Percorso professionalizzante

# PRIVACY EXPERT E DATA PROTECTION OFFICER IN BANCA 2024 - 2° Edizione

1° MODULO • **16, 17 e 18 ottobre 2024**
2° MODULO • **6, 7 e 8 novembre 2024**
3° MODULO • **26, 27 e 28 novembre 2024**
TEST FINALE • **9 dicembre 2024**

**Aula virtuale**

## 1° MODULO
## PRINCIPI E REGOLE DELLA NUOVA PRIVACY
16, 17 e 18 ottobre 2024

### Prima giornata • 16 ottobre 2024 (10.30-16.30)

- **Linee guida del percorso professionalizzante**

- **General Data Protection Regulation (GDPR), Codice privacy, Legge 675/1996 e Direttiva 46/95 : gli snodi chiave della disciplina sulla privacy in banca**
  - La direttiva sulla protezione dei dati personali 46/1995.
  - L'evoluzione normativa che ha portato al Regolamento europeo 679/2016. Differenze tra regolamento e direttiva
  - Discipline nazionali sulla privacy precedenti. Legge 675/1996 e Codice Privacy
  - Il decreto 101/2018 come completa la normativa italiana
  - L'European Data Protection Board o Comitato europeo per la protezione dei dati
  - Ambito di applicazione e definizioni del GDPR
  - Il trasferimento di dati all'estero: il nuovo 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
  - Trasparenza sulle informazioni
  - Limitazione della conservazione e sua comunicazione
  - Accountability, analisi dei rischi e approccio sistematico alla privacy
  - Privacy by design e by default
  - L'applicazione del GPDR nei provvedimenti del Garante: lesson learned

- **I principali soggetti della disciplina privacy**
  - Il titolare, il contitolare, i soggetti designati
  - La definizione dei ruoli in base al principio della Accountability
  - Le designazioni: come farle e conseguenze sui contenuti
  - Atto giuridico di Contitolarità
  - Le Istruzioni ai soggetti designati. Differenze giuridiche sulla responsabilità
  - Il DPO della banca

- **Il GDPR ed i diritti degli interessati**
  - Presupposti di liceità del trattamento
  - Dati particolari e dati giudiziari (penali)
  - Informative agli interessati
  - Diritto di accesso ai dati personali
  - Limitazione del trattamento
  - Diritto alla cancellazione ed oblio
  - Portabilità dei dati

## Seconda giornata • 17 ottobre 2024 (10.00-16.00)

- **Il rapporto con i Responsabili del trattamento**
  - I fornitori di servizi: tra esternalizzazione e protezione dei dati personali
  - Il contenuto del Data Processing Agreement
  - Il monitoraggio sui responsabili del trattamento: tra GDPR e DORA
  - La ripartizione di responsabilità
- **Le informative e i consensi ai sensi del GDPR e delle indicazioni dell'EDPB. Analisi dei provvedimenti della Corte di Giustizia UE e del Garante per la protezione dei dati personali**
- **Il Registro dei trattamenti: come elaborarlo e come aggiornarlo**
- **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
  - I dati del whistleblowing
  - I dati dell'antiriciclaggio ed i provvedimenti del Garante in materia di privacy
  - Esternalizzazione di servizi anche alla luce degli orientamenti EBA e della Circolare Banca d'Italia e Regolamento DORA
  - 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**
  - L'attribuzione delle responsabilità in materia di trattamento dei dati personali in banca e la formazione del personale che partecipa ai trattamenti
  - Raccolta e utilizzo dei dati dei clienti
  - Il consenso al trattamento dei dati
  - Trattamento di dati giudiziari
  - Trattamento dei dati per il collocamento di prodotti di terzi
  - Le principali banche dati pubbliche e private di interesse in ambito bancario
  - Il codice di condotta in materia di informazioni commerciali
  - Il credit scoring secondo la Corte di Giustizia Europea

## Terza giornata • 18 ottobre 2024 (10.00-16.00)

### ▸ Trattamento dei dati a fini marketing, gestione dei cookie e legal design

### ▸ Trattamento dei dati personali a fini di marketing

- Il trattamento dei dati personali a fini di marketing ed il GDPR
- Marketing diretto, profilazione e legittimo interesse
- La disciplina dei cookie e il graduale superamento degli stessi tramite altri strumenti di tracciamento
- Profilazione per finalità di marketing e Privacy Impact Assesment
- La nuova disciplina del telemarketing ed il codice di Condotta

