Informativa sul General Data Protection Regulation n. 2016/679

Il 25 maggio 2018 è entrato in vigore il nuovo Regolamento Europeo in materia di protezione dei dati personali che prevede un nuovo regime sulla protezione dei dati personali.
La Direttiva n. 95/46, che disciplinava a livello comunitario il trattamento dei dati, è stata espressamente abrogata dal Reg. 2016/679.
Il Regolamento è divenuto immediatamente operativo anche in Italia in quanto - diversamente dalla Direttiva - è direttamente vincolante in ogni sua parte sia per gli Stati membri che per i cittadini dell'Unione.
Il Decreto Legislativo n. 101/2018 del 10.08.2018 (Decreto Privacy – adeguamento della normativa nazionale alle disposizioni del Regolamento Europeo) è entrato in vigore il 19.09.2018 ed ha modificato ed integrato il Codice in materia di protezione dei dati personali del 30.06.2003 n. 196.

La nuova disciplina è incentrata sul principio di "*accountability*", ovvero sull'esigenza di incentivare i Titolari del trattamento al principio di responsabilizzazione in materia di privacy, adottando comportamenti proattivi tali da assicurare l'effettiva applicazione del Regolamento.
In particolare, secondo il concetto di Data Protection by Design, viene affidato ai Titolari il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative ed alla luce di alcuni criteri specifici indicati nel regolamento stesso.

Ciò premesso, è stata predisposta una *check list* (sulla base delle Linee Guida dettate dal Garante Privacy) che consenta ai Titolari del Trattamento di capire quali sono i principali requisiti da implementare, e comprendere se la propria organizzazione, sia da un punto di vista logistico, sia di sicurezza informatica sia adeguata a tale normativa.

1) E' stata scritta una informativa sulla protezione dei dati e messa a disposizione dei vostri dipendenti e iscritti?

Il GDPR prevede, infatti, la creazione di una informativa sulla protezione dei dati per documentare come viene svolto il trattamento dei dati.
Tale documentazione deve essere scritta in forma semplice, chiara, e descrivere il fine della raccolta dati, i diritti del titolare dei dati, se tali dati saranno trasferiti all'estero e con quali strumenti, nonché il periodo di conservazione. L'informativa sarà utile nel migliorare la comprensibilità della logiche di trattamento dei dati personali da parte dei vostri associati e/o iscritti, dipendenti ed eventualmente potrà essere fornita alle autorità di vigilanza.

Sul sito è possibile inserire tra le varie informazioni una sezione dedicata alla Privacy Policy.

2) E' stata strutturata una protezione de dati secondo la nuova normativa, ovvero secondo il concetto ivi espresso di Data Protection by Design?

I titolari del trattamento dei dati hanno il compito di decidere in completa autonomia le modalità di trattamento dei dati personali, la loro conservazione, le garanzie, la conservazione ed i limiti del trattamento stesso alla luce dei principi enunciati del Regolamento europeo 2016/79.
Occorre, pertanto, che prima del trattamento dei dati, siano adottate le garanzie per un corretto trattamento dei dati personali anche da un punto di vista informatico. La tecnologia, infatti, costituisce un valido aiuta nella implementazione delle procedure di sicurezza nel trattamento dei dati.
Sul punto, sarebbe utile da un punto di vista informatico – al fine di adeguarsi al principio di *accountability* dettato dal Regolamento – dotarsi di sistemi di sicurezza informatica sia sotto un profilo di backup dei dati che di eventuale crittografazione degli stessi, nonché di accesso mediante password, il tutto al fine di scongiurare l'ipotesi di perdita degli stessi.

3) E' stata redatta una analisi dei rischi relativa al trattamento dei dati?

