

AI ACT E GDPR: SFIDE E OPPORTUNITÀ PER LE BANCHE

AUTORE: **Aldo Manzi**

Data Protection Officer – ING BANK NV Milan Branch



Milano, maggio 2025

- **Obblighi di trasparenza:**

Come coesisteranno i requisiti del **GDPR** e del **AI Act**?

- **Processo decisionale automatizzato e credit scoring:**

L'equilibrio tra **protezione dei dati personali** e **requisiti del settore finanziario**.

- **Data minimization nei sistemi di AI (anche di grandi dimensioni):**

Le sfide operative nella gestione e riduzione dei dati.

OBBLIGHI DI TRASPARENZA AI SENSI DEL GDPR E DEL AI ACT: COME COESISTERANNO

Principali obblighi di trasparenza ai sensi dell'articolo 50 del AI ACT

Gli obblighi di trasparenza mirano a garantire un **utilizzo etico e responsabile** dell'IA, evitando inganni o manipolazioni

ARTICOLO 50 AI ACT



I sistemi AI siano progettati in modo che gli esseri umani comprendano che stanno interagendo con un sistema AI. A meno che ciò non sia ovvio dal punto di vista di una persona ragionevolmente ben informata. Si applica solo ad AI che interagiscono direttamente con persone fisiche (es. chatbot). L'obbligo non si applica ad alcuni sistemi autorizzati dalla legge.

I sistemi AI che generano contenuti sintetici (testo, audio, immagine, ecc.) devono garantire che l'output sia contrassegnato in un formato leggibile da una macchina. Ad esempio, i falsi devono essere contrassegnati come «generati AI» utilizzando soluzioni tecniche adeguate (ad esempio la marcatura digitale). Tale obbligo non si applica se i sistemi forniscono solo assistenza per l'editing standard o non modificano sostanzialmente i dati di input, nonché alcuni sistemi autorizzati dalla legge.



Chi utilizza un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica devono informare le persone fisiche del funzionamento e del trattamento dei dati personali da parte del sistema conformemente alla legislazione sulla protezione dei dati (GDPR, regolamento 2018/1725 e direttiva sulle attività di contrasto). Analogamente a quanto sopra, l'obbligo non si applica ai sistemi autorizzati dalla legge.



Deepfake e Contenuti Sintetici Audio, immagini, video o testi generati da IA devono essere chiaramente identificati come artificialmente prodotti. In tal senso si deve informare che il contenuto è stato generato o manipolato artificialmente. Tali obblighi non si applicano ai sistemi autorizzati dalla legge. Inoltre, se la produzione è un'opera evidentemente artistica, gli obblighi di trasparenza impongono di divulgare il contenuto generato artificialmente in modo da non ostacolarne l'apprendimento.

I sistemi AI che generano o manipolano contenuti testuali, che hanno lo scopo di informare il pubblico su questioni di interesse pubblico, devono rivelare che il testo è stato generato o manipolato artificialmente. Tali obblighi non si applicano ai sistemi AI autorizzati dalla legge. Inoltre, devono informare se il contenuto generato dall'AI è sotto la supervisione umana o una supervisione editoriale.

La **Commissione** elaborerà **orientamenti sull'attuazione pratica degli obblighi di trasparenza** di cui sopra. L'inadempienza sarà soggetta a **un'ammenda** fino a un massimo di **EUR 15M o del 3%** del fatturato mondiale, se superiore.

OBBLIGHI DI TRASPARENZA AI SENSI DEL GDPR E DEL AI ACT: COME COESISTERANNO

Altri obblighi di trasparenza ai sensi della legge AI



RECITAL 27

Tutti i sistemi devono essere sviluppati e utilizzati in modo da garantire la tracciabilità.

Tutti i sistemi devono essere progettati in modo da garantire che gli individui sappiano che stanno interagendo con un sistema AI.

Gli operatori dei sistemi devono essere informati delle capacità e dei limiti del sistema AI.



RECITAL 53

I fornitori che considerano il loro sistema AI non ad alto rischio devono fornire una valutazione prima che tale sistema sia diffuso sul mercato.

In questi casi, i fornitori devono anche garantire che la documentazione di tale valutazione sia disponibile, su richiesta, alle autorità nazionali.

