La conformità al GDPR nel white label banking

Il white label banking è un settore in rapida espansione, ma comporta anche importanti sfide regolatorie. Questo articolo esplora le principali implicazioni in materia di GDPR per le organizzazioni che operano nell'UE e nel Regno Unito, offrendo indicazioni pratiche per agevolare la conformità.

Il white label banking consente alle aziende di offrire servizi finanziari – come conti di risparmio, prestiti e carte di pagamento – con il proprio marchio, appoggiandosi all'infrastruttura di un fornitore terzo. Questo modello garantisce rapidità e scalabilità, ma introduce anche rischi complessi per la protezione dei dati personali.

Ai sensi del Regolamento Generale sulla Protezione dei Dati (GDPR), tutte le parti coinvolte – brand, banche e fornitori terzi – devono collaborare per garantire conformità, trasparenza e responsabilità.

Di seguito analizziamo nel dettaglio ciascuna di queste aree critiche:

- **Condurre DPIA congiunte**
- **Definire ruoli e responsabilità**
- **Includere clausole GDPR nei contratti**
- **Mantenere un Registro delle attività di trattamento (RoPA)**
- **Dare priorità alla trasparenza**
- **Stabilire le responsabilità per le richieste degli interessati**
- **Definire un piano di risposta alle violazioni**
- **Condurre un'adeguata due diligence**

Comprendere i rischi GDPR nel white label banking

Nel sistema bancario tradizionale, i flussi di dati sono solitamente centralizzati e gestiti da un unico titolare del trattamento: la banca. La compliance è definita in un quadro unitario con responsabilità ben definite in materia di sicurezza, trasparenza e diritti degli interessati.

Nel white label banking, queste responsabilità sono spesso condivise. La banca autorizzata è di norma il titolare del trattamento per i servizi finanziari principali. Tuttavia, la società che offre il servizio in white label può essere considerato contitolare se influenza le modalità di raccolta o uso dei dati dei

clienti. In alcuni casi, la società fornitrice del front-end del servizio agisce invece come responsabile del trattamento, su istruzioni della banca.

Ulteriori soggetti terzi, come fornitori KYC (Know Your Customer), strumenti di monitoraggio delle frodi o piattaforme cloud, possono agire come responsabili o sub-responsabili a seconda del loro ruolo nei flussi di dati.

Questa struttura frammentata, con molteplici attori coinvolti, comporta un ecosistema di dati dispersivo e incrementa il rischio di:

- Ruoli e responsabilità poco chiari o sovrapposti
- Ritardi nella notifica delle violazioni, con rischio di superare il termine di 72 ore previsto dal GDPR
- Risposte inadeguate alle richieste degli interessati
- Carenze nella trasparenza e nell'accountability

Per garantire la conformità al GDPR, tutte le parti devono comprendere i propri obblighi e collaborare per trattare i dati personali in modo lecito, corretto e trasparente.

Come garantire la conformità al GDPR

Per gestire questi rischi, le organizzazioni che intraprendono progetti di white label banking dovrebbero adottare le seguenti strategie:

1. Condurre valutazioni d'impatto congiunte (DPIA)

Ai sensi dell'art. 35 del GDPR, è richiesta una DPIA quando il trattamento può comportare un rischio elevato per i diritti degli interessati, ad esempio, trattamenti di dati finanziari su larga scala, aventi ad oggetto categorie particolari di dati, o attività di profilazione. In un modello white label, è essenziale che il soggetto che offre il servizio white label, banca e soggetti terzi coinvolti conducano DPIA congiunte per identificare i rischi e concordare le misure di mitigazione.

2. Definire ruoli e responsabilità

È necessario stabilire chiaramente se ciascuna parte agisce come titolare, contitolare o responsabile del trattamento. Di norma, la società partner gestisce le attività di marketing e onboarding dei clienti, mentre la banca si occupa della gestione dei conti e degli obblighi regolatori. I ruoli devono essere definiti ai sensi degli artt. 4(7) e 4(8) GDPR per garantire una corretta attribuzione delle responsabilità.

3. Includere clausole GDPR nei contratti

I contratti devono riflettere le responsabilità privacy di ciascun attore. L'art. 28 GDPR prevede clausole specifiche nei rapporti con i responsabili (es. riservatezza, uso di sub-responsabili, sicurezza, notifica delle violazioni). In caso di contitolarità, l'art. 26 richiede un accordo scritto che definisca le rispettive responsabilità e le modalità di esercizio dei diritti da parte degli interessati.

4. **Mantenere un Registro delle attività di trattamento (RoPA)**

L'art. 30 del GDPR impone, al ricorrere di determinate circostanze, la tenuta di un registro delle attività di trattamento. In un contesto white label, ciò implica mappare i flussi di dati tra la società partner, banca e terzi. Un registro ben documentato supporta la responsabilizzazione, agevola la risposta agli incidenti e semplifica la gestione delle richieste di accesso.

5. **Dare priorità alla trasparenza**

I clienti potrebbero non essere consapevoli della presenza di più soggetti dietro le quinte. L'informativa privacy deve chiarire quali entità trattano i dati, con quale ruolo, e come gli interessati possono esercitare i propri diritti.

6. **Gestire le richieste degli interessati**

Le parti devono concordare e documentare come verranno gestite le richieste degli interessati – ad esempio accesso, rettifica o cancellazione – cooperando per garantire una risposta tempestiva e appropriata.

7. **Definire un piano di risposta alle violazioni**

In un contesto con molteplici controparti, le violazioni possono non essere rilevate o comunicate tempestivamente. È necessario predisporre un piano congiunto di risposta alle violazioni di dati, da integrare nei contratti, che definisca ruoli e responsabilità e assicuri il rispetto del termine di notifica di 72 ore.

8. **Condurre una due diligence accurata**

Non bisogna presumere che il rispetto delle normative finanziarie implichi automaticamente la conformità al GDPR. Prima di stipulare un accordo white label, è fondamentale condurre una due diligence sui partner, verificando le informative, certificazioni di sicurezza, precedenti violazioni e procedure per la gestione dei diritti degli interessati

Conclusioni

Il white label banking consente alle società partner che offrono il servizio white label di espandere rapidamente le proprie attività e offrire servizi finanziari integrati ai propri clienti. Tuttavia, la presenza di molteplici attori nel trattamento dei dati personali rende la conformità al GDPR una sfida complessa.

Le aziende devono definire chiaramente ruoli e responsabilità, garantire trasparenza nei confronti dei clienti, condurre un'accurata due diligence su tutti i partner e integrare la protezione dei dati fin dalle fasi iniziali, attraverso DPIA e contratti solidi. Rendendo la compliance parte integrante del rapporto contrattuale, le organizzazioni possono offrire servizi finanziari affidabili, che rispettano i diritti degli interessati e mantengono elevati standard di protezione dei dati.

Se la tua azienda può beneficiare di una consulenza specialistica in materia di protezione dei dati, contattaci per scoprire come i nostri servizi in outsourcing possono supportare il tuo business.
