

ATTUALITÀ

L'informativa privacy nella relazione bancaria

Dalla completezza del testo all'effettività
della trasparenza

2 Ottobre 2026

Aurora Agostini, Partner, Lexia





Aurora Agostini, Partner, Lexia

> Aurora Agostini

Aurora Agostini è partner responsabile del team Data & Technology Innovation di Lexia Avvocati. Assiste clienti in tutti i settori del diritto dell'informatica, della proprietà intellettuale e delle nuove tecnologie, con un'ampia competenza sugli aspetti della protezione dei dati e della privacy. La sua attività si concentra sulle misure di compliance, come le procedure e la documentazione richieste dal GDPR, la valutazione della base giuridica del trattamento, la conformità digitale (ad esempio i cookie), le politiche sulla privacy, le risposte ai reclami e l'esercizio dei diritti, i trasferimenti transfrontalieri di dati.

Avvocati

Lexia



Due recenti provvedimenti del Garante - il caso Isybank e il caso BBVA - mostrano che, nel settore bancario, la trasparenza è una proprietà del processo: scelta della base giuridica, progettazione dei canali e coerenza delle risposte operative.

Nella prassi degli intermediari, la trasparenza è spesso ricondotta alla corretta redazione dell'informativa ex artt. 13 e 14 GDPR: si elencano finalità, ruoli, recapiti del titolare e del DPO, si aggiorna la tassonomia dei trattamenti e si verifica la completezza delle clausole. Si tratta però di un'attività necessaria ma non sufficiente: la trasparenza non coincide con la sola disponibilità formale del testo. Un'informativa può essere impeccabile sul piano redazionale e, nondimeno, inadeguata se raggiunge il cliente in un canale o in un momento che non consente di comprendere l'uso dei dati, oppure se tace proprio il trattamento da cui dipende una modifica rilevante della relazione bancaria.

1. Il caso Isybank: il trattamento che mancava e la comunicazione che non emergeva

La vicenda del trasferimento di parte della clientela di Intesa Sanpaolo a Isybank, che ha interessato circa 2,4 milioni di rapporti, offre una rappresentazione particolarmente nitida di come una scelta organizzativa, se non accompagnata da un'informazione adeguata e da una corretta qualificazione dei trattamenti sottostanti, possa tradursi in un problema di trasparenza e di liceità del trattamento.

Con il provvedimento n. 163 del 12 marzo 2026, il Garante ha ritenuto illecito il trattamento relativo alla selezione dei clienti da trasferire - applicando una sanzione di 17.628.000 euro e contestando violazioni degli artt. 5, par. 1, lett. a), 6, par. 1, e 14 GDPR - in quanto l'istituto, per individuare il segmento di clientela "prevalentemente digitale", aveva applicato criteri fondati, tra l'altro, sui comportamenti d'uso dei servizi, dando così luogo, secondo l'Autorità, a una profilazione ai sensi dell'art. 4, n. 4, GDPR, distinta dalla profilazione commerciale già illustrata alla clientela.

L'informativa dedicata all'operazione societaria, tuttavia, richiamava soltanto quest'ultima e non spiegava che i dati sarebbero stati utilizzati per definire il perimetro dei rapporti da conferire alla nuova banca, con la conseguenza che il difetto informativo si collocava proprio nel punto in cui la conoscenza del trattamento era più rilevante, poiché la selezione non serviva a proporre un prodotto ma contribuiva a determinare il mutamento dell'interlocutore bancario e delle modalità operative del rapporto.

Il provvedimento richiama, in questo quadro, l'art. 14, par. 2, lett. g), in tema di informazioni sul processo decisionale automatizzato e, nei casi dell'art. 22, sulla logica, sull'importanza e sulle conseguenze, sottolineando che non ogni segmentazione costituisce "profilazione" ai sensi del GDPR e che la profilazione, a sua volta, non coincide necessariamente con una decisione basata unicamente su trattamenti automatizzati che produca effetti giuridici o analogamente significativi. La corretta qualificazione richiede quindi di esaminare in concreto dati utilizzati, componente automatizzata, ruolo dell'intervento umano ed effetti della selezione; anche quando non ricorrono tutte le condizioni dell'art. 22, permane l'obbligo di descrivere con chiarezza finalità nuova, categorie di dati, base giuridica e conseguenze prevedibili, evitando letture semplicistiche che pretendano di trarre dal caso una regola generale secondo cui ogni perimetrazione di un ramo bancario richiederebbe il consenso del cliente o l'informazione "rafforzata" prevista per le decisioni automatizzate.