Tali fornitori devono registrare il loro sistema nella banca dati dell'UE istituita ai sensi del AI Act.



RECITAL 59

Garantire la trasparenza dei sistemi AI previene gli impatti negativi e mantiene la fiducia del pubblico nei confronti dell'AI.

La trasparenza garantisce la responsabilità e consente un uso efficace.

Tutti i sistemi devono essere concepiti in modo da rispettare i diritti fondamentali, tra cui la non discriminazione, la protezione dei dati personali ed una corretta amministrazione.



RECITAL 72

I sistemi AI ad alto rischio devono essere progettati in modo tale che gli operatori siano in grado di comprendere come funziona il sistema e di comprenderne quindi capacità e limiti.

I fornitori devono garantire che tutta la documentazione comprenda istruzioni per l'uso e contenga informazioni complete in un linguaggio facilmente comprensibile per i destinatari.

Tali obblighi sono richiesti prima della diffusione sul mercato del sistema AI.



RECITAL 102-103

I fornitori di servizi di modelli AI devono redigere un'adeguata documentazione tecnica che deve essere messa a disposizione dei dipartimenti AI e delle autorità competenti.

La documentazione comprende una descrizione generale del modello AI, nonché gli elementi del modello (scopo del sistema, rischi, capacità tecniche, ecc.).

I requisiti specifici per tale documentazione sono elencati nell'allegato XXII del AI ACT.

OBBLIGHI DI TRASPARENZA AI SENSI DEL GDPR E DEL AI ACT: COME COESISTERANNO

Obblighi di trasparenza ai sensi del GDPR

Il regolamento generale sulla protezione dei dati prevede che il trattamento dei dati personali sia **lecito, equo e trasparente** (articolo 12).

Informare gli interessati

Lo scopo esatto del trattamento (il "perché") e come i loro dati vengono raccolti, utilizzati o trattati in qualsiasi altro modo

In che misura sono trattati (i dati devono essere adeguati, pertinenti e limitati allo scopo)

Identità del responsabile del trattamento

I rischi di tale trattamento

i diritti degli interessati

Caratteristiche dell'Informativa

Concisa, facilmente accessibile e facilmente comprensibile;

Scritta in un linguaggio chiaro e semplice, soprattutto se è diretto a un bambino (la visualizzazione è una mezzo consentito)

Le informazioni sul trattamento possono essere fornite in forma elettronica (ad esempio tramite un sito web)

Il GDPR ha introdotto alcuni **meccanismi di certificazione** per la protezione dei dati che possono essere utilizzati come elemento per **dimostrare il rispetto degli obblighi di trasparenza** e di **altri principi di protezione dei dati**. **L'inosservanza** degli obblighi di trasparenza (di cui all'articolo 12) può comportare **un'ammenda** fino a **20 milioni di EUR** o il **4% del fatturato mondiale**, se superiore.

OBBLIGHI DI TRASPARENZA AI SENSI DEL GDPR E DEL AI ACT: COME COESISTERANNO

Recenti ammende per gli obblighi di trasparenza

04/01/2023

La commissione irlandese per la protezione dei dati ha inflitto un'ammenda a Meta per violazione del principio di trasparenza:

Meta ha violato il principio di trasparenza utilizzando avvisi sulla privacy a più livelli.

Gli utenti per leggere e accettare le condizioni d'uso sono stati guidati attraverso una serie di contenuti collegati ad altri contenuti. Tale avviso stratificato non è conciso, chiaro e completo come richiesto dal principio di trasparenza. Il livello di specificità richiesto non è stato raggiunto.

La DPA irlandese ha imposto 390 milioni di euro ai servizi Meta (210 milioni di euro contro Facebook, 180 milioni di euro contro Instagram).

16/05/2024

L'autorità olandese per la protezione dei dati ha imposto un'ammenda a ClearviewAI per il mancato rispetto dei requisiti di trasparenza nei confronti delle persone che si trovano nella banca dati Clearview. L'azienda non avrebbe mai dovuto creare un database contenente foto di persone con codici biometrici univoci.

Le persone i cui dati sono stati raccolti nella banca dati non sono state sufficientemente informate del fatto che le loro foto e i loro dati biometrici sono memorizzati nella banca dati Clearview.

