STUDIO ASSOCIATO CONSULENTI DEL LAVORO
SALVATORE LAPOLLA E CARLO CAVALLERI

16128 - GENOVA - VIA CORSICA, 9/2 SC. B - TEL. 010 5455511 - FAX 010 5704028

E-MAIL: *lapolla@tpservice.it* *cavalleri@tpservice.it*

CIRCOLARE 10/2018 **Genova, 05/04/2018**

Oggetto: LA NUOVA LEGGE SULLA PRIVACY EUROPEA IN VIGORE DAL 24 MAGGIO 2016

Anche se materia che esula dalle nostre competenze come Diritto del Lavoro e come attività di Studio e sicuri dell'attenzione dei professionisti specializzati che seguono le vostre aziende in merito all'oggetto, desideriamo comunque informarvi che **la nuova legge sulla privacy** approvata dal parlamento europeo è divenuta legge operativa in tutti gli stati membri dell'unione a far data dal 24 maggio 2016.

Le norme transitorie presenti nel testo di legge permettono ai titolari del trattamento di adottare quanto previsto dal suddetto testo di legge, **entro e non oltre il 25 maggio 2018**.

Nello specifico vi sono molte nuove prescrizioni e misure inserite nel testo normativo e che andranno meglio definite con decreto legge da parte degli stati membri.

Le modifiche di maggior rilevanza sono le seguenti.

- **Analisi dei rischi** preliminare con conseguenti **misure di sicurezza.**
- **Il Responsabile per la Protezione dei Dati** (Data Protection Officer, nuova figura che può essere assimilata all'evoluzione del Responsabile Privacy e del Consulente Privacy).
- La tenuta di un **Registro dei Trattamenti** (in parte simile al vecchio DPS) con indicazione delle misure di adottate per ridurre i rischi, dei trasferimenti dati verso organizzazioni internazionali ovvero verso l'estero (comprensive anche delle decisioni di adeguatezza in merito espresse da parte dell'Autorità Garante a livello europeo), le basi giuridiche del trattamento, gli interessi perseguiti, etc.
- **Il Piano per l'Impatto sui Trattamenti Dati** (Data Protection Impact Assessment - DPIA).

- L’interpello preventivo all’Autorità Garante per trattamenti indicati come a rischio grave nel DPIA con **potenziale blocco preventivo delle attività.** Il Garante potrebbe impiegare fino a 14 settimane prima di permettere la ripresa dei trattamenti (per trattamenti in corso prima del 25 maggio) o l’inizio degli stessi.
- **L’autodenuncia** entro 72 ore **dall’accesso illegittimo sui dati trattati** da parte di terzi.
- La presenza o meno di dati di minori, dati genetici, dati personali particolari e dati biometrici.
- La creazione di **contratti con i responsabili, che prevedano il diritto di ispezione** da parte dei titolari al trattamento nelle strutture dei responsabili **stessi**,.
- I software dovranno essere adeguati ed ingegnerizzati – per i nuovi software – con le modalità privacy previste dalla legge.
- La certificazione privacy, o sigillo di Garanzia Europeo, è una certificazione volontaria simile a quella sulla qualità, sarà emessa da organismi riconosciuti dall’Autorità Garante.

  I trattamenti svolti da soggetti certificati saranno identificati come trattamenti a rischio ridotto.
- I **Responsabili** dovranno tenere un **registro dei trattamenti** contenente, in aggiunta, le **categorie dei trattamenti effettuati** per ogni singolo titolare unitamente ai dati di contatto del Responsabile del trattamento, del **rappresentante** del titolare, del **Responsabile della protezione dei dati** (data protection officer). Attenzione particolare dovrà essere posta da parte dei responsabili nel rispetto della vigente normativa poiché in difetto del quale il Responsabile al trattamento diventerebbe Titolare rientrando nel meccanismo sanzionatorio gravante sui titolari al trattamento (fino a 20 mln di euro od il 4% del fatturato dell’anno precedente)
- Un panorama sanzionatorio che oscilla fino ad un massimo di 20 milioni di euro o il 4% della sommatoria mondiale del fatturato annuale per una multinazionale.