### ▸ Esercitazione guidata: Svolgimento del test di prevalenza per la valutazione del bilanciamento nell'applicazione del legittimo interesse

### ▸ Intelligenza artificiale e protezione dei dati personali

- La regolamentazione dei sistemi di intelligenza artificiale nell'AI Act
- 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

### ▸ Le regole della videosorveglianza

- Le linee guida dell'European Data Protection Board in materia di videosorveglianza
- Videosorveglianza e Data Protection Impact Assessment
- I rapporti tra videosorveglianza e controlli sui lavoratori: la circolare n. 5/2018 dell'Ispettorato Nazionale Lavoro e le successive evoluzioni
- L'intervento del Garante italiano
- Sanzioni e rimedi: analisi delle principali sanzioni in materia di videosorveglianza applicate in Europa

2° MODULO

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

6, 7 e 8 novembre 2024

## Prima giornata • 6 novembre 2024 (10.30-16.30)

### ▸ Identikit del Data Protection Officer in banca

- Designazione del DPO: criteri ed indicazioni dell'EDPB e del Garante
- Requisiti personali e professionali, formazione continua
- Verifica di possibili conflitti di interesse e/o incompatibilità
- Posizionamento organizzativo e ufficio di supporto: rapporto con privacy expert
- Autonomia ed indipendenza del DPO
- Compiti consultivi e di controllo del DPO
- Responsabilità del DPO
- Il DPO in un gruppo bancario e l'ipotesi di esternalizzazione
- La certificazione professionale
- Primi orientamenti giurisprudenziali sulla figura del DPO

### ▸ I rapporti del DPO con le diverse funzioni della banca e con il Garante per la protezione dei dati personali

- 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 di controllo, la consultazione di propria iniziativa e la cooperazione su richiesta
- L'attività di informazione, consulenza e indirizzo nei confronti del titolare o responsabile del trattamento
- I rapporti con le diverse funzioni della banca: Board, Revisori, IA, IT, Security, Risorse Umane
- Documentazioni e flussi informativi

### ▸ Esercitazione guidata: la gestione delle ispezioni e delle richieste dell'Autorità di controllo

### ▸ Il piano di implementazione «protezione dei dati personali» per la gestione del GDPR

- Gli strumenti per attuare l'implementazione del GDPR e per la conformità su misura
- Analisi e mappatura dei processi in banca
- La privacy by design e by default in pratica. La nuova ISO 31700-1:2023
- Esempi di policy interna per l'implementazione del GDPR
- Privacy by design: un principio «grimaldello» nei provvedimenti del Garante
- Protezione dei dati personali e gestione della crisi

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

## Seconda giornata • 7 novembre 2024 (10.00-16.00)

- **Il sistema documentale data protection previsto dal nuovo Regolamento Europeo**
  - Il sistema documentale come strumento di accountability
  - I registri
  - I documenti di attestazione
  - Le liste dei soggetti al trattamento dei dati
  - Audit report e verifiche compliance in ambito privacy
- **La gestione dei data breach**
  - 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 circa la notifica agli interessati
  - Data breach, Regolamento DORA e rapporti con la Banca d'Italia
  - Analisi dei provvedimenti del Garante
- **Esercitazione guidata: la gestione di un data breach dalla raccolta delle informazioni alla notifica all'Autorità di controllo**
- **L'approccio basato sul rischio per la data protection: aspetti organizzativi e procedurali**
  - Risk data protection: determinazione, valutazione e approccio risk based
  - Individuazione delle aree bancarie ad alto rischio
  - Analisi dei trattamenti di dati personali della banca
  - Aree da sottoporre ad audit
  - Strumenti di monitoraggio e reporting
- **Esercitazione guidata: il Risk Assessment data protection**

