Deloitte.

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

# La modifica della certificazione dei DPO

**Community Privacy e DPO Unindustria**

**25 novembre 2025**

# Le competenze chiave del DPO

**Per supportare efficacemente le Organizzazioni**, il Data Protection Officer (**DPO**) dovrebbe possedere **competenze multidisciplinari**:

## *Conoscenza del contesto dell'organizzazione*

Il DPO deve essere un **partner strategico per il business**, partendo da una profonda conoscenza degli **obiettivi aziendali**, delle **iniziative** e dell'**ecosistema delle terze parti** coinvolte. Questa **visione olistica** permette di trasformare la compliance da obbligo normativo a leva di **vantaggio competitivo**.

## *Formazione specifica*

Il ruolo del DPO richiede un **perimetro di competenze** che non si ferma al **GDPR** ma integra **standard** e ***best practice*** (es. ISO), **normative di settore** come NIS 2 e DORA, i nuovi **framework europei** sui dati (es. AI Act, Data Act, Data Governance Act), senza trascurare le componenti **legali e giuslavoristiche** connesse alla gestione dei dati personali.

## *Conoscenza dei sistemi di controllo*

Il DPO deve padroneggiare **metodi, sistemi e framework di controllo**, comprendendo **processi, indicatori e strumenti di monitoraggio** per assicurare l'efficacia delle misure organizzative e tecniche lungo l'intero ciclo di vita dei dati.

## *Expertise tecnologica*

Il DPO deve conoscere le **tecnologie** coinvolte nel trattamento dei dati — sistemi **informativi**, **cloud, analytics**, **IA** e sicurezza — per identificare **rischi e minacce** e garantire **presidi e controlli** efficaci.

## *Soft Skills*

Il DPO deve possedere naturale **empatia, capacità di connessione e comunicazione**, per interagire e collaborare con tutti gli ***stakeholder*** e fungere da **punto di contatto** sia per le Autorità sia per gli interessati, garantendo un **dialogo chiaro ed efficace**.

# Introduzione alla certificazione dei DPO

**Il GDPR non richiede una certificazione abilitante**, ma impone che il DPO nominato possieda una "***conoscenza specialistica*** *della normativa e delle prassi in materia di protezione dei dati*" (art. 37 par. 5).
In questo contesto, le certificazioni professionali rappresentano uno **strumento volontario di *accountability*** per attestare **competenze del DPO** secondo **standard tecnici** riconosciuti.

## Enti di normazione

***Ente Italiano di Normazione***
elabora e pubblica norme tecniche valide in Italia.

***Comitato Elettrotecnico Italiano***
definisce standard nel settore elettrico, elettronico e ICT.

***Comité Européen de Normalisation***
organismo di Normazione Europea di cui fa parte anche l'Italia


Le **certificazioni** garantiscono il riconoscimento ufficiale delle **competenze e dei requisiti professionali** delle figure che operano nella **privacy e protezione dei dati personali.**
Tra i ruoli certificabili vi è anche il **Data Protection Officer.**

**2017**

### UNI 11697:2017

La norma UNI 11697:2017 - con le relative **Linee Guida operative UNI PdR 66:2019** - ha rappresentato il principale riferimento **nazionale** per la certificazione del **DPO**, definendo in modo chiaro i **requisiti di conoscenza, abilità e competenza** richiesti per svolgere correttamente il ruolo secondo il **GDPR.**

**2024**

### UNI CEI EN 17740:2024

Recepisce lo **standard europeo emesso dal CEN nel 2023,** a sostituzione della UNI 11697:2017, innovando i criteri per la **valutazione e certificazione delle competenze del DPO** e garantendo **uno standard armonizzato europeo.**

*Linee Guida Operative:* **UNI/TS 11945:2024**

Fornisce le **linee guida operative** per applicare la UNI CEI EN 17740 nei processi di **certificazione dei soggetti della privacy**, assicurando **uniformità e chiarezza delle procedure**.

# Evoluzione della certificazione DPO

2017

## UNI 11697:2017

*« Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza»*

### AMBITO E APPROCCIO

La norma è applicabile solo a **livello nazionale.**
Sono definiti **4 profili professionali** per la protezione dei dati personali, tra cui è incluso **il DPO.**

### STRUTTURA COMPETENZE

Modello di competenza basato sull'approccio **EQF** European Qualification Framework, **quadro europeo generale** che classifica le **qualifiche professionali** in **8 livelli.**
La norma prevede requisiti di:

- **esperienza professionale specifica** (es. Laurea Magistrale in discipline inerenti, seniority di 4 anni in data protection, di cui 3 in posizioni manageriali) e **80 ore di formazione specifica** in data protection;
- aree di **Competenza** (es. gestione del rischio), **conoscenze (Knowledge)** necessarie, comprese normative e tecniche di sicurezza dei dati, nonché le **abilità (Skills) del DPO** (es. pianificazione, gestione dei processi).

