DataVerso

Protezione e governance per il patrimonio delle informazioni

Modello organizzativo per la data protection ai sensi del GDPR

(GENERAL DATA PROTECTION REGULATION-REGOLAMENTO UE 2016/679)

Servizio in collaborazione con

PACTA AVVOCATI ASSOCIATI | VIA BATTAGLIONE VAL CHIESE, 10 – 36100 VICENZA

SOLUZIONI S.R.L. | VIA UGO LAMBERTINI, 6 - 40026 IMOLA (BO)

INTRODUZIONE

Premessa

Nel presente documento con il termine Sistema di Controllo Preventivo Privacy ai sensi del D.Lgs. 196/03 e del GDPR (General Data Protection Regulation - Regolamento UE 2016/679) (d'ora in poi, per brevità, indicato anche con "Sistema di Controllo Privacy" o con "Sistema Privacy" o con "Modello Organizzativo Data protection") si intende un Sistema formalizzato in documenti che riportano l'insieme delle componenti definite ed adottate dalla Società per la gestione e il trattamento dei dati personali, in base a quanto disposto dal D.Lgs. 196/03 e dal GDPR (General Data Protection Regulation - Regolamento UE 2016/679).

Con il termine Sistema di autoregolamentazione aziendale (d'ora in poi, per brevità, indicato anche con "Sistema autoregolamentazione") si intende l'insieme degli strumenti predisposti dall'azienda per la regolamentazione delle proprie attività (quali Manuali, Regolamenti, Procedure, Istruzioni, Moduli e ogni altro documento di autoregolamentazione esistente in applicazione di Sistemi di gestione adottati, in adempimento a norme di legge e/o per lo svolgimento della gestione in linea con gli obiettivi aziendali).

INQUADRAMENTO

Gli aspetti rilevanti del GDPR rispetto alla precedente normativa

Dalla riservatezza alla protezione dei dati personali

Il concetto di Privacy si è andato a modificare e si modificherà con l'evoluzione tecnologica e dei servizi che sempre più velocemente pervadono le nostre attività e la nostra vita privata.

Si passa dalla riservatezza dei dati personali alla protezione dei dati, intendendo con tale termine la protezione del contesto complessivo in cui si svolgono i trattamenti dei dati.

Il GDPR mira a adeguare la *data protection* rispetto al contesto - politico, economico e sociale - di riferimento e all'evoluzione tecnologica. Il mutato contesto ha reso sempre più centrali l'impatto e la cultura del dato. L'evoluzione tecnologica sta determinando un crescente valore economico e sociale del dato e un progressivo aumento dei dati scambiati tra attori pubblici e privati, rendendo così necessari - da un lato - una più libera circolazione di dati all'interno dell'Unione Europea, ma - dall'altro - un più elevato livello di protezione.

Approccio basato sulla valutazione del rischio

Una delle principali novità è il principio di *accountability* che richiede al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate a garantire - ed essere in grado di dimostrare - che il trattamento è effettuato conformemente al GDPR. L'approccio è basato sulla valutazione del rischio: la conformità al GDPR si fonda su un processo di risk management e deve essere integrata nei processi aziendali.

In pratica, una volta individuati e valutati i rischi rilevanti in ambito Privacy, il Titolare deve valutare – con modalità che gli consentano di poterlo dimostrare - l'adeguatezza delle misure organizzative e tecniche adottate per mitigare i rischi rilevati ad un livello tale da non ledere i diritti e le libertà fondamentali delle persone fisiche.

Si tratta di una novità rilevante per la protezione dei dati, in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Le misure di sicurezza devono garantire un livello di sicurezza adeguato al rischio del trattamento: si passa quindi dalle misure minime tassativamente previste dalla versione precedente del Codice Privacy ad una valutazione di adeguatezza rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificatamente individuati.

Gestione integrata di tutte le informazioni aziendali

In base a quanto disposto dal GDPR, si rafforza la correlazione tra protezione dei dati personali e sicurezza delle informazioni, tema peraltro sempre più cruciale per ogni azienda in riferimento al valore strategico delle informazioni per la gestione dell'azienda stessa: la distruzione o la divulgazione non consentita di un'informazione di business produce sempre e comunque un danno all'azienda.

Il mutamento di prospettiva indotto nella gestione dei dati personali, l'evoluzione tecnologica e gli scenari di mercato qualificano come metodo più efficace per perseguire e mantenere la conformità al GDPR la gestione integrata di tutte le attività aziendali che riguardano le informazioni nell'ambito di un'impostazione organizzativa unitaria e con un approccio multidisciplinare.

Protezione dei dati personali per lo sviluppo e la crescita del valore

D'altra parte, la trasformazione digitale - che sta interessando e interesserà sempre più i mercati e le attività economiche – rende centrale per la strategia di sviluppo di ogni azienda la gestione dei dati e delle informazioni.

In tale scenario - tanto per sottolineare uno degli aspetti rilevanti del cambiamento - un portafoglio di consensi, da una pluralità di potenziali clienti, al trattamento dei propri dati personali per finalità di marketing (quali trasmissioni di newsletter, profilazione per proposte mirate) costituisce un asset che determina un maggiore valore per l'azienda che lo detiene rispetto al concorrente che ne è privo.