Questa distinzione concettuale si riflette immediatamente sul piano della base giuridica: l'art. 58 TUB disciplina il trasferimento dei rapporti nelle cessioni in blocco e non impone, di per sé, il consenso del cliente ceduto. Ciò non significa, tuttavia, che ogni trattamento preparatorio - inclusa un'eventuale profilazione della clientela funzionale a individuare chi confluirà nel perimetro ceduto - possa essere automaticamente ricondotto alla medesima esigenza organizzativa; per questo il Garante, ritenendo insufficiente il legittimo interesse invocato per la selezione, valorizza l'incidenza concreta della scelta sulla posizione dei clienti e la distanza tra ciò che essi potevano ragionevolmente attendersi e quanto era stato loro comunicato, spostando il fuoco dal contrasto astratto tra cessione e privacy alla verifica separata del fondamento della comunicazione dei dati necessari al trasferimento e di quello dell'analisi preliminare che individua chi sarà trasferito.

Accanto al contenuto dell'informativa, la decisione dedica ampio spazio al modo in cui l'avviso fu reso, evidenziando come la collocazione nella sezione archivio dell'area riservata *web* e dell'*app*, l'assenza di particolare evidenza o di notifiche *push*, l'invio a partire dal 28 giugno 2023 - dunque in larga parte nel periodo estivo - e l'assegnazione di un termine per manifestare dissenso, cui era attribuito un preciso significato operativo al silenzio, abbiano determinato, per alcuni interessati, l'impossibilità di notare o leggere in tempo utile la comunicazione e di opporsi nei termini, sicché l'affermazione secondo cui la trasparenza riguarda anche le modalità di resa dell'informazione non costituisce un inciso marginale,

ma il punto in cui la scelta del canale viene collegata alla possibilità effettiva di conoscere un trattamento inatteso.

Occorre, tuttavia, evitare l'eccesso opposto, poiché il caso non dimostra che l'*app* sia sempre inadatta per comunicazioni giuridicamente rilevanti, né introduce un obbligo generalizzato di notifica *push*, presa visione o *opt-in*, ma mostra piuttosto come l'adeguatezza del canale dipenda dalla combinazione tra rilevanza del messaggio, prevedibilità dell'operazione, tempo concesso per reagire e peso attribuito al silenzio, sicché una comunicazione ordinaria e una comunicazione che prelude al trasferimento del rapporto bancario non possono essere progettate con la stessa gerarchia visiva e la stessa sequenza di avvisi, senza accrescere il rischio che il cliente non comprenda ciò che sta per accadere.

Le Linee guida del Gruppo di lavoro articolo 29 sulla trasparenza ai sensi del GDPR (WP260 rev.01, 2018), fatte proprie dall'EDPB, e le Linee guida EDPB 4/2019 sull'articolo 25 GDPR (Protezione dei dati fin dalla progettazione e per impostazione predefinita) convergono, del resto, nel chiarire che forma e modalità della comunicazione non costituiscono un elemento meramente esteriore ma rientrano a pieno titolo tra le "misure appropriate" in capo al titolare, il quale è chiamato a rendere l'informazione contestuale, pertinente per il destinatario, accessibile su più canali e organizzata per livelli, così da conciliare completezza e comprensione, senza che ciò implichi l'adozione di una soluzione grafica univoca e standardizzata, giacché le modalità devono rimanere proporzionate alla natura del trattamento e al pubblico di riferimento.

2. La trasparenza come proprietà del processo

Le stesse Linee guida WP29/EDPB sulla trasparenza (WP260 01/2018) e le Linee guida EDPB 4/2019 sull'articolo 25 GDPR convergono su questa impostazione: la trasparenza va integrata tra le misure appropriate del titolare e il momento informativo deve essere progettato - per contenuti, forma, canali e tempistiche - alla luce del pubblico di riferimento e delle operazioni sui dati che rende conoscibili.

