PROCEDURA OPERATIVA
Accesso alle informazioni personali degli ex clienti

Procedura emessa il 30/04/2024

Owner della procedura: Organization & Business Continuity

SOMMARIO

1 PREMESSA

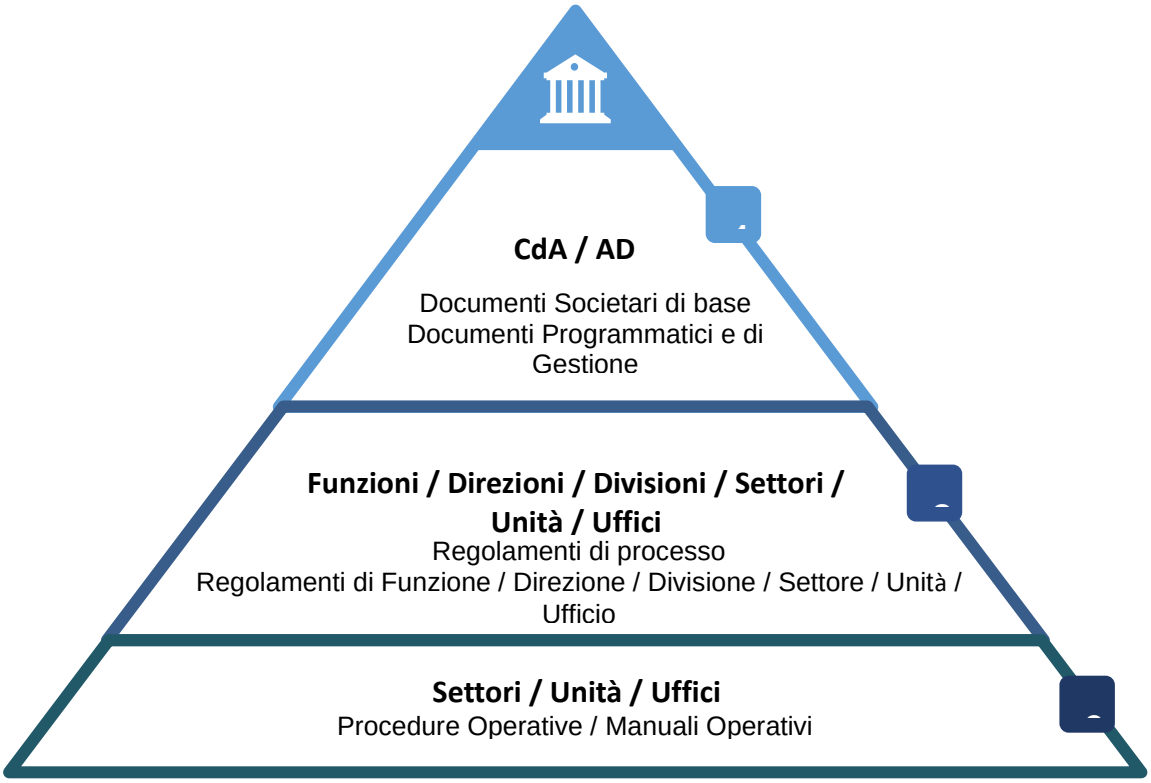
Per adempiere alle disposizioni del Regolamento UE 2016/679 (in seguito anche "GDPR"), il Consiglio di Amministrazione di Flowe ha approvato una specifica Policy (Data Retention Policy) che indica i principi cui gli operatori della Società devono ispirarsi per il trattamento delle informazioni personali degli ex clienti, gli stessi nello specifico prevedono che siano "nascoste" le informazioni personali dei clienti che hanno chiuso il rapporto da oltre tre anni salvo esplicita richiesta del cliente o dell'autorità sino a 10 anni dalla chiusura del rapporto e sino a 15 anni per esigenze e finalità della Società.

In ogni caso l'accesso alle informazioni dei clienti che hanno chiuso il rapporto da oltre tre anni è subordinato al benestare dell'Ufficio Privacy della Capogruppo Banca Mediolanum.

2 OBIETTIVI

Obiettivo del documento è descrivere il processo attraverso cui gli operatori possono accedere alle informazioni personali dei clienti che hanno chiuso il rapporto da oltre tre anni.

