Corso interaziendale

AUDIT SU PRIVACY, GDPR E GESTIONE DEI DATI PERSONALI: LE NUOVE ESIGENZE

23 e 24 GIUGNO 2021 • Aula virtuale

PRIMA GIORNATA • **23 GIUGNO 2021**

▶ Il trattamento dei dati personali nell'era Covid-19: tra Remote Working e Recovery Phase

- Le implicazioni per la data protection dell'emergenza pandemica Covid-19
- Le indicazioni dell'Autorità Garante Privacy su Coronavirus e protezione dei dati sensibili sulla salute
- Il punto di vista sull'emergenza Covid-19 dell'EDPB e delle Autorità Garanti Europee per la protezione dei dati personali

▶ Il concetto di sicurezza del trattamento dei dati personali ai sensi del GDPR

- I rischi per i diritti e le libertà delle persone fisiche
- L'analisi della probabilità e della gravità del rischio
- L'adozione da parte del Titolare di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio
- Focus: le istruzioni del Titolare ai Responsabili del trattamento e a chiunque agisca sotto la sua autorità in caso di accesso a dati personali

▶ La violazione dei dati personali (data breach): definizione, gestione, possibili conseguenze

- Definizione ed elementi caratterizzanti alla luce del GDPR e delle Linee Guida dell'EDPB (WP Art. 29)
- Esempi di data breach e casistiche di riferimento: accesso o acquisizione dei dati da parte di terzi non autorizzati; impossibilità di accedere ai dati per cause accidentali o attacchi esterni; perdita o distruzione di dati personali a causa di incidenti o eventi avversi; divulgazione non autorizzata dei dati
- I potenziali danni fisici, materiali o immateriali
- Fase di detection di un incidente di sicurezza
- Fase di valutazione dell'incidente di sicurezza volta all'identificazione di un'ipotesi di data breach
- Fase di gestione del data breach: valutazione dell'impatto e prime azioni di mitigazione

▶ La notifica del data breach all'Autorità di controllo

- Quando si deve notificare ai sensi del GDPR
- Quadro sinottico dei casi di notifica
- La procedura di notifica (completa o per fasi): timing, modalità, canali, modulistica
- La comunicazione agli interessati
- La tenuta del Registro delle violazioni di sicurezza

SECONDA GIORNATA • **24 GIUGNO 2021**

▶ Il framework normativo aggiornato relativo ai controlli in materia di data protection

- L'accountability quale principio cardine della nuova normativa e le principali implicazioni per le banche
- I trasferimenti di dati personali al di fuori dell'Unione Europea e il Trasfer Impact Assessment (TIA) a seguito della decisione c.d. "Schrems II"
- Possibili novità normative in ambito data protection

▶ Gli ambiti della data protection da sottoporre al vaglio del Sistema dei Controlli Interni

- Il modello organizzativo della data protection e il ruolo del DPO
- Data mapping e Registro dei trattamenti quale strumento cardine per la gestione ed il monitoraggio
- Analisi dei rischi e Data Protection Impact Assessment
- Modalità di gestione dei rapporti con i fornitori
- Obblighi di trasparenza e modalità di gestione dei diritti degli interessati
- Corpus normativo e documentale in ambito data protection
- Comunicazione e formazione
- La "Privacy by design e by default" nella realizzazione dei prodotti bancari

▶ Le attività di controllo: approfondimento ed analisi dei ruoli del DPO e dell'Internal Audit

- La definizione del Data Protection Control Framework e i ruoli di DPO e Internal Audit
- Metodologia di pianificazione delle attività del DPO e valutazione da parte dell'Audit
- Metodologie e strumenti di revisione delle attività di consulenza e vigilanza in capo al DPO
- Flussi informativi da e verso gli Organi aziendali e le altre Funzioni aziendali di controllo

▶ L'Internal audit nell'ambito del complessivo Sistema dei Controlli Interni sulla data protection

- Le sinergie di ruolo e operative con le altre Funzioni aziendali di controllo
- I controlli di 1° livello: controlli di linea demandati a incaricati del trattamento, Referenti Privacy e Data manager
- I controlli di 2° livello: la verifica della funzione di Conformità rispetto al framework normativo
- I controlli di 3° livello: focus sulla Funzione Internal Audit dedicata al ruolo di assurance sulla complessiva adeguatezza del modello di controllo
- I controlli sulle terze parti, con specifico riferimento ai Responsabili del trattamento