La DPA olandese ha imposto una multa di 30,5 M EUR e ha ordinato di porre fine alle violazioni.

02/11/2024

Il Garante per la protezione dei dati personali ha inflitto un'ammenda all'Open AI per il trattamento di dati personali senza base giuridica per formare ChatGPT e violando il principio di trasparenza e gli obblighi di informazione nei confronti degli utenti.

OpenAI dovrà pagare EUR 15M. Inoltre, condurre una campagna di informazione che dovrebbe promuovere la comprensione e la consapevolezza del funzionamento di ChatGPT, concentrandosi in particolare sulla raccolta di dati a fini di formazione.

A partire dal 21 marzo 2025, la decisione è stata temporaneamente sospesa a condizione che siano fornite garanzie.

OBBLIGHI DI TRASPARENZA AI SENSI DEL GDPR E DEL AI ACT: COME COESISTERANNO

Come possono coesistere la trasparenza del GDPR e gli obblighi di trasparenza della AI?

TRASPARENZA AI ACT

Si concentra sui sistemi AI, compreso il modello dell'AI ad alto rischio. Copre sia i fornitori che gli operatori di tali sistemi.

Si concentra sulla garanzia che gli individui capiscano che stanno interagendo con AI.

Richiede un'etichettatura adeguata se un contenuto viene generato o manipolato da un AI.

Richiede una documentazione tecnica in un linguaggio chiaro che spieghi lo scopo dei sistemi AI, le loro capacità, i rischi e le limitazioni.

La violazione degli obblighi di trasparenza può comportare un'ammenda fino a 15 milioni di euro, pari al 3% del fatturato annuo mondiale.

Ambito

Scopo

Requisiti principali

Ammende

TRASPARENZA GDPR

Si concentra sul trattamento dei dati personali delle persone fisiche, introducendo obblighi di trasparenza per i Titolari del trattamento e per i Responsabili del trattamento.

Si concentra sulla garanzia che le persone comprendano perché e come i loro dati personali vengono trattati.

Richiede che le informazioni sul trattamento siano fornite alle persone in modo conciso, accessibile e scritto in un linguaggio semplice.

Richiede che le persone siano sui propri diritti e che tali diritti siano adeguati in modo da avere un maggiore controllo sui dati personali trattati.

La violazione degli obblighi di trasparenza può comportare un'ammenda fino a 20 milioni di euro, pari al 4% del fatturato annuo mondiale.

PROCESSO DECISIONALE AUTOMATIZZATO E VALUTAZIONE DEL MERITO DI CREDITO

CJEU Causa C-634/21

Nella causa C-634/21, OQ vs. CRIF GmbH (SCHUFA), la CJEU ha esaminato se il punteggio di credito costituisca un processo decisionale automatizzato ai sensi dell'articolo 22 del GDPR.

Ha esaminato se le persone fisiche abbiano diritto alla trasparenza e alla contestabilità quando sono sottoposte a decisioni di valutazione del merito di credito.

La CJEU ha ritenuto che il credit scoring possa essere una decisione esclusivamente automatizzata con effetti significativi ai sensi dell'articolo 22 del regolamento generale sulla protezione dei dati.

BACKGROUND

L'uso di un punteggio di merito creditizio nella concessione o nel rifiuto di credito costituisce una decisione che incide significativamente sulle persone.

I soggetti che fanno affidamento su tali punteggi devono garantire il rispetto delle salvaguardie del GDPR, tra cui trasparenza, equità e diritto di contestare le decisioni.

RISULTATI CHIAVE

Rafforza l'interpretazione secondo cui il credit scoring richiede una supervisione e una spiegazione umana.

Costituisce un precedente giudiziario che sottolinea l'importanza dell'articolo 22 del regolamento generale sulla protezione dei dati nel processo decisionale finanziario.

Incoraggia una più rigorosa aderenza agli obblighi del GDPR quando si implementa l'ADM nei mercati del credito.

Getta le basi per l'interpretazione delle pratiche di valutazione del credito ai sensi del AI ACT

IMPATTO

PROCESSO DECISIONALE AUTOMATIZZATO E VALUTAZIONE DEL MERITO DI CREDITO

GDPR & AI ACT Obblighi nel Credit Scoring

Sia il GDPR che l'AI ACT impongono obblighi agli utenti dei sistemi che comportano un processo decisionale automatizzato in relazione al punteggio di credito.