Un ulteriore rischio, ben noto a chi governa i processi informativi nel settore bancario, deriva dalla sovrapposizione di obblighi che l'ordinamento impone su piani differenti: nel medesimo rapporto, infatti, l'avviso privacy convive con documenti contrattuali, fogli informativi, comunicazioni periodiche e informative settoriali, con il risultato che l'accumulo di testi può, da un lato, soddisfare formalmente

ogni obbligo e, dall'altro, rendere difficile per il cliente capire quali passaggi richiedano attenzione immediata, sicché la soluzione non è fondere indiscriminatamente contenuti eterogenei, ma coordinarli, chiarendo quale documento disciplina le condizioni del rapporto, quale illustra il trattamento dei dati e quali facoltà possono essere esercitate in ciascun ambito, e preservando in particolare la distinzione tra consenso privacy, consenso contrattuale e diritto di opposizione, perché l'uso indistinto del termine "consenso" rischia di far credere che un unico gesto legittimi – o impedisca – fenomeni giuridici differenti.

3. Il caso BBVA: il diritto spiegato deve poter essere esercitato

Il provvedimento n. 613 del 3 settembre 2026 nei confronti di Banco Bilbao Vizcaya Argentaria Italia si colloca su un terreno diverso ma complementare, poiché riguarda l'ipotesi in cui un cliente, dopo essersi opposto alle comunicazioni commerciali tramite le impostazioni dell'app e aver ribadito la richiesta all'assistenza, abbia continuato a ricevere messaggi promozionali per circa sette mesi (da ottobre 2025 a maggio 2026).

L'istituto ha ricondotto l'anomalia a un mancato allineamento tra l'applicazione e il database *marketing*, giustificazione che il Garante ha ritenuto insufficiente, accertando violazioni degli artt. 5, par. 1, lett. a), 12, 21 e 24 GDPR e applicando una sanzione di 5.508.000 euro, anche alla luce di un precedente pertinente.

Qui, infatti, l'oggetto principale della censura non è la qualità redazionale di un'informativa pubblicata, bensì l'ineffettività concreta dell'opposizione al *marketing* e l'inadeguatezza del riscontro all'interessato, giacché l'Autorità respinge l'argomento secondo cui il cliente avrebbe dovuto utilizzare esclusivamente gli indirizzi e-mail indicati nella *privacy policy*, rilevando come l'opposizione fosse stata esercitata tramite la funzione messa a disposizione nell'app – cioè attraverso un canale reso dallo stesso titolare – e poi ribadita a un operatore che ne aveva compreso il significato, sicché una procedura interna non può trasformarsi, a posteriori, in una condizione ulteriore che restringe un diritto esercitato in modo comprensibile lungo i canali offerti dal titolare.

L'istruttoria mette poi in luce quanto sia delicata la coerenza delle risposte rese al cliente, mostrando come una comunicazione del servizio clienti, nella quale si affermava che le notifiche promozionali

in app non potevano essere rimosse e che l'interessato avrebbe potuto semplicemente ignorarle, sia stata smentita dai successivi interventi tecnici, che hanno dimostrato la possibilità di bloccarle, con la conseguenza che la descrizione del trattamento non può esaurirsi nel testo della *policy*, ma deve riflettersi anche nelle risposte operative: se il documento riconosce il diritto di opposizione ma l'interfaccia non propaga la scelta, o l'assistenza dichiara impossibile una modifica che i sistemi consentono, la promessa di controllo sull'uso dei dati resta solo apparente.

I due casi non descrivono, dunque, la medesima fattispecie, ma, letti insieme, forniscono un quadro unitario per chi governa i processi: nel primo, l'attenzione è rivolta alla conoscibilità di un trattamento inatteso e alla liceità della selezione della clientela in funzione di un'operazione di cessione; nel secondo, all'attuazione effettiva della volontà dell'interessato e all'esattezza delle informazioni rese durante l'esercizio del diritto di opposizione, a conferma che la trasparenza non termina con la consegna del documento ma prosegue nella configurazione dei canali, nella circolazione interna delle richieste e nella capacità di restituire riscontri coerenti con quanto i sistemi fanno davvero.

