Percorso professionalizzante

PRIVACY EXPERT E DATA PROTECTION OFFICER IN BANCA

1° MODULO • 8, 9 e 10 aprile 2025
2° MODULO • 7, 8 e 9 maggio 2025
3° MODULO • 21, 22 e 23 maggio 2025
TEST FINALE • 29 maggio 2025

Aula virtuale

1° MODULO
PRINCIPI E REGOLE DELLA PRIVACY IN BANCA
8, 9 e 10 aprile 2025

Prima giornata • 8 aprile 2025 (10.00-16.00)

- **Il quadro regolatorio per la privacy in banca: una visione di insieme**
  - General Data Protection Regulation
  - I Provvedimenti del EDPB: impatti per le banche
  - I Provvedimenti di Banca d'Italia rilevanti per la Data Protection
  - Il Data Privacy Framework per i flussi UE-USA
- **Il GDPR e il rafforzamento dei principi relativi al trattamento dei dati**
  - Liceità del trattamento, limitazione delle finalità, proporzione, esattezza e minimizzazione dei dati: come si applicano sulla base anche dei principi previsti dall'art. 5 GDPR
  - Trasparenza sulle informazioni: raccolta dei dati presso l'interessato e presso terzi soggetti
  - Limitazione della conservazione
  - Presupposti di liceità del trattamento dei dati comuni e dei dati particolari
  - Privacy by design e by default: esempi di progetto
- **Il GDPR ed i diritti degli interessati**
  - Diritto di accesso ai dati personali
  - Limitazione del trattamento
  - Diritto alla cancellazione ed oblio
  - Portabilità dei dati
- **I principali soggetti della disciplina privacy**
  - Modelli organizzativi: differenze tra banche di piccole/medie dimensioni e di grandi dimensioni
  - Ruolo e responsabilità del CDA
  - Gli altri ruoli privacy all'interno dell'organizzazione
  - Le istruzioni ai soggetti nominati e designati. Differenze giuridiche sulle responsabilità
  - Il DPO della banca: differenze tra banche di piccole/medie dimensioni e di grandi dimensioni

Seconda giornata • 9 aprile 2025 (10.00-16.00)

▸ Il Responsabile del trattamento
- Ruolo e Responsabilità
- Il monitoraggio sui responsabili del trattamento
- Il rapporto del Responsabile del trattamento con fornitori di servizi: esternalizzazione e protezione dei dati personali
- Il contenuto del Data Processing Agreement e i contenuti minimi contrattuali

▸ Circolazione dei dati all'interno e all'esterno dell'impresa bancaria
- Circolazione dei dati tra banche e nel gruppo bancario
- Attività di recupero credito e di cessione di crediti
- Circolazione dei dati nell'esternalizzazione di servizi
- Trattamento dei dati nell'ambito dei servizi di pagamento: flussi PSD2 e responsabilità degli attori coinvolti

▸ Trattamento dei dati personali della clientela bancaria di altri soggetti e relative implicazioni
- Il codice di condotta in materia di informazioni commerciali: prassi ricorrenti
- L'open banking: tra PSD2 e GDPR. Il provvedimento dell' European Data Protection Board
- Attività di recupero credito e di cessione di crediti: regole e limiti prescritti dall'Autorità

▸ Trattamento dei dati personali a fini di marketing
- Marketing diretto, profilazione e soft spam
- Gestire un sistema di CRM: decalogo delle regole per la gestione dei dati personali
- Consenso e revoca. Gestire lo storico. Durata. Aggiornamenti dei consensi
- La disciplina dei cookie e il graduale superamento degli stessi tramite altri strumenti di tracciamento
- La Privacy Impact Assesment
- La nuova disciplina del telemarketing ed il Codice di Condotta

▸ Esercitazione guidata

Terza giornata • 10 aprile 2025 (10.00-16.00)

▸ La politica legislativa europea sul digitale e sulla protezione dei dati
- Un quadro di insieme sulla strategia digitale della UE e impatti per la sicurezza e protezione dei dati
- Interventi delle autorità e proposte regolatorie sulle tecnologie emergenti
- Il Regolamento Europeo sull'Intelligenza Artificiale
- Data Governance Act
- Evoluzione dell'identità digitale: le modifiche al Regolamento eIDAS ed il superamento di SPID
- Il MiCAR sulle cripto-attività e gli aspetti privacy
- Il Regolamento FIDA

