Condotta (o in presenza di autorizzazione nazionale, ossia del Garante, ora necessaria solo in caso di utilizzo di clausole contrattuali non riconosciute dalla Commissione Europea);
- **introduzione dell'obbligo per il titolare (e per il responsabile del trattamento) di tenere il Registro delle attività di trattamento** (che di fatto confluisce nel DPS - Documento programmatico sulla Sicurezza già presente in azienda), dove devono essere contenute determinate informazioni (relative al titolare, agli eventuali contitolari, rappresentanti, responsabili del trattamento e responsabile della protezione dei dati, alle finalità del trattamento, alle categorie degli interessati e dei dati personali, alle categorie dei destinatari a cui sono o saranno comunicati i dati -compresi destinatari

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

di paesi terzi o organizzazioni internazionali-, nonché, ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati ed una descrizione delle misure di sicurezza tecniche ed organizzative progettate ed adottate).

Oltre agli obblighi sopra descritti, che potremmo definire di prevenzione dei rischi connessi al trattamento, è stato infine introdotto anche l'obbligo di **notificare e comunicare all'autorità di controllo** (ed in determinati casi anche ai diretti interessati) **la violazione dei dati personali, entro il termine di 72 ore** (nell'ottica di limitare i potenziali danni).

***

Le tempistiche per lo svolgimento delle attività necessarie per adeguare il "modello privacy" di una impresa di medie dimensioni varia da poche settimane ad alcuni mesi. Non a caso il legislatore comunitario aveva previsto un **termine (tassativo e non prorogabile) di due anni** dalla data di entrata in vigore della nuova normativa, che scadrà definitivamente il 25.5.2018.

Tenuto conto delle gravi conseguenze di legge nel caso di violazione degli obblighi dalla stessa sanciti, si appalesa quanto mai opportuno (se non indispensabile) fare ricorso all'opera di professionisti qualificati per dare corso (nei pochi mesi ormai a disposizione) ad un corretto adempimento delle attività di adeguamento, individuando le **lacune e i correttivi** da apportare, in particolare attraverso:

- la verifica della corretta formalizzazione per iscritto delle **deleghe/nomine** e dei **contratti** che definiscano i ruoli e le responsabilità di tutti i soggetti coinvolti (eventuale contitolare, eventuale responsabile interno, responsabile esterno dei trattamenti, responsabile della protezione dei dati, incaricati del trattamento), nonché delle **procedure di controllo e vigilanza** sui soggetti medesimi;
- la verifica della correttezza dei **contenuti dell'informativa/consenso** agli interessati (clienti/utenti, fornitori, dipendenti, anche in relazione ad esempio ad eventuali controlli elettronici sugli utenti e sui dipendenti, per i quali è anche necessario un accordo sindacale o, in mancanza, l'autorizzazione della Direzione territoriale del Lavoro competente) e dei **contenuti del proprio sito web** (si pensi che da una stima di Federprivacy del 2016 oltre il 30% dei siti web italiani non è in regola con quanto prescritto dalla normativa relativa);
- la **predisposizione o revisione e modifica** (laddove già esistente) della **documentazione** di cui sopra (testi delle informative/consensi, testi contenuti nel sito e nei social media, testi contrattuali, Registro dei Trattamenti, ecc.), il **coordinamento tra le procedure documentali e le soluzioni e procedure informatiche** adottate e l'**adattamento e l'implementazione dei processi** necessari al corretto adeguamento imposto dal legislatore, anche in modo da **favorire** il necessario **controllo periodico** e **facilitare** un **costante adeguamento** e rispetto delle norme **nel tempo (cd. approccio "strutturato e continuo")**;
- non ultimo, la **formazione** dei deleganti e dei delegati, dei responsabili del trattamento (come ad esempio degli amministratori di sistema, degli agenti commerciali, dei responsabili delle risorse umane), degli addetti ai controlli elettronici e quindi dei dipendenti (anche al fine di rendere autonoma l'impresa nella gestione degli adempimenti privacy).

***

Porre in essere tale adeguamento, cui è comunque obbligatorio dare corso e che ogni imprenditore è tenuto a completare in **tempi ormai ristretti** avrà certamente un costo non banale, ma occorre anche sottolineare che questo obbligo può rappresentare (ove le attività di assessment e di organizzazione sia affrontate con spirito costruttivo) un'**opportunità per l'impresa per acquisire maggiore efficienza e valore.** L'obbligo di adeguamento può infatti rappresentare l'occasione per incrementare i livelli di sicurezza, ottimizzando quei processi operativi cui oggi nessuna impresa può ormai più sottrarsi anche al fine di proteggere il patrimonio informa-

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

tivo riservato della propria azienda ed il regolare svolgimento della propria attività commerciale.