4. Il legal design tra metodo e responsabilità giuridica

In questa prospettiva si colloca il *White Paper* "Rendere le informative privacy più comprensibili. Il legal design come approccio rivolto all'utente", pubblicato nel 2025 dal Garante e da Creative Commons Italia, che non introduce nuovi obblighi cogenti né sostituisce le norme del GDPR, ma propone un metodo per colmare il divario tra disponibilità dell'informazione e sua effettiva comprensione.

Il *legal design* è descritto come una metodologia multidisciplinare centrata sulla persona destinataria, capace di impiegare anche codici visivi e sensoriali, e che, per il settore bancario, rileva soprattutto nella parte in cui insiste sulla verifica dell'efficacia: semplificare senza svuotare il significato giuridico, considerare le asimmetrie informative, validare il risultato mediante parametri osservabili.

Le banche, del resto, dispongono già di competenze che possono essere utilmente riutilizzate in questa direzione, poiché le disposizioni della Banca d'Italia sulla trasparenza delle operazioni e dei servizi bancari e finanziari richiedono, per i documenti cui si applicano, correttezza, completezza e comprensibilità, attenzione alla leggibilità, ordine logico delle informazioni, chiarezza lessicale e coerenza con il canale comunicativo, sicché il parallelismo con l'informativa privacy è soprattutto metodologico –

trasparenza bancaria e GDPR mantengono presupposti, oggetti e rimedi distinti - ma non impedisce di impiegare, nella progettazione delle comunicazioni sui dati, strumenti di analisi del destinatario e di verifica della comprensione già usati per i documenti bancari, a condizione di coinvolgere, accanto alle funzioni commerciali, anche le funzioni privacy, legale, operative e tecnologiche.

Una revisione efficace dovrebbe partire dal trattamento, non dalla pagina, e procedere, in primo luogo, verificando la corrispondenza tra operazione effettiva e finalità descritte - se un progetto modifica il perimetro dei dati, i ruoli o gli effetti per il cliente, l'informativa va riconsiderata prima dell'avvio - in secondo luogo valutando la base giuridica per ciascuna attività distinta, evitando di confondere la norma che facilita la cessione del rapporto con la liceità di una profilazione preliminare, e, in terzo luogo, classificando correttamente i processi automatizzati, distinguendo analisi statistiche, profilazione e decisioni rientranti nell'art. 22 e documentando quando e come l'intervento umano incide realmente sull'esito.

Segue poi la verifica del percorso informativo, rispetto al quale, per un avviso che annuncia un cambiamento rilevante, l'intermediario dovrebbe essere in grado di spiegare perché ha scelto quel canale, quella collocazione e quel momento, quale evidenza ha attribuito al messaggio e quanto tempo ha lasciato al cliente per agire, utilizzando le metriche di consegna o apertura come strumento per individuare comunicazioni che non raggiungono il pubblico atteso, ma senza confondere tali indicatori con una prova di comprensione, né equiparare una conferma di presa visione, se raccolta meccanicamente, a un consenso o a una sanatoria di un trattamento privo di base giuridica, poiché solo quando la decisione sul canale è proporzionata e la sua ragione è documentata l'*accountability* diventa verificabile senza ridursi a un esercizio di raccolta di clic.

Il punto d'arrivo che emerge da questo percorso è, quindi, più esigente di una mera revisione redazionale, ma al tempo stesso più utile per l'intermediario, poiché un'informativa ben costruita rende visibile una decisione di trattamento che la banca ha già verificato, un canale adeguato ne consente la conoscenza nel momento in cui serve, e sistemi e operatori coerenti permettono al cliente di esercitare diritti effettivi.

La trasparenza non è l'ultimo passaggio di un progetto, ma lo accompagna fin dalla scelta iniziale di

finalità e mezzi, perché solo così il linguaggio può descrivere con fedeltà ciò che l'organizzazione farà e la forma può rendere quella descrizione effettivamente accessibile.

DB non solo
diritto
bancario

A NEW DIGITAL EXPERIENCE

 **dirittobancario.it**