▸ Focus Intelligenza artificiale e la protezione dei dati personali
- La regolamentazione dei sistemi di intelligenza artificiale nell'AI Act
- Punti di contatto con il GDPR
- Basi giuridiche e liceità dei trattamenti effettuati con sistemi di intelligenza artificiale
- Gli interventi delle Autorità e le indicazioni dell'European Data Protection Board in materia di privacy e IA
- Gli adempimenti privacy per l'utilizzo dei sistemi di IA in banca

▸ Focus: Antiriclaggio e privacy: punti di contatto
- La tutela dei dati personali nel contesto della normativa antiriclaggio
- Il bilanciamento tra le normative
- I provvedimenti del Garante in materia di antiriclaggio e le indicazioni dell'EDPB
- Gli adempimenti e l'integrazione delle policy interne antiriclaggio per il rispetto della privacy

2° MODULO

REQUISITI, COMPITI E ATTIVITÀ DEL DPO E DEL PRIVACY EXPERT IN BANCA

7, 8 e 9 maggio 2025

Prima giornata • 7 maggio 2025 (10.00-16.00)

- **Ruolo, compiti e rapporti del DPO in banca**
  - Ruolo e controlli del DPO rispetto alle tre linee di difesa
  - I rapporti con le diverse funzioni della banca: Revisori, IA, IT, Security, Risorse Umane, Responsabile della Conservazione
  - Il DPO come punto di contatto con gli interessati: modalità di gestione e riscontro di richieste e reclami privacy
  - Il DPO come facilitatore dei rapporti con l'autorità, la consultazione di propria iniziativa e la cooperazione su richiesta
  - L'attività di informazione, consulenza e indirizzo: fino a dove può arrivare?
  - Qualifica del servizio di DPO quando è esternalizzato: esternalizzazione semplice o FEI?
  - La relazione del DPO al Consiglio di Amministrazione
  - Il ruolo del DPO nell'AI
- **Esercitazione guidata: la gestione delle richieste dell'Autorità di controllo**
- **Gli strumenti di accountability**
  - Il sistema documentale data protection previsto dal Regolamento Europeo
  - Il registro dei trattamenti: obiettivi e funzione
  - I documenti di attestazione
  - Le liste dei soggetti al trattamento dei dati
  - I documenti digitali: tra CAD e GDPR
- **Esercitazione guidata: la protezione dei dati sin dalla progettazione di un prodotto bancario**

Seconda giornata • 8 maggio 2025 (10.00-16.00)

- **La gestione dei data breach**
  - Data breach, incidenti di sicurezza e gravi incidenti di sicurezza: tra GDPR, DORA e PSD3
  - La violazione dei dati personali: significato ed individuazione
  - La raccolta delle informazioni: rapporti tra DPO, strutture interne e responsabili esterni
  - Analisi della violazione e contromisure
  - La valutazione sulla notifica agli interessati
  - La comunicazione agli interessati
  - Gestione di una procedura di comunicazione interna ed esterna: tra GDPR e DORA
  - Analisi dei recenti provvedimenti del Garante
- **Esercitazione guidata: simulazione di una violazione dei dati personali**
- **La valutazione di impatto sulla protezione dei dati (DPIA)**
  - La Valutazione di Impatto sulla protezione dei dati: approfondimenti delle Autorità
  - Le linee guida del Working Party art. 29 sulla conduzione della DPIA: presupposti e metodologie
  - La ISO/IEC 29134:2017
- **Esercitazione guidata: la conduzione di una data protection impact analysis**

Terza giornata • 9 maggio 2025 (10.00-16.00)

- **Quadro di sorveglianza e di vigilanza nazionale ed europea**
  - Cooperazione internazionale delle autorità di controllo
  - Compiti e poteri delle autorità di controllo
  - Meccanismi di individuazione dell'autorità capofila
  - Cooperazione tra l'autorità capofila e le autorità di controllo interessate
  - Operazioni congiunte
- **Il sistema e il procedimento sanzionatorio**
  - Strumenti di tutela dell'interessato
  - Le sanzioni amministrative nel GDPR
  - Responsabilità civile da illecito trattamento di dati personali e profili giurisprudenziali
  - Condizioni generali che l'Autorità deve applicare nell'irrogazione delle sanzioni pecuniarie: art. 83 GDPR, quantificazione e pluralità di violazioni.
  - Procedimento sanzionatorio: disamina di un caso concreto