ULTERIORI INFORMAZIONI SU QUESTO ARGOMENTO O SU FATTISPECIE CORRELATE POSSONO ESSERE RICHIESTE A:

avv. Fabrizio Marchionni e avv. Rosanna Visintainer
+39 0461 23100 – 260200 - 261977
fm@slm.tn.it rv@slm.tn.it

DISCLAIMER

Le Newsletter di SLM rappresentano uno strumento di informazione gratuito a disposizione di tutti coloro che siano interessati a riceverle (newsletter@slm.tn.it). Le Newsletter di SLM non possono in alcun caso essere considerate pareri legali, né possono essere ritenute idonee a risolvere casi specifici in assenza di una preventiva valutazione della fattispecie concreta da parte di un legale.

INFORMATIVA EX ART. 13 D. LGS. 196/2003 (Codice Privacy) ED ART. 12 a 22 REGOLAMENTO UE 679/2016 (Regolamento)

Le Newsletter di SLM sono inviate esclusivamente a soggetti ("interessati") che hanno liberamente fornito i propri dati personali in ragione di rapporti professionali intercorsi con SLM, o in occasione di convegni, seminari, master (o eventi di altro genere), o all'atto della navigazione e/o registrazione in questo sito web e/o attraverso messaggi di posta elettronica, per la finalità di ottenere aggiornamenti giuridici ed informazioni sull'attività di SLM.

I dati usati per l'invio delle newsletter si limitano all'indirizzo email dell'interessato e ad eventuali dati anagrafici (nome e cognome, denominazione e ragione sociale, sede o domicilio) e di reperibilità, forniti dall'interessato stesso o raccolti da SLM presso pubblici registri o elenchi (es. professionali) e/o su pagine internet.

A tal fine i dati possono essere trattati con o senza l'ausilio di mezzi elettronici e/o telematici ed essere utilizzati e comunicati per la finalità sopra indicata ai dipendenti e collaboratori di SLM, incaricati e/o responsabili del trattamento e non a terzi. In caso di necessità, per attività legate alla manutenzione della parte tecnologica del sito SLM, i dati possono essere trattati da incaricati di Maciej Michno, responsabile del trattamento dei dati ai sensi dell'art. 29 del Codice Privacy e 28 del Regolamento.

Idonee misure di sicurezza sono osservate per prevenire la perdita di dati, usi illeciti o non corretti ed accessi non autorizzati.

Il conferimento dei dati è facoltativo ed il rifiuto a fornire i dati stessi comporta soltanto

l'impossibilità di ottenere i servizi di SLM ed in particolare il servizio newsletter.
I dati forniti sono trattati nel rispetto dei diritti degli interessati, dei requisiti e delle modalità previsti dal d.lgs. 30 giugno 2003 n. 196 (Codice) e dal Regolamento UE 679/2016 (Regolamento). La durata del trattamento perdurerà a tempo indeterminato fino a quando l'interessato non revochi validamente il consenso se precedentemente prestato, oppure fino a quando l'interessato non comunichi l'opposizione all'ulteriore trattamento per finalità di invio newsletter.
L'interessato ha i diritti previsti dall'art. 7 del Codice e tra cui il diritto, in ogni momento di: i) ottenere la conferma dell'esistenza o meno dei dati che lo riguardano e la loro comunicazione, nonché di conoscerne l'origine; ii) ottenere l'aggiornamento, la rettifica, l'integrazione dei medesimi e verificarne l'esattezza. L'interessato può inoltre chiedere la limitazione del trattamento, la cancellazione, la trasformazione in forma anonima, la portabilità dei dati o il blocco dei dati trattati in violazione di legge, nonché opporsi in ogni caso, per motivi legittimi, al loro trattamento e proporre reclamo ad un'autorità di controllo.
Il titolare del trattamento è Studio Legale Marchionni & Associati (SLM), con sede in Trento, Viale San Francesco d'Assisi n. 8 ed i trattamenti dei dati connessi al servizio Newsletter hanno luogo presso la predetta sede e, in limitati casi di stretta necessità, presso la sede del terzo manutentore tecnico sopra indiato Maciej Michno – Consulenza Web, UX, informatica, con sede in Trento, via dei Guarinoni 18.
L'interessato può rivolgersi, tramite l'indirizzo e-mail rv@slm.tn.it, per esercitare i diritti sopra indicati e per ottenere ulteriori informazioni.
Il considerando 47 al Regolamento indica che un interesse legittimo del titolare, idoneo a costituire una valida base giuridica del trattamento dei dati personali, può essere costituito dalla finalità marketing diretto.
Ciononostante, chi avesse ricevuto o ricevesse le Newsletter di SLM per errore oppure desiderasse non ricevere più comunicazioni di questo tipo in futuro o comunque intendesse revocare il consenso prestato al trattamento può comunicarlo in ogni momento inviando una email a rv@slm.tn.it oppure cliccando il tasto "*annulla iscrizione*" posto in calce a ciascuna newsletter.

Per maggiori informazioni su privacy and cookies policy si veda anche in calce a ciascuna pagina del sito SLM

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it