### VERIFICA E CERTIFICAZIONE

Superamento della valutazione dei **titoli**, due **prove scritte** (di cui una su casi-studio pratici) e una **prova orale**.
La certificazione ha durata **quadriennale** e richiede un **aggiornamento formativo** continuo per il mantenimento.

Da un ruolo nazionale ad un DPO con **competenze armonizzate** e riconosciute **in tutta l'Europa**

2024

## UNI CEI EN 17740:2024

*«Requisiti per i profili professionali relativi al trattamento e protezione dei dati personali»*

### AMBITO E APPROCCIO

**Framework europeo** per i requisiti professionali relativi specificatamente ai **ruoli della data protection,** garantisce **l'armonizzazione dei ruoli e delle competenze.**
**Sono definiti 5 profili professionali** tra cui il **DPO.**

### STRUTTURA COMPETENZE

Rispetto allo standard nazionale, si è operata una **ottimizzazione delle competenze** assegnate e dei livelli richiesti, allineandoli agli **standard europei per i ruoli professionali ICT** (rif. e-CF EN 16234-1).
**Recepisce i requisiti** di seniority, formazione specifica, Conoscenza (Knowledge), di Abilità (Skills) e Competenza della **UNI nazionale, tenendo conto delle evoluzioni normative e delle più recenti best practice** in campo di protezione dei dati personali.

### VERIFICA E CERTIFICAZIONE

**Recepisce interamente** le modalità di conseguimento, durata (4 anni) e mantenimento **della UNI nazionale** pur **assumendo un carattere europeo.**

*Entro il 30.04.2025 le certificazioni UNI nazionali devono migrare al nuovo standard Europeo per mantenere la validità*

# Le certificazioni per la protezione dei dati

L'***International Association of Privacy Professionals*** **(IAPP)** certifica le competenze in materia **privacy**, offrendo percorsi che costituiscono uno **standard internazionale** per la conoscenza normativa della **protezione dei dati personali**, declinata secondo aree geografiche e sistemi legislativi.

## CIPP – *Certified Information Privacy Professional*

**La Certificazione CIPP** si rivolge ai professionisti che operano in ambito **privacy**, attestando le competenze necessarie per interpretare e applicare leggi, regolamenti e standard di **protezione dei dati** nel proprio contesto giurisdizionale.

**La CIPP/E** certifica le conoscenze sul **GDPR, sulle istituzioni europee e sul quadro normativo UE,** attestando le competenze necessarie per i professionisti della data protection operanti nel contesto europeo.

## CIPM – *Certified Information Privacy Manager*

**La CIPM** certifica le conoscenze sulla **gestione operativa dei programmi di privacy**, attestando le competenze necessarie per stabilire, implementare e gestire un programma di protezione dei dati lungo tutto il suo ciclo di vita, con particolare focus sulla **leadership** e sulla **governance dei processi** privacy.

Abbinata alla certificazione **CIPP/E**, fornisce il **mix di competenze legali e gestionali** richieste a chi deve ricoprire ruoli di responsabilità nella protezione dei dati, come il DPO secondo il GDPR.

## CIPT – *Certified Information Privacy Technologist*

**La CIPT** certifica le conoscenze sulle tecnologie e sui processi di ingegneria della privacy, attestando le competenze necessarie per **progettare, implementare e valutare soluzioni tecnologiche che rispettino la protezione dei dati,** con particolare attenzione alla privacy by design e alla governance dei processi IT.

A differenza della **CIPM**, focalizzata sulla gestione dei programmi di privacy, la **CIPT** è rivolta ai professionisti che operano principalmente su aspetti tecnologici e infrastrutturali.

**L'Artificial Intelligence Governance Professional (AIGP)** risponde alla diffusione dei sistemi di Intelligenza Artificiale (IA) certificando le competenze dei professionisti per la **governance dei sistemi IA**, definendo e attestando la capacità di costruzione di framework etici e conformi alle normative per garantire **trasparenza, equità e sicurezza.**

# Le certificazioni per audit e sicurezza delle informazioni

Per un DPO, anche la **padronanza delle metodologie di audit**, nonché la conoscenza dei principali **standard internazionali in materia di sicurezza delle informazioni** sono fondamentali.