3° MODULO
IT, SICUREZZA E PROTEZIONE DATI
21, 22 e 23 maggio 2025

Prima giornata • 21 maggio 2025 (10.00-16.00)

- **I principali canali per l'accesso ai servizi della banca da parte della clientela**
  - L'accesso all'home banking e corporate banking: i dati sensibili e loro trattamento
  - ATM (Automatic Teller Machine) e POS (Point of Sales)
  - Tecniche di Strong Authentication: Direttiva PSD2, Regolamento eIDAS ed indicazioni della Banca d'Italia
  - Digital marketing e privacy compliance: nuovi servizi per la fidelizzazione e profilazione della clientela
  - Privacy tra omnicanalità e scoring dei clienti con i big data
- **La tutela della sicurezza dei dati dei clienti nel Provvedimento 192/2011 del Garante sulla tracciabilità delle operazioni**
  - Tracciabilità delle operazioni bancarie: misure e regole da rispettare
  - I recenti provvedimenti del Garante tra Data breach e Tracciabilità
  - Analisi di casi pratici
- **Analisi dei rischi e minacce nel trattamento dei dati**
  - Analisi delle minacce e delle vulnerabilità che insistono sugli asset delle informazioni e dei dati aziendali, il cyber risk
  - Analisi dei rischi per la sicurezza dei dati
  - Pianificazione delle misure di rimedio
  - Monitoraggio e controllo dei fornitori
- **Strumenti per la sicurezza informatica**
  - Strumenti per la protezione di infrastrutture
  - Anonimizzazione: tecniche di randomizzazione e generalizzazione
  - Pseudonimizzazione: tecniche di crittografia, di hashing di tokenizzazione
- **Ruolo, compiti e responsabilità degli amministratori di sistema**
  - Provvedimento del Garante del 27/11/2008
  - Definizione dell'amministratore di sistema
  - Requisiti per la nomina
  - Misure di sicurezza e controllo
- **L'amministratore di sistema le misure di sicurezza previste dalla Circolare 192/2011**
  - Sistemi di log
  - Sistemi di alert
  - Audit IT e controlli interni

Seconda giornata • 22 maggio 2025 (10.00-16.00)

▸ L'evoluzione delle normative in tema di privacy e sicurezza informatica

- L'evoluzione della sicurezza informatica nella normativa italiana ed europea
- Misure di sicurezza, cybersecurity e standard internazionali: dal GDPR al DORA
- Il DORA e gli impatti sulla protezione dei dati personali
- Integrità, disponibilità e riservatezza: i principi cardine della sicurezza informatica
- Il nuovo approccio della cybersecurity: analisi dei rischi, Linee guida ENISA e le indicazioni del DORA
- Il rischio ICT come rischio operativo: le previsioni di Banca d'Italia

▸ Misure tecnico-organizzative per la sicurezza dei dati

- Misure organizzative e tecniche di custodia e controllo dei dati
- Sistemi di autenticazione ed autorizzazione informatica
- Tracciamento e controlli degli accessi ed operazioni

▸ Esercitazione guidata

- L'individuazione del posizionamento dei trattamenti all'interno dell'architettura ICT della banca
- Le domande da porre alla funzione IT per ricavare le informazioni necessarie sulla mappatura dei trattamenti
- L'individuazione delle aree a maggior rischio per la tutela degli interessati

Terza giornata • 23 maggio 2025 (10.00-16.00)

▸ Ispezioni e controlli in ambito sicurezza e privacy

- Strategie di audit e verifica: il piano nazionale delle ispezioni e il monitoraggio della conformità
- Processo di ispezione e poteri delle autorità
- Il ruolo del Garante nella sicurezza dei dati
- Input e fattori scatenanti delle attività ispettive

▸ Come prepararsi ad una attività ispettiva

- Documentazione essenziale da esibire durante una attività ispettiva
- Le ispezioni tecniche: i punti di maggiore interesse in sede di ispezione
- Istruttoria a seguito di una attività ispettiva e avvio procedimento sanzionatorio

▸ Esercitazione guidata: la gestione delle fasi dell'ispezione

- Modalità di preavviso
- Ruolo e attività del pool ispettivo e del team della banca nell'ispezione
- Acquisizione della documentazione e accesso alle banche dati