## Terza giornata • 8 novembre 2024 (10.00-16.00)

- **La valutazione di impatto sulla protezione dei dati (DPIA)**
  - Le novità sulla Valutazione di Impatto: elenchi e approfondimenti delle Autorità
  - La data protection impact analysis (DPIA) per acquisire una visione chiara e completa dei trattamenti dei dati personali e garantire la conformità ai principi del GDPR
  - Le linee guida del Working Party art. 29 sulla conduzione della DPIA: presupposti e metodologie
  - La ISO/IEC 29134:2017
  - Come condurre una DPIA e strumenti operativi a supporto
- **Esercitazione guidata: la conduzione di una data protection impact analysis**
- **Il sistema sanzionatorio**
  - Le sanzioni amministrative nel GDPR
  - Condizioni generali che l'Autorità deve applicare nell'irrogazione delle sanzioni pecuniarie: art. 83 GDPR, quantificazione e pluralità di violazioni. I rapporti tra ordinamento europeo e diritto interno
  - Responsabilità civile da illecito trattamento di dati personali e profili giurisprudenziali
- **Esercitazione guidata – La gradazione delle sanzioni amministrative**

3° MODULO
# IT, SICUREZZA E PROTEZIONE DATI
26, 27 e 28 novembre 2024

## Prima giornata • 26 novembre 2024 (10.30-16.30)

### ▸ Protezione dei dati personali e le attività di marketing della banca
- Digital marketing e privacy compliance: nuovi servizi per la fidelizzazione e profilazione della clientela
- Privacy e gestione dei cookie
- Privacy tra omnicanalità e scoring dei clienti con i big data

### ▸ 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

### ▸ L'impatto per le banche della politica legislativa europea sul digitale
- La resilienza operativa tecnologica ed il DORA: le specifiche misure di sicurezza per le banche
- Evoluzione dell'identità digitale: le modifiche al Regolamento eIDAS ed il superamento di SPID
- L'AI Act: requisiti e adempimenti per l'utilizzo dei sistemi di intelligenza artificiale in banca
- Il Regolamento MiCA sulle cripto-attività, l'Euro digitale e gli aspetti privacy
- Interventi delle autorità e proposte regolatorie sulle tecnologie emergenti. Un quadro di insieme sulla strategia digitale della UE (AI Act, Data Governance Act, Data Act, MiCA, DMA, DSA, DORA)

### ▸ Analisi dei rischi sul trattamento dei dati: dal GDPR al DORA
- 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
- Le principali previsioni del DORA per la resilienza dei sistemi bancari. Monitoraggio e controllo dei fornitori

### ▸ Strumenti per la sicurezza
- Strumenti per la protezione di infrastrutture
- Anonimizzazione: tecniche di randomizzazione e generalizzazione
- Pseudonimizzazione: tecniche di crittografia, di hashing di tokenizzazione

## Seconda giornata • 27 novembre 2024 (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 previsioni del DORA
- Il rischio ICT come rischio operativo: le previsioni di Banca d'Italia
- Sicurezza informatica ed esternalizzazione di funzioni: adempimenti e controlli nel DORA

### ▸ Le misure di sicurezza in banca alla luce dell'emergenza
- Protezione dello smart-working
- Continuità delle funzioni critiche di Cybersecurity e di Business
- Contrastare minacce opportunistiche rispetto al nuovo scenario di smart-working e digitalizzazione dei servizi

### ▸ 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

### ▸ Data protection e data governance

### ▸ Esercitazione guidata:
- L'individuazione del posizionamento dei trattamenti all'interno dell'architettura ICT della banca
- Quali domande 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 • 28 novembre 2024 (10.00-16.00)

### ▸ Le ispezioni in ambito privacy
- Piano nazionale delle ispezioni
- Le fasi delle ispezioni ed i poteri delle autorità di controllo
- Attività del Garante, competenza, compiti, poteri e meccanismi di cooperazione e coerenza
- Poteri Ispettivi dell'Autorità (art. 58 GDPR)
- Operazioni congiunte delle Autorità di controllo
- Input delle attività ispettive

### ▸ Come prepararsi ad una attività ispettiva
- Documentazione essenziale da esibire durante una attività ispettiva
- Istruttoria a seguito di una attività ispettiva e avvio procedimento sanzionatorio

### ▸ Esercitazione guidata – La gestione delle fasi dell'ispezione