Con riferimento alla "Policy di redazione e divulgazione della normativa interna", il presente documento si colloca al secondo livello della piramide documentale richiamata nello schema seguente:



2.1 AMBITO DI APPLICAZIONE

La presente procedura si applica a Flowe S.p.A. Società Benefit.

2.2 AGGIORNAMENTO DEL DOCUMENTO

L'aggiornamento e la revisione del presente documento sono di responsabilità dell'Unità manageriale di supporto *Organization & Business Continuity*.

3 STRUMENTI A SUPPORTO DEL PROCESSO

L'infrastruttura tecnologica di cui si è dotata Flowe per supportare il processo in oggetto include gli strumenti informatici di seguito descritti.

3.1 TEMENOS

Flowe si avvale dell'outsourcer Temenos - applicativo di Core Banking T24 – attraverso il quale apre la posizione anagrafica del cliente e il conto di pagamento a fronte dell'esito positivo di tutti i controlli di onboarding. T24 permette inoltre di gestire i processi "core" della Società per la gestione delle operazioni di pagamento.

3.2 P0 PLATFORM

P0 è la Piattaforma della Società (*full cloud* – Microsoft Azure) sulla quale è realizzata la logica applicativa. Supporta il processo di *onboarding* e gestisce le informazioni anagrafiche della clientela rendendole disponibili tramite API specifiche a sistemi terzi o tramite query specifiche che possono essere sottomesse solo da operatori autorizzati.

Agendo sulle API di cui sopra è stato realizzato il principio di anonimizzazione delle informazioni indicato nella Data Retention Policy, queste infatti restituiscono stringhe di caratteri convenzionali ("*") in luogo delle informazioni personali laddove vengano richieste informazioni relative a clienti aventi il profilo chiuso da oltre tre anni.

3.3 FANBASE

Fanbase è la piattaforma applicativa sviluppata internamente alla Società basata su tecnologia *cloud* Microsoft *Power Platform*.

Tale soluzione mette a disposizione degli operatori di *front* e *back office* funzionalità volte al supporto diretto e indiretto del cliente finale (*Customer Relationship Management*) includendo tra queste anche la possibilità di accedere alle informazioni personali del cliente.

4 ATTORI, RUOLI E RESPONSABILITÀ

Di seguito sono indicati i principali attori, coinvolti nel processo di *onboarding* ed apertura Conto di pagamento della clientela di Flowe e i relativi ruoli e responsabilità nell'ambito delle attività descritte.

4.1 PAYMENT SERVICES & CONTROLS

Gli operatori della Funzione *Payment Services & Controls* che ne avessero necessità[1]:

a) richiedono tramite messaggio di posta elettronica all'Ufficio Privacy della Capogruppo (privacy.ufficio@mediolanum.it) l'accesso alle informazioni personali di clienti che hanno chiuso il rapporto da oltre tre anni, al messaggio allegano sempre copia dell'autorità/cliente richiedente;

b) inoltrano agli operatori autorizzati a sottomettere query in ambiente P0 l'eventuale benestare ricevuto dall'Ufficio Privacy di Banca Mediolanum;

4.2 OPERATORI AUTORIZZATI PRODUCT DEVELOPMENT & IT SERVICES

Gli operatori della Funzione *Product Development & IT Services*, abilitati a sottomettere le query nell'ambiente P0 di produzione, sono autorizzati ad accedere alle informazioni dei clienti che hanno chiuso il profilo da oltre tre anni, solo a fronte della autorizzazione scritta dell'Ufficio Privacy ed in questo caso:

a) sottomettono la query fornendone i risultati al richiedente;

b) conservano copia delle richieste ricevute e delle risposte fornite agli operatori che hanno fatto richiesta di estrazione delle informazioni criptate.

L'attività di interrogazione del database anagrafico di P0 è registrata "in background"[2] in appositi "log" disponibili per eventuali attività di controllo.

