

Percorso professionalizzante

## PRIVACY EXPERT E DATA PROTECTION OFFICER IN BANCA

1° MODULO • 14, 15 e 16 ottobre 2026

2° MODULO • 4, 5 e 6 novembre 2026

3° MODULO • 25, 26 e 27 novembre 2026

TEST FINALE • 4 dicembre 2026

Aula virtuale

### 1° MODULO

## PRINCIPI E REGOLE DELLA PRIVACY IN BANCA

14, 15 e 16 ottobre

Prima giornata • 14 ottobre (10.00-16.00)

#### ► Il quadro regolatorio per la privacy in banca: una visione di insieme

- Digital Omnibus: novità, impatti e coordinamento con le altre normative europee
- La normativa privacy e le interconnessioni con le recenti novità introdotte da eIDAS 2.0, AI ACT, DORA e PSD3
- I Provvedimenti del EDPB più rilevanti 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, dei dati particolari e dei dati giudiziari
- Privacy by design e by default: esempi di progetto

#### ► Il GDPR ed i diritti degli interessati

- I diritti degli interessati nel nuovo assetto normativo
- Controllo sui dati alla luce del Data ACT
- Cancellazione e oblio: criticità e sfide

#### ► 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 bancaria
- Coordinamento di ruoli con le altre normative europee
- Il DPO della banca: differenze tra banche di piccole/medie dimensioni e di grandi dimensioni



## Seconda giornata • 15 ottobre (10.00-16.00)

---

### ► Il Responsabile del trattamento

- Ruolo e Responsabilità
- Il monitoraggio sull'intera catena di fornitori 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
- La possibile standardizzazione del Data Processing Agreement

### ► 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 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 del EDPB
- Attività di recupero credito e di cessione di crediti: regole e limiti

### ► 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, la durata e l'aggiornamento dei consensi
- La disciplina dei cookie e il graduale superamento degli stessi tramite altri strumenti di tracciamento
- La Privacy Impact Assessment
- La disciplina del telemarketing ed il Codice di Condotta

### ► Esercitazione guidata

## Terza giornata • 16 ottobre (10.00-16.00)

---

### ► La disciplina 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
- Il Digital Omnibus e le semplificazioni del GDPR e AI Act
- Il Regolamento Europeo sull'Intelligenza Artificiale
- Il Data Act
- Evoluzione dell'identità digitale: le modifiche al Regolamento eIDAS ed il superamento di SPID
- Il MiCAR sulle crypto-attività e gli aspetti privacy
- L'evoluzione verso l'open finance: 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: Antiriciclaggio e privacy: punti di contatto

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



## 2° MODULO

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

4, 5 e 6 novembre

Prima giornata • 4 novembre (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: IT, Security, Risorse Umane, Responsabile della Conservazione e Revisori Contabili
- 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: semplificazioni e armonizzazione normativa

### ► Esercitazione guidata: la gestione delle richieste dell'Autorità di controllo

### ► Gli strumenti di accountability

- Il sistema documentale data protection previsto dal Regolamento Europeo nel contesto del GDPR
- Il registro dei trattamenti del titolare: obiettivi e funzione
- Il registro dei trattamenti del responsabile: obiettivi e funzione

### ► Esercitazione guidata: la protezione dei dati sin dalla progettazione di un prodotto bancario

Seconda giornata • 5 novembre (10.00-16.00)

### ► La gestione dei data breach

- Data breach, incidenti di sicurezza e gravi incidenti di sicurezza tra GDPR, DORA e NIS2
- Data breach alla luce del single entry point
- 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, DORA e NIS2
- 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 • 6 novembre (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**

25, 26 e 27 novembre

## Prima giornata • 25 novembre (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 del Garante sulla tracciabilità delle operazioni**

- Tracciabilità delle operazioni bancarie: misure e regole da rispettare
- I recenti provvedimenti del Garante
- 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 e il ruolo dell'information security officer**

- Le misure di sicurezza previste dal provvedimento sulla tracciabilità delle informazioni bancarie
- Sistemi di log
- Sistemi di alert
- Audit IT e controlli interni



## Seconda giornata • 26 novembre (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 • 27 novembre 2026 (10.00-16.00)

---

### ► **Ispezioni e controlli in ambito sicurezza e privacy**

- 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

### ► **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