Ai sensi della GDPR

Articolo 22 GDPR: Gli individui hanno il diritto di non essere soggetti a decisioni basate esclusivamente sul trattamento automatizzato, compresa la profilazione, se tali decisioni producono effetti legali o similmente significativi.

Considerando 71 del GDPR: sottolinea la necessità di garanzie adeguate, tra cui il diritto di ottenere l'intervento umano, esprimere il proprio punto di vista e contestare la decisione.

Gli obblighi comprendono:

Fornire informazioni significative sulla logica in questione.

Garantire l'accuratezza dei dati e la pertinenza dei modelli di punteggio.

Rispettare i principi di minimizzazione dei dati e di limitazione delle finalità.

Ai sensi della legge AI

Credit Scoring = AI ad alto rischio (allegato III e articolo 6): i sistemi utilizzati per valutare il merito di credito delle persone sono classificati come ad alto rischio.

Ciò comporta obblighi rigorosi per i fornitori e gli utenti, tra cui:

Articolo 9: Attuare e documentare un sistema di gestione dei rischi durante l'intero ciclo di vita dell'AI.

Articolo 10: Garantire serie di dati di elevata qualità, rappresentative e con attenuazione degli errori sistematici.

Articolo 13: Fornire agli utenti informazioni chiare e comprensibili sulle capacità e sui limiti del sistema.

Articolo 14: Istituire meccanismi di controllo umano per prevenire o ridurre al minimo i rischi.

Articolo 17: Mantenere un sistema di monitoraggio post-commercializzazione per monitorare le prestazioni e la conformità del sistema nel tempo.

Ai sensi del regolamento generale sulla protezione dei dati, le violazioni delle disposizioni relative al processo decisionale automatizzato possono comportare ammende fino a **20 milioni di EUR** o al **4% del fatturato annuale globale** - ai sensi del AI ACT, le violazioni degli obblighi per i sistemi ad alto rischio possono comportare ammende fino a **35 milioni di EUR** o al **7% del fatturato globale**. Queste sanzioni mirano a garantire che i sistemi di IA ad alto rischio rispettino le normative sulla sicurezza, trasparenza e protezione dei diritti fondamentali.

PROCESSO DECISIONALE AUTOMATIZZATO E VALUTAZIONE DEL MERITO DI CREDITO

Interazione tra GDPR e AI ACT

Obiettivi condivisi

Entrambi i regolamenti pongono l'accento sulla trasparenza, l'equità, la responsabilità, e la supervisione umana nelle decisioni di credito guidate da AI.

Stabiliscono obblighi complementari che garantiscono che le persone siano protette da decisioni automatizzate inique o poco trasparenti.

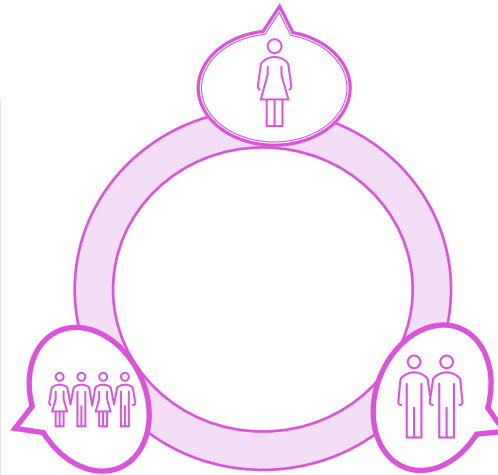
Impatto sul credit scoring compliance

Le istituzioni finanziarie e gli sviluppatori di AI devono conformarsi sia con il GDPR che con l'AI ACT.

Il diritto alla spiegazione (articolo 22 del GDPR) è in linea con i requisiti di trasparenza del AI ACT (articolo 13), richiedendo che i modelli di valutazione del credito siano interpretabili.

Le disposizioni in materia di controllo umano contenute nel GDPR (articolo 22, paragrafo 3) sono rafforzate dall'intervento umano conferito dal AI ACT (articolo 14 della legge AI).