## ISACA (Information Systems Audit and Control Association)

**CISA**: attesta l'esperienza nell'audit, controllo e sicurezza dei sistemi informativi.

**CDPSE**: valida le competenze nell'implementazione di soluzioni privacy by design e nella valutazione dei controlli di privacy, spesso attraverso audit tecnici.

**CRISC**: Focalizzata sulla gestione del rischio IT e dei controlli, è utile per il DPO nell'identificare e mitigare i rischi legati al trattamento dei dati.

## IIA (Institute of Internal Auditors)

**CIA:** copre un'ampia gamma di competenze di audit, inclusi gli audit operativi e di conformità.

**CRMA**: sulla gestione del rischio e sull'assicurazione.

## Certificazione ISO per persone fisiche

- **ISO 9001:2015**
  Sistemi di Gestione per la Qualità - QMS
- **ISO 22301:2019**
  Sistemi di Gestione della Continuità Operativa - BCMS
- **ISO/IEC 27001:2022**
  Sistemi di Gestione della Sicurezza delle Informazioni - ISMS
- **ISO/IEC 42001:2023**
  Sistemi di Gestione dell'Intelligenza Artificiale - AIMS
- **ISO/IEC 27701:2025**
  Estensione alla Gestione della Privacy delle Informazioni - PIMS

# Il DPO: un ruolo europeo, competente e strategico

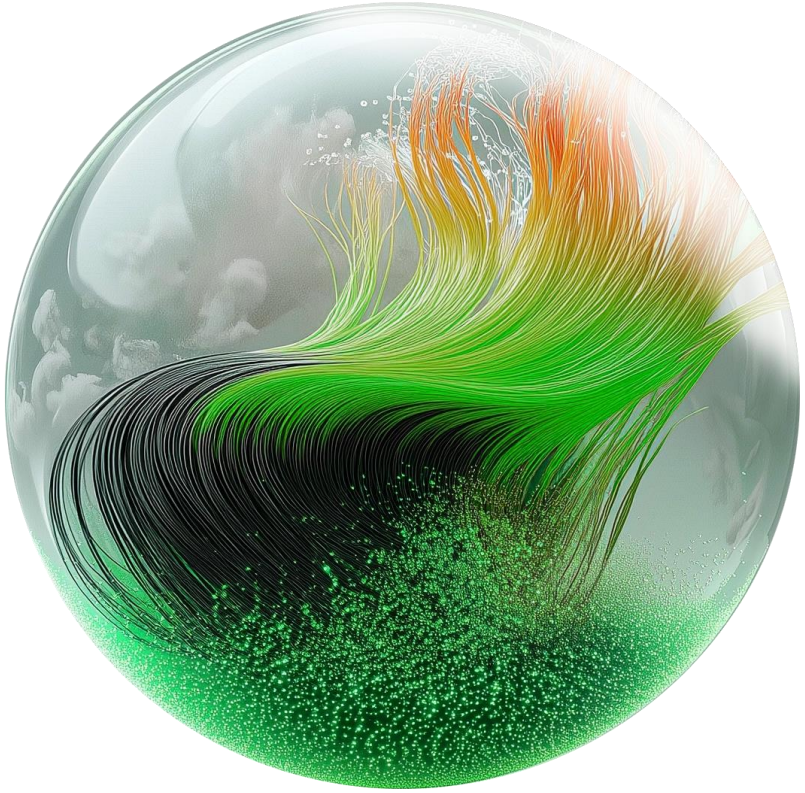
L'evoluzione dello standard di certificazione ha trasformato il DPO da figura nazionale ad **ruolo professionale** riconosciuto a livello **europeo**. Questa evoluzione lo posiziona come **guida strategica** per affrontare le **nuove sfide digitali**, grazie **a un set di competenze** e **abilità** che lo rendono una figura centrale anche per il **business**.

*Dall'Italia all'Europa, dal GDPR alle nuove sfide digitali...*


*..il DPO garantisce competenza, visione e indipendenza*

Deloitte.

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO



# Aggiornamenti su protezione dei dati e telemarketing

**Community Privacy e DPO Unindustria**

**25 novembre 2025**

# Introduzione alla Data Protection nel Telemarketing e Teleselling

Le attività di telemarketing e teleselling hanno assunto un ruolo sempre più **centrale e strategico** grazie alla crescente digitalizzazione dei processi. Questo sviluppo ha anche portato a una **crescente attenzione** verso il rispetto dei requisiti di privacy, con l'obiettivo di **garantire** che il trattamento dei dati avvenga nel **pieno rispetto** delle normative vigenti e degli orientamenti delle autorità di controllo.