Uno degli obblighi del titolare è individuare e mitigare i rischi derivanti dal trattamento dei dati, attraverso una valutazione che tenga conto dei rischi noti, e delle misure tecniche organizzative che il titolare deve adottare per minimizzare il rischio discendente dal trattamento dei dati personali.
Il titolare del trattamento dei dati deve valutare il rischio prima di iniziare il trattamento, in base all'esito della valutazione, può procedere al trattamento, oppure consultare l'autorità di controllo, in tale secondo caso l'Autorità avrà il compito di indicare le misure ulteriori da adottare per implementare le misure correttive ai sensi dell'art. 58 (dall'ammonimento del titolare fino alla limitazione o al divieto del trattamento stesso).
A tal fine, è indispensabile effettuare un'analisi delle categorie di dati personali ed interessati coinvolti nel trattamento e pertanto elencare le categorie di interessati e dati personali raccolti e conservati (ad es. relativi al personale dipendente, dati relativi agli iscritti e/o agli associati), dello scopo per i quali i dati vengono raccolti, valutare se vengono trattate speciali categorie di dati personali (ad es. dati sanitari, genetici, biometrici).

4) E' stato nominato un Responsabile della Protezione dei Dati?

La nomina di un responsabile, il cd "DPO" è obbligatoria solo per alcune tipologie di organismi.
In particolare, quando il trattamento e le attività principali siano svolte da un organismo pubblico, o consistano in elaborazioni che richiedano un controllo sistematico dei dati e del loro flusso, oppure consistano in elaborazioni su larga scala di dati personali sensibili o che abbiano rilevanza penale.
Il Garante incoraggia la nomina di un DPO in via cautelativa anche laddove la nomina non è obbligatoria, ma deve essere munito di tutti i mezzi necessari per lo svolgimento del suo ruolo, comprese le risorse economiche per implementare le misure di sicurezza opportune. Il DPO può far parte del personale del titolare del trattamento (RPD interno) ovvero assolvere i suoi compiti in base ad un contratto di servizi (RPD esterno). Se il medesimo viene scelto tra i dipendenti non dovrà avere posizioni in conflitto di interesse. In tal caso l'RPD sarà in diretto contatto con la realtà dell'organismo al fine di poter effettuare e verificare tutte le situazioni concrete di rischio. In tale ipotesi, il dipendente dovrà essere adeguatamente formato mediante appositi corsi al fine di poter assolvere all'incarico e dovrebbe anche disporre di risorse economiche ed organizzative a budget per poter implementare le misure necessarie a tutela della privacy.
Nel caso invece, in cui la funzione di RPD venga svolta da un fornitore esterno di servizi, i compiti stabiliti potranno essere assolti efficacemente anche da un team operante sotto l'autorità di un contatto principale designato quale responsabile.
Resta inteso che in virtù del principio di *accountability*, la responsabilità rimane totalmente in carico al Titolare del Trattamento per il caso di eventuali violazioni e non anche all'RPD.

5) E stato creato un registro dei trattamenti?

Tale strumento è obbligatorio per le realtà che abbiano 250 dipendenti, mentre per le altre non è obbligatorio a meno che l'elaborazione dei dati comporti un rischio elevato per gli individui, l'elaborazione riguardi i dati cd sensibili e non sia occasionale.
E' in ogni caso auspicabile anche per le realtà minori dotarsi di un registro dei trattamenti, mediante programma in file di Excel nel quale vengano rispettati i seguenti contenuti obbligatori:
a) Nome e dati di contatto del titolare del trattamento e se nominati del rappresentante del titolare del trattamento e del responsabile della protezione dati (RPD).
b) Finalità del trattamento.
c) Descrizione categorie interessati a cui i dati sono stati o saranno comunicati compresi i destinatari dei paesi terzi od organizzazioni internazionali.

Il Garante privacy ha recentemente chiarito (successivamente all'entrate in vigore della normativa di adeguamento italiana) come il registro sia in realtà necessario anche per le PMI (piccole-medie imprese) sulla base di criteri inerenti la tipologia di attività svolta.