Tutti gli sviluppatori devono garantire che i modelli di credit scoring siano spiegabili, imparziali, e continuamente monitorati per prevenire discriminazioni e violazioni normative.



Differenze chiave

GDPR (Data Protection Focus):

Tutela i diritti individuali relativi al trattamento dei dati personali e al processo decisionale automatizzato.

Stabilisce diritti quali spiegazione, contenzibilità, e intervento umano.

AI ACT (AI System Governance Focus):

- Introduce un quadro basato sul rischio per regolamentare le applicazioni di AI in base al loro impatto sociale.
- Richiede garanzie tecniche ed operative per i sistemi di AI ad alto rischio oltre alla protezione dei dati (ad esempio, gestione del rischio, prove di robustezza, documentazione di conformità).

MINIMIZZAZIONE DEI DATI NEL CONTESTO DEI SISTEMI DI IA

Le basi della minimizzazione dei dati



PRINCIPIO DI MINIMIZZAZIONE DEI DATI

Che cos'è?

L'articolo 5, paragrafo 1, lettera c), del GDPR definisce la minimizzazione dei dati come un principio che richiede che i dati personali siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità del trattamento.

Perché è importante?

La minimizzazione dei dati è strettamente collegata al principio della limitazione delle finalità. È necessario uno scopo chiaramente definito per determinare quali dati personali siano necessari per lo scopo. La riduzione al minimo dei dati è uno dei requisiti della privacy by design e by default. Ciò significa che i responsabili del trattamento devono attuare misure tecniche e organizzative adeguate per garantire che vengano trattati solo i dati personali necessari.

Sentenze recenti:

- 4 ottobre 2024, la CJUE ha deciso che Meta dovrebbe limitare l'uso dei dati personali per la pubblicità online e limitare l'uso dei dati disponibili al pubblico al loro scopo originario.
- 9 gennaio 2025, CJUE C-394/23 - la raccolta di dati personali relativi ai titoli dei clienti ("Mr", "Ms") non è obiettivamente indispensabile quando si acquistano biglietti di trasporto online.



CHALLENGES IN AI

Tutti i modelli richiedono grandi quantità di dati per ottenere prestazioni adeguate.

La limitazione dei dataset può ridurre le prestazioni previste.

È inoltre alquanto difficile definire quali siano i dati minimi necessari per le prestazioni di un modello AI. Gli sviluppatori AI spesso non sanno quali dati saranno richiesti in anticipo per le prestazioni corrette di un modello AI.

Se la minimizzazione dei dati non viene implementata correttamente, i modelli AI possono creare output imprecisi (mancanza di diversità che porta a risultati o decisioni di parte).

L'infrastruttura per i grandi sistemi AI è spesso distribuita su più server. La pulizia di questi server per mantenere la minimizzazione dei dati richiede molte risorse.

MINIMIZZAZIONE DEI DATI NEL CONTESTO DEI SISTEMI DI IA

La maggior parte dei sistemi AI utilizzati al giorno d'oggi si basano su **modelli di apprendimento automatico**, noto anche con l'inglese **Large Language Model**.

Un modello di apprendimento automatico che utilizza i dati in due fasi principali.

Durante la fase di addestramento

Il modello è dotato di un dataset di grandi dimensioni contenenti elementi di input e output.

Il modello impara da questi dati per creare schemi.

Non appena il modello raggiunge il livello previsto, la fase di addestramento si completa e si passa alla fase di inferenza.

Fase di Inferenza

Al termine della fase di addestramento, il modello addestrato effettua previsioni sulla base di nuovi set di dati (dati invisibili).

In questa fase il modello fa previsioni o classificazioni basate sui nuovi dati alimentati.

La fase di inferenza è utilizzata per il riconoscimento facciale, la traduzione di testi o l'individuazione di transazioni fraudolente.

MINIMIZZAZIONE DEI DATI NEL CONTESTO DEI SISTEMI DI IA

Per affrontare le **sfide della minimizzazione dei** dati nei grandi sistemi di AI, esistono alcune **soluzioni innovative** che possono essere utili per garantire la tutela della vita privata e al contempo rispettare le prestazioni attese dai sistemi AI.

1

L'apprendimento federato addestra i modelli AI su dispositivi decentralizzati (ad esempio, dispositivi degli utenti quali smartphone, laptop, ecc.).