Cercando di entrare, anche se in sintesi pratica, nel dettaglio:

1) **Responsabile Sicurezza Dati – Data protection officer.**

Il Responsabile della sicurezza dei dati, svolge per il Titolare, i seguenti compiti:

A. vigilare e monitorare il corretto e continuo rispetto della normativa di riferimento in materia di trattamento dati, portando all'attenzione dei vertici aziendali situazioni potenzialmente pericolose per i dati;
B. erogare formazione periodica verso gli incaricati al trattamento dati;
C. valutare in maniera critica – da un vertice di osservazione relativo alla protezione dei dati – l'operato ed i progetti dell'Ente;
D. dare indicazioni al fine di risolvere problematiche, verificatesi o potenziali, relative alla privacy;
E. preparare l'azienda - con sufficiente anticipo - per il recepimento di nuovi provvedimenti emanati dall'autorità garante;
F. se del caso, redigere l'auto denuncia da inoltrare all'autorità garante laddove vi siano data breaches, nonché dare riscontro alle richieste dell'autorità garante;
G. laddove necessario redigere il piano di impatto sulla protezione dei dati (data protection impact assessment).

Il Responsabile della Sicurezza dei Dati effettua attività ispettive autonome, acquisisce le informazioni dal management dell'Ente che lo coinvolge in ogni processo decisionale o di modificazione del trattamento dati ed emette atti e consulenze al fine di indirizzare l'operato dell'Ente in maniera da risultare rispondente alla normativa vigente.

Il Responsabile della Sicurezza dei Dati svolge compiti simili a quelli di un "Garante Privacy interno" all'azienda in modo da indirizzare in modo funzionale per la data protection.

2) **Piano di Impatto sulla protezione dei dati - Data Protection Impact Assessment.**

Il Piano di Impatto sulla protezione dei dati è un piano preventivo che viene redatto a tutela delle libertà ed i diritti degli interessati ed il suo svolgimento è monitorato dal Responsabile della sicurezza dei dati. Ogni progetto apportante significativi cambiamenti al trattamento dei dati (siano essi occorrenti a livello risorse umane, strumenti elettronici hw o sw, aree di trattamento, processi, procedure, dati trattati – tipologia, estensione, modalità) potrebbe necessitare di un Piano di Impatto.

3) **Registro dei trattamenti.**

Il Registro delle attività di Trattamento contiene gli estremi identificativi delle figure chiave per le responsabilità in capo ai trattamenti, le finalità di trattamento, la descrizione delle categorie di interessati e dei dati personali ad essi riferiti, gli estremi identificativi dei soggetti o categorie di soggetti a cui i dati saranno comunicati, l'identificazione soggetti esteri e dei paesi terzi verso i quali i dati saranno trasferiti unitamente alla documentazione a supporto delle garanzie di adeguatezza dei suddetti soggetti, i termini previsti per la cancellazione dei dati degli interessati, la descrizione generale delle misure tecniche ed organizzative previste dall'articolo 32 paragrafo 1. Detto paragrafo prevede, tra le altre misure:

a. le misure idonee a garantire un livello di sicurezza adeguato ai rischi incombenti sui dati. (derivanti da preventiva analisi dei rischi);
b. le misure di pseudonimizzazione (1);
c. le misure di cifratura dei dati;
d. le misure per assicurare la resilienza dei sistemi (2) di trattamento, la capacità di ripristinare tempestivamente i sistemi e l'accesso ai dati in caso di incidente fisico o tecnico;
e. le procedure di verifica regolare circa l'efficacia delle misure tecniche ed organizzative per garantire la sicurezza dei trattamenti.

4) Meccanismi di certificazione.

La certificazione privacy europea è uno strumento che rappresenta un'innovazione rispetto a quanto previsto dal d.lgs. 196/03. Di per sé non esime il Titolare al trattamento dalle conseguenze di illeciti, fraudolenti o volontariamente non conformi trattamenti effettuati, tuttavia risulta essere funzionale per:

a. comprovare la rispondenza normativa di quanto viene certificato (sia essa l'azienda nella sua totalità od un singolo processo) nei confronti dei clienti, autorità, pubbliche amministrazioni (immaginiamo, ad esempio, una p.a. o un soggetto pubblico economico che non desideri verificare la rispondenza normativa dei partecipanti ad una gara d'appalto ma che si limiti ad attribuire maggiori punti a coloro che sono certificati per la privacy europea);
b. mitigare le sanzioni pecuniarie
   - "…al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi …omissis …..
   - "l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e"

Auspicando di aver fatto cosa gradita andando a ribadire l'argomento, lasciamo ovviamente ai professionisti che seguono per voi questa materia, l'analisi sia delle procedure che degli obblighi in merito.