**DATA PROTECTION COME ELEMENTO CHIAVE IN TUTTE LE FASI**


*Main Goals*

**PROTEGGERE I DATI PERSONALI**

**FIDUCIA DEL CLIENTE**

**MINIMIZZARE RISCHI**

*legali, reputazionali e sanzionatori*

**MASSIMIZZARE il POTENZIALE dei DATI**

*Occorre garantire la Compliance nelle diverse **fasi dell'intero ciclo di vita** del cliente, **dall'acquisizione del contatto** di un potenziale cliente **fino alla cessazione** del rapporto, includendo eventuali attività di **ricontatto successive**.*

# Il Framework normativo di riferimento per le attività di Marketing e Digital Marketing

Nel contesto del Marketing e del Digital Marketing, la protezione dei dati personali è regolamentata da un **insieme articolato di normative** specifiche che ne disciplinano la **raccolta**, l'**utilizzo** e la **conservazione**.

## Normativa Europea

- **GDPR**
- **DIRETTIVA e-Privacy**
- **DIGITAL MARKET ACT (DMA)**
- **DIGITAL SERVICES ACT (DSA)**

## Normativa Italiana

- **CODICE PRIVACY**

## Linee guida e Provvedimenti EDPB e Garante

- **LINEE GUIDA SUL CONSENSO**
- **LINEE GUIDA SUI COOKIE**
- **CODICE DI CONDOTTA**
- **PROVVEDIMENTI DEL GARANTE**

# Campagne di Telemarketing e Teleselling: condizioni e misure di compliance

**Sin dalle prime fasi di acquisizione del dato** è necessario considerare **alcuni aspetti chiave**:


## Fonte del dato

- Identificare **chi** ha raccolto il dato, **come** è stato raccolto e **da chi** è stato fornito
- Verificare la **provenienza** delle **liste** acquistate da terzi, assicurando affidabilità e conformità

## Vigilanza sui terzi

- Verificare **l'affidabilità** e la **reputazione** delle agenzie prima dell'ingaggio
- Formalizzare **ruoli**, responsabilità, e **modalità** di raccolta e consensi
- Monitorare nel tempo **l'operato** delle agenzie

## Raccolta del consenso

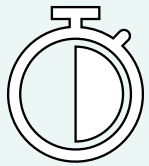
- Fornire **un'informativa** chiara, trasparente e accessibile
- Raccogliere un **consenso** libero, specifico, informato, inequivocabile e granulare
- Predisporre canali idonei per la gestione delle richieste dei **diritti** degli interessati.

*È fondamentale valutare la **validità temporale del consenso**, verificando: il **contesto temporale** in cui è stato raccolto, se al momento della raccolta era **valido e informato**, e se sono disponibili **prove sufficienti a dimostrarlo**.*

# La validità temporale del consenso prestato

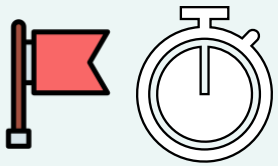
Solo un consenso attuale e correttamente informato autorizza il trattamento dei dati in modo legittimo. È quindi fondamentale verificare **quando il consenso è stato ottenuto**, se **rimane valido** nel contesto temporale e **quali azioni** sono consentite entro l'**arco temporale definito**, assicurandosi adeguate evidenze a supporto.

Ogni consenso prestato è caratterizzato da una **validità temporale** che occorre considerare **prima dell'avvio di una campagna promozionale**



Il consenso acquisito in un dato momento tende a **perdere forza** trascorso un determinato **lasso di tempo** da definire all'interno di una politica sulla conservazione dei dati

Tale lasso di tempo **inizia a scorrere dall'ultimo contatto** o **dall'ultimo contratto concluso** e si esaurisce nel momento in cui è **ragionevole presumere** che il **cliente o l'ex cliente possa non desiderare** più di ricevere comunicazioni promozionali



Giunti a questa fase, **non è sempre necessario rivitalizzare il consenso**, ma è **obbligatorio ricordare al cliente il consenso in precedenza prestato** e la costante possibilità di **revocarlo in qualsiasi momento**