I dati vengono conservati localmente su un dispositivo personale, quindi ogni utente sta addestrando i modelli sui propri dati senza inviarli all'esterno.

La tastiera di Google utilizzava l'apprendimento federato per suggerire le parole durante la digitazione. I dati inviati ai server di Google non contengono dati personali, ma i cosiddetti gradienti (ad esempio dopo "hey" l'utente di solito scrive «There»).

2

La perturbazione consiste nell'aggiungere "rumore" controllato ai dati per nascondere elementi che possono essere considerati dati personali.

Ad esempio, sfocando i volti di una foto, mantenendo lo sfondo riconoscibile allo stesso tempo. Un altro esempio di perturbazione è quello di evitare di dare informazioni esatte, ad esempio se un sistema AI tiene traccia delle vostre operazioni al giorno, riceve dati come "l'utente fa 5-10 operazioni al giorno" invece di fornire il numero esatto.

3

In alcuni casi, un modello AI può essere sviluppato utilizzando dati sintetici. Comporta la generazione di dataset falsi ma realistici per imitare i modelli del mondo reale.

Ad esempio, un fondo raccoglie 1000 transazioni azionarie di persone reali e sulla base di questo crea 100.000 operazioni sintetiche. Permette di preservare le tendenze principali, come le fluttuazioni dei prezzi, mantenendo allo stesso tempo la protezione dei dati.

- Entrambe le normative puntano a garantire chiarezza e tutela per gli utenti.
- Il GDPR si concentra sulla protezione dei dati personali, mentre l'AI Act regola l'uso responsabile dell'IA. Entrambe le norme mirano a tutelare l'individuo ed a prevenire bias discriminatori.
- Le istituzioni finanziarie dovranno integrare le due normative per garantire conformità e fiducia nei propri sistemi digitali.

Queste normative e regole applicative che verranno rappresentano una sfida, ma anche un'opportunità per il settore Bancario e Finanziario di distinguersi per etica e innovazione

PIANO ISPETTIVO AUTORITY' GARANTE FOCUS SU CONFORMITA' C.D. PROVVEDIMENTO «GARANTE 2»

AUTORE: **Aldo Manzi**

Data Protection Officer – ING BANK NV Milan Branch



Milano, maggio 2025

Il piano ispettivo del primo semestre 2025

- Aree di interesse dell'Autorità;
- Ispezioni privacy: come prepararsi;
- Conformità al Provvedimento recante «Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie» c.d. Garante 2;
 - Il caso Banca Intesa e Unicredit.

Il **Garante privacy** nei primi mesi dell'anno ha pubblicato il **piano ispettivo per il primo semestre 2025**, con cui sono stati confermati i principali ambiti di intervento dell'Autorità:

- **protezione delle banche dati pubbliche,**
- **trattamento dei dati personali** nelle banche e negli istituti di credito,
- **gestione dei dati biometrici** e nelle scuole,
- **cookie e tracciamento online.**

LE AREE DI INTERESSE PER IL SETTORE BANCARIO

Tra i settori che si pongono in continuità con gli accertamenti già avviati e di maggior interesse per il settore bancario finanziario, si evidenziano:

- il **trattamento dei dati nelle banche e negli istituti di credito**. Proseguiranno gli accertamenti sui sistemi di trattamento dei dati personali nelle **banche e negli istituti di credito**, con particolare attenzione alle **violazioni dei dati personali** che sono state notificate al Garante. In tale ambito verranno esaminati i sistemi di rilevamento delle violazioni, nonché le **misure adottate per prevenire le violazioni e le misure adottate per evitare il ripetersi della violazione**.
- i sistemi di **cookie di profilazione e tracciamento online**. Proseguiranno anche le verifiche sull'utilizzo dei cookie di profilazione, con particolare attenzione all'utilizzo dei cookie di profilazione e a pratiche di tracciamento non conformi alla normativa, in linea con le linee guida del 10 giugno 2021. Tale attività di ispezione può essere condotta anche da remoto con successiva richiesta di chiarimenti.

Complessivamente sono già in corso **circa 40 accertamenti ispettivi**, svolti anche con il supporto del Nucleo Speciale Privacy della Guardia di Finanza. Questi ambiti sono stati individuati in continuità con le attività ispettive precedenti, l'Autorità infatti intende proseguire il monitoraggio e rafforzare il controllo in tali ambiti.