Studio Associato
Consulenti del Lavoro
Salvatore Lapolla e Carlo Cavalleri

---

(1) La pseudonimizzazione ovvero la sostituzione dei dati identificativi con codici che non consentono di individuare i singoli interessati.
(2) La resilienza dei sistemi it ovvero la capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati

SCHEMA ATTIVITÀ GDPR

ATTIVITÀ PRELIMINARI

- GAP ANALYSIS PRELIMINARE INDICARE I MOTIVI DELLE AZIONI DA INTRAPRENDERE E DI QUELLA DA NON INTRAPRENDERE
- **ANALISI PRELIMINARE**
- PRINCIPIO DI RESPONSABILIZZAZIONE (ACCOUNTABILITY) RISPETTARE I PARADIGMI DELLA ISO 31000
- **MAPPATURA ED ANALISI DEI RISCHI**
- INSERIRE NEL REGISTRO TRATTAMENTI
- **ADOZIONE MISURE IDONEE PER RIDURRE I RISCHI**
- SOLO VERSO NUOVI INTERESSATI O NUOVI TRATTAMENTI DI DATI
- **ANALISI E REDAZIONE INFORMATIVE**
- COMMERCIALISTA, CONSULENTE DEL LAVORO, MEDICO COMPETENTE
- **GESTIONE RESPONSABILI**
- PRIVACY BY DESIGN, PRIVACY BY DEFAULT
- **SOFTWARE E TRATTAMENTI A NORMA**

ATTI E DOCUMENTI DA PRODURSI

- DOCUMENTO IDONEO A COMPROVARE LA PROPRIA "ACCOUNTABILITY"
- **REGISTRO TRATTAMENTI (REGISTRO ATTIVITA' DI TRATTAMENTO)**
- PER CASISTICHE PARTICOLARI O RISCHI ALTI NON SANATI DA MISURE DI SICUREZZA ADOTTATE ISO 29134;2017
- **PIANO DI IMPATTO SUI DATI DPIA DATA PROTECTION IMPACT ASSESSMENT**
- DA EFFETTUARSI CASO DI RISCHI ALTI NELLA DPIA FINESTRA TEMPORALE DI RISPOSTA FINO A 14 SETTIMANE. PRIMA DELLA RISPOSTA NON SI POSSONO PIÙ (ANCORA) TRATTARE I DATI
- **INTERPELLO PREVENTIVO AUTORITÀ GARANTE PER LA PRIVACY**

ATTIVITÀ ULTERIORI

- UNI 11697:2017
- **DATA PROTECTION OFFICER**
- ISDP 10003_2015
- **CERTIFICAZIONE VOLONTARIA**
- **ADESIONE A CODICI DI CONDOTTA**
- **TRASFERIMENTO DI DATI ALL'ESTERO**
  - I TRASFERIMENTI OCCORRONO ANCHE IN CASO DI SALVATAGGIO DI DATI SU SERVER ESTERI (EMAIL, CLOUD, SISTEMI GESTIONALI)
  - VERIFICARE SE IL PAESE è OGGETTO DI DECISIONE DI ADEGUATEZZA
  - IN ASSENZA DI DECISIONI DI ADEGUATEZZA, VERIFICARE LA POSSIBILITà DI TRASFERIRE COMUNQUE I DATI NEL PAESE ESTERO

ATTIVITÀ NON SISTEMATICHE O DI EMERGENZA

- A RICHIESTA DEGLI INTERESSATI
- **DARE RISCONTRO INTERESSATI**
- A RICHIESTA DEGLI INTERESSATI
- **AGGIORNARE, CANCELLARE DATI**
- A RICHIESTA DEGLI INTERESSATI
- **SOSPENDERE TRATTAMENTI**
- FATTE SALVE LE CIRCOSTANZE PREVISTE ENTRO 72 ORE DAL MOMENTO DELLA CONOSCENZA DELL'ACCESSO
- **NOTIFICA ACCESSO ABUSIVO AI DATI AUTORITÀ GARANTE PER LA PRIVACY**
- FATTE SALVE LE CIRCOSTANZE PREVISTE
- **INFORMARE TUTTI GLI INTERESSATI CIRCA L'AVVENUTO ACCESSO ABUSIVO RELATIVAMENTE AI LORO DATI**