Percorso professionalizzante

PRIVACY EXPERT E DATA PROTECTION OFFICER IN BANCA 2020

PRIMO MODULO • **13, 14 e 15 ottobre 2020**
SECONDO MODULO • **4, 5 e 6 novembre 2020**
TERZO MODULO • **18, 19 e 20 novembre 2020**
TEST FINALE • **30 novembre 2020**

ABISERVIZI ABI FORMAZIONE

Percorso professionalizzante

PRIVACY EXPERT E DATA PROTECTION OFFICER IN BANCA 2020

PRIMO MODULO • **13, 14 e 15 ottobre 2020**
SECONDO MODULO • **4, 5 e 6 novembre 2020**
TERZO MODULO • **18, 19 e 20 novembre 2020**
TEST FINALE • **30 novembre 2020**

PRIMO MODULO • **PRINCIPI E REGOLE DELLA NUOVA PRIVACY**

13 OTTOBRE 2020

- **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, 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 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 e 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 e oblio
  - Portabilità dei dati

PRIMO MODULO • PRINCIPI E REGOLE DELLA NUOVA PRIVACY

14 OTTOBRE 2020

- **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
  - 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

15 OTTOBRE 2020

- **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 e il GDPR
  - Marketing diretto, profilazione e legittimo interesse
  - Profilazione per finalità di marketing e Privacy Impact Assesment
  - 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 e il legal design**
  - La trasparenza come nuovo principio base della tutela dei dati personali
  - 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
  - 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 e 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
  - Sanzioni e rimedi

SECONDO MODULO • REQUISITI, COMPITI E ATTIVITÀ DEL DPO E DEL PRIVACY EXPERT IN BANCA

4 NOVEMBRE 2020

- **Identikit del Data Protection Officer in banca**
  - Criteri per la designazione del DPO: le indicazioni del Garante
  - Posizionamento organizzativo, requisiti personali e professionali, formazione continua
  - Doveri, poteri, responsabilità e verifica di possibili conflitti di interesse e/o incompatibilità
  - L'indipendenza del DPO
  - Compiti consultivi e di controllo del DPO
  - Il DPO in un gruppo bancario e l'ipotesi di esternalizzazione
  - La certificazione professionale
  - Le posizioni 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 l'autorità di controllo, la consultazione di propria iniziativa e la cooperazione su richiesta
  - I rapporti con le diverse funzioni della banca: Board, IT, Security, Risorse Umane
  - L'attività di informazione, consulenza e indirizzo nei confronti del titolare o responsabile del trattamento
  - L'attività di supervisione delle "figure privacy" interne alla banca
  - 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
  - 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. Il trattamento dei dati all'epoca del Covid-19

Esercitazione guidata – La protezione dei dati sin dalla progettazione di un prodotto bancario

5 NOVEMBRE 2020

- **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 e 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
  - Analisi dei provvedimenti del Garante

Esercitazione guidata – La gestione di un data breach dalla raccolta delle informazioni alla notifica all'Autorità di controllo

SECONDO MODULO • REQUISITI, COMPITI E ATTIVITÀ DEL DPO E DEL PRIVACY EXPERT IN BANCA

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

6 NOVEMBRE 2020

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

TERZO MODULO • IT, SICUREZZA, PROTEZIONE DEI DATI E ISPEZIONI

18 NOVEMBRE 2020

- **Protezione dei dati personali e le attività di marketing della banca**
  - Digital marketing e privacy compliace: nuovi servizi per la fidelizzazione e profilazione della clientela
  - 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 e indicazioni della Banca d'Italia
- **L'utilizzo delle nuove tecnologie in banca e i principi per il trattamento dei dati**
  - Cloud computing
  - Smart contract
  - L'identità digitale
  - Big data privacy
  - Blockchain e registri distribuiti
  - Intelligenza artificiale, dati e algoritmi
  - Privacy by design: le Linee guida EDPB e l'applicazione alle nuove tecnologie
- **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

19 NOVEMBRE 2020

- **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
  - Integrità, disponibilità e riservatezza: i principi cardine della sicurezza informatica
  - Il nuovo approccio della cybersecurity: analisi dei rischi e Linee guida ENISA
  - 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 e autorizzazione informatica
  - Tracciamento e controlli degli accessi e operazioni
- **Analisi dei rischi sul trattamento dei dati**
  - Analisi delle minacce e delle vulnerabilità che insistono sugli asset delle informazioni e dei dati aziendali
  - Analisi dei rischi per la sicurezza dei dati
  - Pianificazione delle misure di rimedio
- **Strumenti per la sicurezza**
  - Strumenti per la protezione di infrastrutture
  - Anonimizzazione: tecniche di randomizzazione e generalizzazione
  - Pseudonimizzazione: tecniche di crittografia, di hashing di tokenizzazione

TERZO MODULO • IT, SICUREZZA, PROTEZIONE DEI DATI E ISPEZIONI

20 NOVEMBRE 2020

- **Le ispezioni in ambito privacy**
  - Piano nazionale delle ispezioni
  - Le fasi delle ispezioni e 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 a un'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

A conclusione del Percorso è previsto un **test finale di verifica** delle conoscenze acquisite.

OBIETTIVI

I percorso trasferisce conoscenze utili a:

- individuare gli elementi significativi nell'evoluzione della normativa privacy in ambito nazionale e comunitario, nonché gli impatti sull'operatività bancaria
- garantire la conservazione della documentazione che il titolare del trattamento deve tenere a disposizione dell'autorità di controllo e consegnare in caso di richiesta
- conoscere i sistemi informativi della banca, identificare gli strumenti per l'attuazione delle misure di sicurezza dei dati personali
- individuare le attività da svolgere in caso di ispezione attraverso l'analisi delle procedure previste dalla normativa privacy, dei regolamenti del Garante e dalle best practices comunemente adottate

MODALITÀ DI EROGAZIONE

Ciascun modulo si svolgerà in **aula virtuale**, attraverso una piattaforma dedicata che consente interazione tra docenti e partecipanti. In relazione all'evoluzione dell'emergenza sanitaria in corso, alcune giornate potrebbero tenersi nelle sedi di Roma/Milano e in diretta streaming per coloro che volessero seguirle a distanza.