Nuovo Regolamento Europeo per la Protezione dei Dati Personali

Introduzione alle novità e descrizione di un possibile approccio metodologico

La Commissione europea ha sviluppato, a partire dal 2012, il cosiddetto «pacchetto protezione dati» con lo scopo di dare una risposta alla necessità dei cittadini rispetto al rischio di vedere diminuito il controllo sui propri dati, a fronte della progressiva diffusione massiva di tecnologie che consentono la raccolta e la gestione di enormi quantità di dati relativi ai comportamenti delle persone (es. app, social network, internet of things,…). Il pacchetto si compone di due diversi strumenti, il Regolamento e la Direttiva. Per la nostra trattazione ci soffermeremo in particolare sul **Regolamento**, concernente «la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati», volta a disciplinare i trattamenti di dati personali sia nel settore privato sia nel settore pubblico in tutti gli stati membri dell'Unione Europea. Il Regolamento è stato adottato dal Parlamento Europeo nell'aprile 2016 e diventerà **definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.** Nello stesso sono definite le sanzioni amministrative pecuniarie per la eventuale violazione delle disposizioni fino ad un massimo di **20 Milioni di €** o fino **al 4 % del fatturato mondiale totale annuo dell'esercizio precedente,** se superiore. Le aree di novità rispetto alla normative vigente italiana (Codice in materia di protezione dei dati personali) sono illustrate nella figura di seguito riportata:

1. **Responsabilità:** il GDPR promuove la **responsabilizzazione (accountability)** dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali possa comportare per i diritti e le libertà degli interessati.
2. **Data Protection Officer:** viene introdotta la figura del «Data Protection Officer» **(DPO)**, o «Responsabile della Protezione dei Dati» (RPD) che deve essere designato dal Titolare o dal Responsabile del trattamento e dovrà adempiere alle sue funzioni in piena **indipendenza** ed in **assenza di conflitti di interesse**
3. **Informative:** vengono stabilite **regole più chiare** in merito all'informativa ed al consenso con precisi limiti al trattamento automatizzato dei dati, alla relativa violazione ed all'interscambio degli stessi al di fuori della Comunità Europea.
4. **Data Protection Impact Assessment:**
   4.1. Obbligo per ciascun Titolare di svolgere e documentare una **autovalutazione del rischio** prima di procedere al singolo trattamento**,** se il tipo di trattamento può presentare un rischio elevato *per «i diritti e le libertà delle persone»*.

UHY Italy provides a wide variety of services, ranging from corporate and organizational consulting, to corporate assistance, as well as tax and consulting assistance, audit, payroll and outsourced services.

UHY Advisor Srl, UHY Associati Stprl, UHY Bompani Srl, FiderConsult Srl are all members of UHY Italy

Our partners are certified professionals with years of experience in public practice and with leading international firms.

Via Birmania 81
00144 Roma
Tel. +39 06 591.74.69
Fax +39 06 591.35.82

Via Bernardino Telesio 2
20145 Milano
Tel. +39 02 480.12.534
Fax +39 02 481.81.43

Viale Giuseppe Mazzini 26
50132 Firenze
Tel. +39 055 234.79.02
Fax +39 055 234.79.09

www.uhyitaly.com
info@uhyitaly.com

4.2. Il Titolare è tenuto a consultare **preventivamente** l'autorità Garante qualora la valutazione d'impatto potenziale sulla protezione dei dati presenti un rischio elevato.

4.3. Il DPIA è un processo **indispensabile** per valutare la necessità e la proporzionalità delle contromisure da implementare per gestire i rischi derivanti dal trattamento di dati personali.

5. **Diritti degli interessati:** vengono introdotte nuove prerogative riconosciute agli interessati al trattamento, tenendo conto dell'attuale sviluppo delle nuove tecnologie: Diritto alla **cancellazione** (cosiddetto Diritto all'oblio), Diritto alla **portabilità e** Diritto di **limitazione.**

6. **Privacy by design & by default:**

6.1. Le misure idonee a proteggere i dati devono essere implementate fin dalla nascita dell'esigenza di trattamento e della realizzazione dei mezzi con cui effettuarlo (**privacy by design**).

6.2. Deve essere garantito il trattamento esclusivamente per le finalità per cui è stato autorizzato e per il periodo di tempo strettamente necessario a tali finalità (**privacy by default**).

7. **Registro del Trattamento:** è introdotto l'obbligo per il Titolare e il Responsabile del trattamento di **conservare**, *«anche in formato elettronico»*, un registro dei trattamenti effettuati, contenente alcuni specifici dettagli quali, ad esempio, le finalità del trattamento, la descrizione delle categorie di interessati, la descrizione generale delle misure di sicurezza tecniche e organizzative, etc.

8. **Data breach notification:** è altresì trodotto l'obbligo per il Titolare di **notificare** eventuali violazioni dei dati personali del trattamento comunicandoli all'Autorità di Controllo, senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza.

Per rispondere con efficacia agli adempimenti richiesti dal GDPR, le **Aziende dovranno predisporre un piano di adeguamento** che dovrà essere calibrato sulle proprie esigenze e sui reali impatti normativi, prediligendo il principio di proporzionalità. Organizzazioni diverse sia per dimensione che per complessità, devono conciliare il più possibile la necessità di conformità con la sostenibilità economica e organizzativa del nuovo impianto privacy. **Il nuovo Regolamento ha un impatto trasversale su tutta l'Organizzazione Aziendale e prevede gruppi di lavoro multidisciplinari** per rispondere adeguatamente alle disposizioni normative. Saranno coinvolte le funzioni/direzioni aziendali: Risorse Umane, Organizzazione, Legale, Compliance, Sistemi Informativi, singoli Responsabili del trattamento delle funzioni operative se presenti. **UHY Italy (**organizzazione italiana del network di società di consulenza e di revisione, **UHY International)** con i suoi professionisti specializzati sulla materia in argomento, propone un approccio metodologico per la conformità al menzionato Regolamento Europeo, che si compone dei seguenti pilastri progettuali:

1. **Analisi e valutazione dell'AS-IS**: valutazione dell'attuale modello organizzativo adottato per la gestione della Privacy e censimento di alto livello delle misure di controllo in essere (presidi), sia tecniche che organizzative richieste.
2. **Gap Analysis e definizione roadmap di adeguamento:** dai risultati della fase precedente di Analisi e valutazione dell'As-Is, si procede con una prima valutazione delle modifiche organizzative che dovranno essere adottate e con una Gap Analysis effettuata con l'ausilio di specifici tool. Al termine viene predisposta una Roadmap di adeguamento.
3. **Definizione della Metodologia per il DPIA:** viene definita la metodologia per l'esecuzione del Data Protection Impact Assessment (DPIA) ed i Profili di Protezione da applicare ai singoli trattamenti.
4. **Attuazione del piano di adeguamento:** sono individuate e dettagliate le esigenze di adeguamento dell'impianto procedurale e definiti e documentati compiti e modalità operative con cui il Data Protection Officer (DPO) dovrà svolgere il proprio mandato. Viene inoltte fornito supporto ai Sistemi Informativi nella valutazione dei presidi tecnico/organizzativi implementati, al fine di garantirne l'adeguatezza rispetto ai profili di protezione individuati.

20 settembre 2017

♣♣♣

Visitate il nostro sito web:
http://www.uhyitaly.com.

Per ulteriori informazioni:
info@uhyitaly.com