4.3 UFFICIO PRIVACY DI BANCA MEDIOLANUM

L'Ufficio Privacy di Banca Mediolanum - in forza del contratto di appalto di fornitura dei servizi di gestione aziendale in essere tra Banca Mediolanum e Flowe svolge e coordina tutti gli adempimenti previsti dalle normative in tema di privacy per la Società in particolare:

a) verifica la conformità a tutti i requisiti legali applicabili relativi al periodo di conservazione dei dati con il supporto delle strutture aziendali competenti in materia;

[1] Le informazioni personali dei clienti che hanno chiuso il conto da più di tre anni compaiono in forma anonimizzata negli applicativi di back office, la necessità di ottenere le informazioni in chiaro si presenterebbe quando l'interrogazione fosse stata effettuata per corrispondere ad una richiesta del cliente stesso, dell'Autorità Giudiziaria o dell'Autorità di Controllo.

[2] La registrazione "in background" comporta la registrazione permanente dell'attività dell'operatore a prescindere dalla volontà di quest'ultimo

b) valuta l'opportunità di fornire il benestare all'accesso alle informazioni personali dei clienti che hanno chiuso il rapporto da oltre tre anni, comunicando al richiedente l'esito della valutazione;

4.4 FUNZIONI AZIENDALI DI CONTROLLO

Le Funzioni Aziendali di Controllo (Internal Audit, Risk Management, Compliance, Unità Controlli Privacy e Antiriciclaggio) hanno la responsabilità di eseguire i controlli di propria competenza:

- sulla corretta applicazione dei principi della Data Retention Policy;
- sul rispetto delle indicazioni della presente procedura;
- sull'efficacia dei sistemi di controllo a presidio dei rischi connessi alla gestione delle informazioni personali dei clienti

5 RICHIESTA DI ACCESSO ALLE INFORMAZIONI PERSONALI DEGLI EX CLIENTI

I sistemi di back office della Società (FanBase) riportano informazioni criptate per i clienti il cui profilo è chiuso da oltre tre anni; non è prevista la possibilità di ripristinare la visualizzazione di tali informazioni in un secondo momento.

Qualora si rendesse necessario accedere alle informazioni criptate a fronte di una richiesta esplicita e formalizzata proveniente da:

a) il cliente stesso;

b) l'Autorità giudiziaria

c) l'Autorità di Controllo

si applica la procedura:

1) l'operatore inoltra la richiesta ricevuta all'Ufficio Privacy (privacy.ufficio@mediolanum.it) della Capogruppo Banca Mediolanum.

2) L'ufficio Privacy della Capogruppo:

   - effettua le proprie valutazioni in ordine all'opportunità di concedere o negare l'accesso in chiaro alle informazioni criptate

   - fornisce risposta al richiedente

3) In caso l'Ufficio Privacy della Capogruppo abbia concesso l'accesso alle informazioni criptate, l'operatore inoltra la risposta dell'Ufficio Privacy della Capogruppo agli operatori della *Funzione Product Development & IT Services*, autorizzati a sottomettere le query in ambiente P0.

4) Gli operatori autorizzati sottomettono la query e restituiscono l'esito all'operatore che ne ha fatto richiesta.

Le query effettuate dagli operatori autorizzati in ambiente P0_produzione sono registrate in appositi log a disposizione delle Funzioni Aziendali di Controllo.

6 RIFERIMENTI NORMATIVI

6.1 NORMATIVA INTERNA

Si riepilogano le fonti informative interne alla Società che presentano relazioni con la procedura in esame:

- Privacy Policy di Banca Mediolanum Spa
- Data Retention Policy

6.2 NORMATIVA ESTERNA

Nel presente capitolo si richiama il contesto normativo nel quale opera la presente Procedura. Si riportano, di seguito i principali riferimenti normativi adottati a livello comunitario e nazionale:

- **Regolamento UE 2016/679** del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- **Codice in materia di protezione dei dati personali: d.lgs. 30 giugno 2003, n. 196**, così come modificato dal d.lgs. 10 agosto 2018, n. 101.
- **Provvedimento generale del Garante per la protezione dei dati personali del 15 maggio 2013** "Consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto";
- **Provvedimenti EDPB e Garante** per la protezione dei dati personali in materia di videosorveglianza;
- **Provvedimento generale del Garante per la protezione dei dati personali del 28 novembre 2008** e s.m.i. "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";