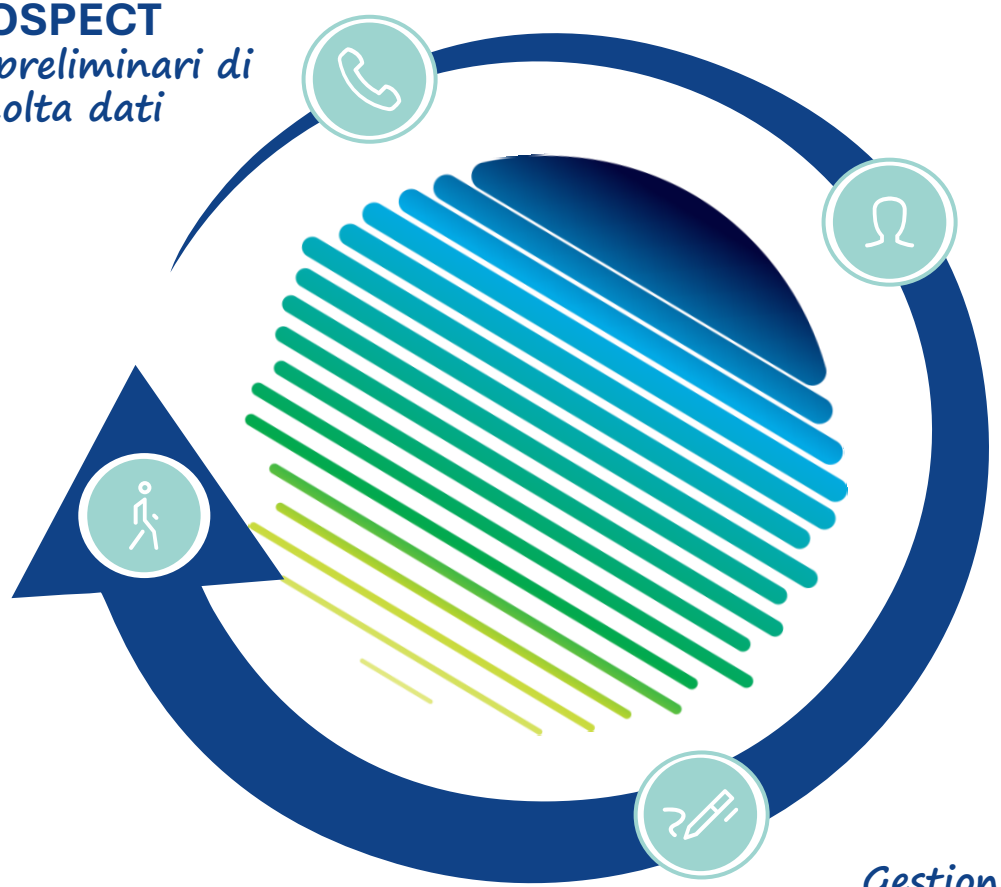
# Il Ciclo di Vita del Dato

Dalla raccolta iniziale delle informazioni fino alle strategie di *win back*, **ogni fase del trattamento dati** richiede attenzione e precisione. Comprendere e ottimizzare questi passaggi permette di **valorizzare i dati**, **migliorare le relazioni** con i clienti e **incrementare le performance** di business.

1

**PROSPECT**

*Attività preliminari di raccolta dati*



2

**LEAD**

*Acquisizione formale del contatto*

3

**CLIENTE**

*Gestione dati durante la stipula e l'esecuzione del contratto*

4

**CESSAZIONE E *WIN BACK***

*Gestione dati cessato il rapporto e strategie di riattivazione*

# Il Ciclo di Vita del Dato

Prospect | Lead | Cliente | Cessazione

## Descrizione della fase

Rappresenta il **primo contatto** preliminare con un **potenziale cliente,** nell'ambito del quale **si intercetta un primo interesse o bisogno** con l'obiettivo di **qualificare il contatto.**

### RISCHI PRINCIPALI

1. Contatti non verificati presso **RPO**
2. Telemarketing **selvaggio**
3. Mancata formalizzazione **nomine a responsabile** (in caso di esternalizzazione attività di gestione prospect)
4. Utilizzo **non lecito** dei dati dei prospect

### PRATICHE VIRTUOSE

- ✓ Verifica liceità e adeguata conformità delle **liste di contatti** da terzi
- ✓ Verifica preventiva presso il Registro Pubblico delle Opposizioni (**RPO**)
- ✓ **Vigilanza** sulle attività di call-center e agenzie esterne per evitare fenomeni di "**sottobosco**"
- ✓ **Black-list** interne per soggetti che hanno espresso diniego o reclamo
- ✓ Adeguate verifiche per garantire la **corretta resa dell'informativa** e la **liceità** nell'utilizzo dei dati dei prospect

