GDPR

Il nuovo Modello Organizzativo sul Trattamento dei Dati

(sulla base del Regolamento Europeo Privacy Ue 2016/679)

Con l'entrata in vigore del Regolamento sulla Protezione dei dati | Reg. (UE) 2016/679 le aziende devono affrontare il tema della "compliance" privacy, in una prospettiva nazionale ed internazionale, esponendosi altrimenti al rischio di sanzioni molto elevate.

A ciò si aggiunga che i dati personali e le informazioni confidenziali sui dati aziendali sono un asset fondamentale per qualsiasi tipo di attività, anche in ragione dello sviluppo sempre più crescente del trattamento dati automatizzato.

A tal proposito il Regolamento obbliga le figure dei Titolari e Responsabili del trattamento a rivedere ed aggiornare tutta i documenti aziendali, ad applicare misure di sicurezza adeguate ed idonee, sia tecnologiche che organizzative, ed a garantirne la loro efficacia: la cd "**accountability"**.

Il Regolamento sostituisce la precedente normativa e introduce una sostanziale inversione della prova: per non rispondere del danno emergente da trattamenti non leciti occorre dimostrare di aver fatto tutto il possibile per evitarlo (Art. 5).

La **3A** ha sviluppato una proposta di soluzioni e servizi al fine di rispondere in modo puntuale e su misura alle esigenze del Cliente rispetto alle nuove regole introdotte dal GDPR.

La **3A,** dunque, è in grado di supportare Titolari e Responsabili del trattamento nell'adempimento delle prescrizioni normative derivanti dal Regolamento Privacy UE, già in vigore dal 25 maggio 2018.

In riferimento al Regolamento Privacy la **3A** è in grado di fornire assistenza e consulenza legale su:

- Messa a norma privacy (Full service)
- Stesura documenti e procedure di privacy; servizio pareri ed opinioni legali privacy; supporto continuo al referente privacy.
- Valutazioni preliminari (DPIA) evaluation Organization and outsourcing
- Privacy funzionale ed altre attività di compliance Cross Border Data Transfer Regulation
- Assistenza per attività con il garante privacy
- Assistenza per reclami, ricorsi e segnalazioni presso il garante Assistenza presso la Giustizia Ordinaria (civile, penale ed amministrativa)
- Formazione specifica e supporto per il **DPO** interno e assunzione del ruolo di DPO esterno;

Composizione dell'offerta

1. Attività incluse

In considerazione del contesto normativo e di quello operativo della vostra azienda, le attività che si prevede di attuare saranno le seguenti:

- raccolta di informazioni per identificare e censire le attività di trattamento;
- interazione con le diverse funzioni aziendali per analizzare e adeguare i flussi di comunicazione e la gestione documentale nel rispetto della normativa europea in materia di privacy
- predisposizione, verifica e aggiornamento continuo della documentazione

Privacy necessaria a consentire lo svolgimento delle attività aziendali e a supporto di tutte le aree aziendali nel rispetto della normativa di riferimento;

- redazione del Registro delle Attività di trattamento;
- supporto nella determinazione delle modalità di trattamento in particolare per i trattamenti che presentano rischi per l'interessato e supporto nell'esercizio del "bilanciamento dei diritti" (a mero titolo esemplificativo, utilizzo videosorveglianza a bordo mezzi, trattamenti di dati sensibili riferiti agli utenti, etc);
- controllo formale ed eventuale redazione dei documenti richiesti dalla nuova normativa privacy, necessari per il corretto trattamento dei dati e per dimostrare la conformità al Regolamento 679/2016;
- analisi e verifica della conformità delle attività di trattamento e delle procedure aziendali interne;
- verifica o redazione di privacy policy interne al fine informare, consigliare e fornire raccomandazioni in merito all'utilizzabilità dei dati personali trattati.
- predisposizione/revisione informative verso clienti, dipendenti, utenti e in generale ogni tipologia di interessato e relativi moduli per la raccolta del consenso: tale documento dovrà indicare tutti i nuovi contenuti dell'art. 13 del Regolamento europeo;
- revisione e/o redazione di Contratti/nomine a responsabile del trattamento che il titolare dovrà effettuare;
- supporto al titolare nella predisposizione organigramma privacy;
- predisposizione nomine per l'autorizzazione al trattamento dei dati personali per il personale incaricato a vario titolo;
- predisposizione del "Registro delle violazioni" (**Data Breach**)[1];
- analisi dei rischi per i trattamenti censiti da documentare e allegare al registro dei trattamenti;
- consulenza per l'adeguamento normativo alle misure di sicurezza in ambito privacy (GDPR 679/2016, D.Lgs. 196/2003, Misure minime di cui alla "Circolare AgID n. 1/2017" del 17 marzo 2017), nonché per le misure necessarie emanate dall'Autorità Garante per la protezione dei dati personali negli specifici provvedimenti a carattere generale e relativa redazione documentale;
- predisposizione e aggiornamento del registro delle verifiche di sicurezza;
- effettuazione di verifiche in merito alla validità delle misure di sicurezza adottate e compilazione del relativo registro delle verifiche con cadenza almeno annuale;
- assistenza nella predisposizione di una eventuale "valutazione d'impatto sulla protezione dei dati" o DPIA (Data Protection Impact Asessment)[2] e

[1] L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro settantadue ore dal momento in cui ne viene a conoscenza. La novità del GDPR, già applicabile dal 25 maggio 2018, è l'estensione dell'obbligo a tutti i titolari.