Criteri per la definizione del progetto d'intervento

Il progetto adeguamento del Sistema Privacy ai sensi del GDPR è definito sulla base dei seguenti criteri principali:

- individuare e valutare la situazione aziendale in relazione a quanto disposto dal GDPR (General Data Protection Regulation - Regolamento UE 2016/679), con evidenziazione delle eventuali criticità per gli ambiti di rischio verso cui la Società è esposta;
- definire e condividere, in base agli esiti della valutazione degli ambiti di rischio individuati, gli interventi da realizzare per la realizzazione dell'adeguamento del Sistema Privacy;
- implementare il Sistema Privacy in base al programma condiviso.

Struttura dell'intervento

Fasi principali

In base ai criteri sopraindicati e al complessivo quadro normativo di riferimento, il progetto prevede l'articolazione nelle fasi principali riepilogata nella tabella seguente.

FASE	AMBITO	INTERVENTO PROPOSTO
1	Verifica situazione aziendale in relazione a quanto previsto dal GDPR	Raccolta e analisi documentazione aziendale esistente in riferimento agli adempimenti Privacy e ad ambiti correlati
2	Censimento trattamenti di dati personali svolti	Trasmissione file per il censimento dei trattamenti Assistenza al referente aziendale per la compilazione del censimento dei trattamenti di dati personali svolti
3	Analisi sito web	Analisi eventuali contenuti presenti sul sito web aziendale rilevanti in ambito GDPR (quali privacy policy, cookie policy, informative e formule di consenso)
4	Registro delle attività di trattamento	Verifica censimento dei trattamenti ricevuto e eventuale integrazione in base ad esiti rilevanti dell'analisi documentale e del sito web svolta
5	Analisi dei rischi	Analisi dei rischi e valutazione del livello di adeguatezza delle misure di sicurezza adottate in relazione a quanto disposto dal GDPR
6	Programma di adeguamento	Elaborazione del Programma di adeguamento e/o di miglioramento per lo sviluppo del Sistema Privacy in relazione a quanto disposto dal GDPR

FASE	AMBITO	INTERVENTO PROPOSTO
7	Identificazione delle responsabilità GDPR	Individuazione articolazione responsabilità con riferimento alla struttura interna societaria e ai fornitori esterni Predisposizione schema: • documenti per la designazione dei soggetti interni coinvolti e dei responsabili esterni • clausole contrattuali per i rapporti con i fornitori interessati • istruzioni del titolare per le diverse categorie di soggetti interni e esterni interessati
8	Informative e consensi	Predisposizione dei testi di riferimento per informative e per le relative formule di consenso
9	Adempimenti specifici per Videosorveglianza, geolocalizzazione, biometria e strumenti di tracciamento	Analisi del contesto, circoscritto allo specifico trattamento scaturito dall'utilizzo dei dispositivi, per determinarne la liceità e il percorso necessario a quanto previsto dal GDPR, dal D.lgs. 196/2003 e s.m.i. e dalla specifica normativa di riferimento, quale a titolo non esaustivo la L. 300/1970 – Statuto dei lavoratori.
10	Ulteriori obblighi	Indicazioni per le azioni di adeguamento richieste in caso di trattamenti svolti che comportino ulteriori obblighi specifici [es. nomina del DPO – Data Protection Officer, realizzazione di DPIA – Data Protection Impact Assessment (valutazione di impatto sulla protezione dei dati), garanzie in caso di trasferimento di dati personali fuori dall'Unione Europea]
11	Formazione	Formazione dei soggetti autorizzati
12	Procedure	Definizione di specifiche procedure per *data breach* (violazione di dati personali) e per esercizio dei diritti degli interessati

Tempi di realizzazione dell'intervento

L'intervento sarà svolto indicativamente in circa 3 mesi complessivi. I tempi possono subire variazioni in riferimento alle disponibilità del referente aziendale di progetto.

Le attività saranno iniziate entro circa 1 mese dalla data di ricezione della proposta siglata per accettazione.

Gli interventi saranno definiti in base ad un piano di lavoro concordato con il referente aziendale di progetto e formalizzato durante la prima attività di consulenza.

Personale e competenze impiegate

L'intervento verrà svolto attraverso un Gruppo di Progetto multidisciplinare.

La scelta dei professionisti che compongono il Gruppo di Progetto è finalizzata a garantire la copertura delle diverse professionalità necessarie.

DataVerso

Protezione e governance per il patrimonio delle informazioni

Servizio in collaborazione con

PACTA AVVOCATI ASSOCIATI

PACTA Avvocati Associati

via Battaglione Val Chiese, 10 – 36100 Vicenza

tel. +39 0444 564365

P.IVA, Cod. Fisc.: 03791420247

info@pactavvocati.it www.pactavvocati.it

Soluzioni CONSULENZA MANAGERIALE

Soluzioni s.r.l.

via Ugo Lambertini, 6 - 40026 Imola BO

tel. e fax: +39 0542 640084

P.IVA, Cod. Fisc. e n. Reg. Imprese BO: 02996441206

R.E.A. BO 483301 - Capitale sociale 16.000,00 € i.v.