

Percorso Professionalizzante

PRIVACY EXPERT E DATA PROTECTION OFFICER IN BANCA – 1^a Edizione

1° MODULO • 12, 13, 14 aprile 2023

2° MODULO • 3, 4, 5 maggio 2023

3° MODULO • 23, 24, 25 maggio 2023

TEST FINALE • 7 giugno 2023

Aula virtuale

1° MODULO

PRINCIPI E REGOLE DELLA NUOVA PRIVACY

12, 13, 14 aprile 2023

Prima giornata • 12 aprile 2023 (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 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 GDPR e il rafforzamento dei principi relativi al trattamento dei dati

- Liceità del trattamento, limitazione delle finalità, proporzionalità, 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 GDR nel 2020: 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 • 13 aprile 2023 (10.00-16.30)

► **Il rapporto con i Responsabile 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
- 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
- Esternalizzazione di servizi anche alla luce degli orientamenti EBA e della circolare Banca d'Italia
- 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



Terza giornata • 14 aprile 2023 (10.30-16.30)

- ▶ **La Direttiva 2002/58/CE (cosiddetta “Direttiva ePrivacy”) e la Proposta di regolamento E-privacy sulle comunicazioni Elettroniche**
- ▶ **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
 - Profilazione per finalità di marketing e Privacy Impact Assessment
 - La nuova disciplina del telemarketing
- ▶ **Esercitazione guidata: svolgimento del test di prevalenza per la valutazione del bilanciamento nell'applicazione del legittimo interesse**
- ▶ **La trasparenza del trattamento ed il legal design**
 - La trasparenza come nuovo principio base della tutela dei dati personali: dalla trasparenza bancaria alla trasparenza «trasversale»
 - Le pronunce in materia di trasparenza: trasversalità dei provvedimenti tra Autorità antitrust e Garante
 - Le linee guida CNIL sulla trasparenza e le Linee Guida WP29 del 11/4/2018. Gli interventi del Garante italiano
 - Informative online, dark patterns e trasparenza: i principi del legal design
- ▶ **Esercitazione guidata: analisi e redazione di un'informativa semplificata in conformità al principio di trasparenza ed al legal design**
- ▶ **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
 - L'intervento del Garante italiano
 - Sanzioni e rimedi



2° MODULO

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

3, 4, 5 maggio 2023

Prima giornata • 3 maggio 2023 (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 • 4 maggio 2023 (10.00-16.30)

► **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 e direttiva NIS e NIS2 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 • 5 maggio 2023 (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

► **Esercitazione guidata: la gradazione delle sanzioni amministrative**



3° MODULO

IT, SICUREZZA E PROTEZIONE DEI DATI

23, 24, 25 maggio 2023

Prima giornata • 23 maggio 2023 (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'utilizzo delle nuove tecnologie in banca e i principi per il trattamento dei dati

- Cloud computing e rapporto con i fornitori.
- L'identità digitale: dallo SPID all'European Identity Wallet. L'evoluzione del Regolamento eIDAS.
- Fintech e PSD2: l'evoluzione del sistema dei pagamenti.
- Blockchain, registri distribuiti e Smart contract. Impatti nell'attività bancaria e profili di privacy.
- Intelligenza artificiale, dati e algoritmi. La AI per il Fintech. Indicazioni EBA, l'AI Act e i profili applicativi
- Interventi delle autorità e proposte regolatorie sulle tecnologie emergenti. Un quadro di insieme sulla strategia digitale della UE

► 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 • 24 maggio 2023 (10.30-16.00)

► **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 alla Direttiva NIS e NIS2
- 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 e Linee guida ENISA
- Il rischio ICT come rischio operativo: le previsioni di Banca d'Italia
- Sicurezza informatica ed esternalizzazione di funzioni: le indicazioni delle Linee guida EBA

► **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 • 25 maggio 2023 (10.30-16.30)

► **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**