**NEWS** **Dal 19/11 blocco automatico chiamate da mobili falsificati disposto con Del. n. 271/25/CONS dell'AGCOM**

# Il Ciclo di Vita del Dato

Prospect | **Lead** | Cliente | Cessazione

## *Descrizione della fase*

Consiste nella raccolta dei dati personali e del consenso del **potenziale cliente**, attraverso un'**interazione diretta con lo stesso** o **mediante il supporto di terzi**.

### RISCHI PRINCIPALI

1. Raccolta dati senza **idonea informativa**
2. Trattamento dati per marketing senza idoneo **consenso**
3. Consenso **non granulare**
4. Mancato **Double Opt-in** e consenso **non adeguatamente dimostrabile**

### PRATICHE VIRTUOSE

- ✓ **Informativa** privacy chiara, trasparente, aggiornata e disponibile
- ✓ Consenso **granulare**
- ✓ Raccolta dati **limitata** e **pertinente**
- ✓ Rispetto delle **preferenze** di opt-in
- ✓ **Double Opt-in e tracciabilità** e **documentazione** dei consensi acquisiti
- ✓ Procedure semplificate per **revoca** tempestiva del consenso
- ✓ Processi efficaci per gestire le richieste di esercizio dei **diritti privacy**

# Il Ciclo di Vita del Dato

Prospect | Lead | **Cliente** | Cessazione

## *Descrizione della fase*

Prevede il trattamento dei dati personali per la **stipula e l'esecuzione** dell'accordo, nonché per l'invio di **comunicazioni strettamente correlate** al servizio offerto.

### RISCHI PRINCIPALI

1. Conclusione contratti **non leciti**
2. Trattamento di dati **inesatti** e **non aggiornati**
3. **Mancata supervisione** dei terzi responsabili
4. Trattamento dei dati per **finalità non previste** in informativa
5. Mancato adempimento dei **diritti privacy**
6. Violazioni di **sicurezza**

### PRATICHE VIRTUOSE

- ✓ **Tracciabilità** delle operazioni di registrazione delle proposte
- ✓ Sistemi di alert per **anomalie** procedurali
- ✓ Procedure di verifica della **volontà del cliente** (es. check-call bloccanti) prima della conclusione definitiva del contratto
- ✓ **Nomina** formale a responsabili per agenzie e sub-agenzie, adeguate istruzioni (es. script) e presidio attivo
- ✓ **Limitazione** del trattamento alle sole finalità dichiarate in informativa
- ✓ **Misure di sicurezza** adeguate alla protezione del CRM e di tutti i *database* contenenti dati dei clienti e contratti

# Il Ciclo di Vita del Dato

Prospect | Lead | Cliente | **Cessazione**

## *Descrizione della fase*

Riguarda la gestione dei dati personali **dopo la conclusione** del rapporto contrattuale, nonché le **attività di riattivazione** clienti, cd. ***win back***, volte a incentivare il ritorno e la fidelizzazione.

### RISCHI PRINCIPALI

1. Trattamento dati **senza base** giuridica
2. Mancata **cancellazione/anonimizzazione**
3. Comunicazioni **indesiderate**

### PRATICHE VIRTUOSE

- ✓ Verifica dei presupposti di legittimità per attività di **win-back**
- ✓ Verifica della **validità temporale** dei consensi acquisiti
- ✓ Politiche per la **conservazione** dei dati personali adeguate
- ✓ Processi per **cancellare/anonimizzare** degli **ex clienti** al decorrere dei termini di Data retention
- ✓ **Registrazione evidenze** delle verifiche effettuate, dei consensi acquisiti e delle misure adottate

Deloitte.



***

Deloitte, one of the largest professional services network in Italy, first started its activity in this country in 1923 and boasts century old roots, combining a tradition of quality with avant garde methods and technological expertise. Deloitte's professional services, which include Audit & Assurance, Consulting, Financial Advisory, Risk Advisory, Tax and Legal, are rendered by various separate and independent firms, specialised in the single professional areas, which are all part of the Deloitte network. Today, the Italian network employs 6,000 professionals who help their clients excel thanks to the confidence in the high level of service, in our multidisciplinary offering and our widespread geographical coverage.

With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s 286,200 professionals are committed to becoming the standard of excellence.