[2] valutazione d'impatto sulla protezione dei dati (**Dpia – Data Protection Impact assessment).** È un processo inteso a garantire e dimostrare la conformità al regolamento europeo e i rischi legati al trattamento dei dati. valutazione d'impatto sulla protezione dei dati (Dpia – Data Protection Impact assessment). È un processo inteso a garantire e dimostrare la conformità al regolamento europeo e i rischi legati al trattamento dei dati. la Dpia "è obbligatoria in tutti i casi in cui un trattamento di dati

sorvegliare i relativi adempimenti;

- formazione specifica e supporto per il DPO interno e assunzione del ruolo di DPO esterno;
- formazione e sensibilizzazione del personale che partecipa ai trattamenti;
- verifica della documentazione contrattuale per confermare la compatibilità con la nuova normativa privacy indicando eventuali clausole da apporre in caso di carenza;
- verifica/integrazione documentazione relativa alla videosorveglianza: in relazione ai sistemi di videosorveglianza, saranno verificati gli adempimenti in relazione allo Statuto dei Lavoratori (ex art. 4 L. 300/70), informative, nomine, cartellonistica, producendo la documentazione necessaria
- revisione del Regolamento Aziendale sulle politiche di trattamento dei dati personali e sul corretto utilizzo degli strumenti informatici e consulenza in materia di privacy nel rapporto di lavoro e controlli a distanza (navigazione Internet e posta elettronica);
- analisi sito web ufficiale dell'azienda e formulazione delle azioni correttive (redazione di informative, istruzioni per eventuali modifiche, etc.);
- redazione di eventuali pareri pro veritate in materia di privacy su questioni controverse che si dovessero rappresentare;
- monitoraggio continuo della normativa in materia di protezione dei dati personali;
- fungere da punto di contatto per l'Autorità Garante per la protezione dei dati personali e per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti qualora non venga designato un DPO interno.

2. Attività escluse

Sono escluse dalla nostra offerta le seguenti attività:

- Revisione di contratti e attività specifiche di carattere legale.
- Sviluppo o modifica di processi aziendali o procedure informatiche.
- Interventi e servizi relativi a dispositivi ICT e infrastrutture.
- Fornitura di hardware o software.

---

può presentare un rischio elevato per i diritti e le libertà delle persone", per esempio quando avviene con l'uso di nuove tecnologie. In particolare il regolamento individua 9 casi specifici:

1. Trattamento valutativi o di scoring, compresa la profilazione.
2. Decisioni automatizzate che producono significativi effetti giuridici (assunzioni, concessioni di prestiti, stipula di assicurazioni).
3. Il monitoraggio sistematico (videosorveglianza).
4. Trattamento di dati sensibili, giudiziari o di natura estremamente personale (come le opinioni politiche).
5. Trattamento dati personali su larga scala.
6. Trattamento di Big Data.
7. Trattamento di dati di soggetti vulnerabili (anziani, minori, richiedenti asilo).
8. Trattamento di dati con l'utilizzo di nuove tecnologie (riconoscimento facciale, dispositivi IoT, ecc…).
9. Trattamento che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

È sufficiente che sussistano due delle nove condizioni allora la Dpia è obbligatoria.

- Procedure o relazioni con Clienti e/o Fornitori.
- In generale, qualsiasi attività non specificata al precedente punto “Attività incluse”.

3. Modalità di esecuzione

Il servizio sarà erogato, operando presso la sede della vostra azienda o da remoto, attraverso nostro personale qualificato organizzato in un team di persone, con competenze specifiche.
Per ottimizzare e velocizzare lo svolgimento delle attività potranno essere coinvolti più consulenti, operanti in parallelo, per lo stesso profilo. Le ore di attività stimate si riferiscono sempre a ore/uomo.

Il cliente prende atto che la presente offerta si riferisce esclusivamente all’azienda cui è intestata, anche nel caso l’azienda fosse parte di un gruppo, sia nella posizione di capofila che di membro.

Infatti, la responsabilità dell’autocertificazione, ai fini del GDPR, è in capo all’azienda stessa come entità giuridica.

4. Obbligo di Riservatezza

La nostra azienda s’impegna a mantenere confidenziali le informazioni di cui venga a conoscenza nell’espletamento del suo incarico per l’intera durata del rapporto e per gli anni successivi, salvo gli obblighi di legge o regolamentari ed i provvedimenti della magistratura.

5. Responsabilità

L’attività di consulenza proposta nella presente offerta non costituisce un trasferimento di responsabilità verso il fornitore. Infatti, in base al GDPR, la responsabilità è esclusivamente in capo al responsabile del trattamento (titolare, rappresentante legale, management …) che deve dimostrare, attraverso un documento di auto valutazione, di aver analizzato i rischi e adottato metodi adeguati per ridurli e potenzialmente annullarli.

Si rimane a disposizione per ulteriori approfondimenti e per formalizzare l’offerta economica, rispetto ai servizi anzi specificati.

Palermo 30/05/2018