6) Durante la raccolta dei dati personali dei associati, iscritti, dipendenti, viene utilizzato un processo di raccolta del consenso per il trattamento successivo dei dati?

Il trattamento di qualsiasi dato personale deve avvenire previo espresso ed informato consenso del titolare del dato stesso circa la sua raccolta, il suo utilizzo e la conservazione del medesimo per fini contrattuali, chiaramente espressi nella informativa.
Occorre, poi, informare che i dati personali, su richiesta del titolare, potranno essere modificati, cancellati o trasferiti.
Occorre che venga stabilita una procedura specifica per la conservazione dei dati stessi, che siano archiviati in modo sicuro e che l'accesso a tale archivio avvenga da parte di personale autorizzato e opportunamente formato.

7) In caso di incidente di sicurezza che coinvolga i dati personali (distruzione, perdita, modifica o divulgazione indebita dei dati, c.d. *data breach*) occorre un processo di gestione dell'incidente e della relativa notifica al Garante.

Se è stato nominato un Responsabile della Protezione dei dati, procederà lui stesso a tale notifica, in caso di mancanza di un DPO, la relativa notifica dovrà essere effettuata dallo stesso organismo, in persona del Titolare, previa indicazione dell'incidente di sicurezza, con contestuale indicazione di tutte le procedure e misure di sicurezza adottate fino a quel momento.
La notifica va effettuata nell'immediatezza del *data breach* e, precisamente, entro 72 ore dall'accadimento.

8) Esiste una procedura per il trasferimento dei dati all'estero, in particolare fuori dell'Unione Europea?

Se i dati personali vengono trasferiti all'estero, fuori della UE, deve essere presente un registro di trattamento, con identificazione del paese terzo e della documentazione che esistano adeguate garanzie per conservazione e trattamento dei dati fuori UE.

9) E' stato offerto ai dipendenti un corso di formazione o campagne di sensibilizzazione in tema protezione dei dati personali?

Uno dei compiti del RPD (e, comunque del Titolare del Trattamento) è quello di aumentare la sensibilizzazione e fornire la formazione a tutti i dipendenti dell'azienda e, in particolare, al personale coinvolto nel trattamento dei dati personali.

10) Durante la raccolta dei dati personali dei vostri associati, iscritti, dipendenti viene usato un processo di consenso esplicito e specifico?

Nessun consenso è valido in caso di silenzio assenso, di casella selezionata di default o di inattività della persona. Inoltre, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei dati personali.

11) Siete in grado di dare alle persone l'accesso a tutti i loro dati personali?

Occorre adottare misure per fornire agli individui i mezzi per richiedere ed accedere ai propri dati personali a titolo gratuito, in modo che essi possano liberamento modificare, cancellare o esercitare la propria opposizione al trattamento. A tal fine può esser utile creare una mail apposita dedicata alla privacy (privacy@ …….. .it). I clienti hanno diritto di portabilità dei dati e pertanto di ricevere i propri dati in modo strutturato, comunemente usato e leggibile da un computer. La persona può anche richiedere al titolare l'invio in forma elettronica dei dati che lo riguardano.

12) Esiste una procedura per la conservazione dei dati personali?

La conservazione dei dati trattati in violazione dei diritti degli interessati rappresenta un trattamento illecito passibile di sanzioni amministrative. Il periodo di conservazione non deve superare il tempo necessario per il raggiungimento dello scopo per il quale sono stati raccolti.

13) Sanzioni

La violazione delle previsioni del Regolamento, comportano sanzioni molto elevate fino a 20.000.000,00 di euro e (per le aziende) di importo pari al 4% del fatturato dell'anno precedente. I singoli Stati (ivi compresa l'Italia) hanno definito ulteriori sanzioni, anche penali, che dovranno essere effettive, proporzionate e dissuasive, fino a poter vietare il trattamento (con conseguenze ancor più gravi di una sanzione amministrativa).

(a cura dell'Avv. Silvia Cannovale Palermo)