ISPEZIONI PRIVACY: COME PREPARARSI

Le Banche dovranno rafforzare le **politiche di protezione dei dati**, aggiornando regolarmente le **misure di sicurezza** per garantire la **conformità alla normativa**.

È fondamentale essere in grado di **dimostrare la conformità** alla normativa tra cui il **rispetto dell'obbligo informativo** nei confronti dell'Interessato e la **corretta gestione dei consensi** nonché l'adozione di **misure tecniche** per la protezione dei dati in **ogni fase di trattamento**.

In caso di **segnalazioni o reclami** da parte degli Interessati, sarà essenziale una **pronta risposta** e la **disponibilità a collaborare** con l'Autorità per garantire la protezione dei diritti degli interessati.

Il **DPO** della Banca deve essere presente durante l'attività di accertamento per supportare la Banca nella raccolta e presentazione della documentazione richiesta e per rispondere tempestivamente alle richieste del Garante. In particolare:

1. Registro delle attività di trattamento (**ROPA**);
2. Valutazioni di impatto sulla protezione dei dati (**DPIA**) e altri assesment (**TIA, LIA e FRIA**), tutte le analisi dei rischi devono essere state condotte e documentate correttamente.;
3. Contratti con i **responsabili del trattamento** (ai sensi dell'art. 28 del GDPR);
4. **Politiche e procedure interne** di protezione dei dati;
5. **Informative** e relativi **moduli di consenso** degli utenti,

FOCUS SU CONFORMITA' C.D. PROVVEDIMENTO «GARANTE 2»

AUTORE: **Aldo Manzi**

Data Protection Officer – ING BANK NV Milan Branch



Milano, maggio 2025

IL CASO DI SPIONAGGIO BANCARIO

Negli ultimi mesi del 2024, il panorama bancario italiano è stato scosso da una serie di episodi inquietanti riguardanti l'accesso non autorizzato ai dati sensibili dei clienti presso due dei maggiori istituti di credito del paese: Intesa Sanpaolo e Unicredit.



Le inchieste giornalistiche hanno rivelato come dipendenti infedeli abbiano effettuato accessi impropri ai conti correnti di personalità di spicco, politici e VIP, senza alcuna necessità operativa legittima. Questi episodi hanno sollevato gravi preoccupazioni sulla sicurezza delle informazioni personali e finanziarie dei correntisti.

L'Autorità Garante per la Protezione dei Dati Personali e la Procura della Repubblica competente sono intervenute prontamente, avviando indagini approfondite su questi casi che hanno minato la fiducia dei clienti nel sistema bancario italiano.

CORTE DI CASSAZIONE: LICENZIAMENTO DIPENDENTE UNICREDIT

La Corte di Cassazione ha emesso una sentenza definitiva contro il dipendente di Unicredit. L'impiegato spiava i conti correnti dei clienti.

Questa violazione ha compromesso il rapporto fiduciario. La protezione della privacy bancaria è stata considerata fondamentale.



E' stata confermata la legittimità del licenziamento per giusta causa del dipendente che viola le policy della Banca e effettua diversi accessi non legittimi ai dati bancari della clientela della Banca stessa.

Il caso riguardava il licenziamento di un area manager di un importante istituto bancario (Unicredit S.p.A.), licenziato dopo oltre 70 accessi non autorizzati ai dati di clienti, senza alcuna ragione lavorativa e senza arrecare alcun danno patrimoniale alla Banca (“assenza di effettive conseguenze pregiudizievoli per il datore di lavoro”).

L'ordinanza n. 4945/2025 della Corte di Cassazione, emessa il 25 febbraio u.s., affronta dunque un tema cruciale legato alla violazione della privacy dei clienti da parte di un dipendente mediante accesso non autorizzato a dati bancari per scopi estranei all'attività lavorativa, sottolineando la gravità di tale condotta.

ANALISI DEL PROVVEDIMENTO DELL'AUTORITÀ GARANTE

Il Garante per la Protezione dei Dati Personali ha emesso un provvedimento specifico a seguito dei casi di violazione emersi, richiamando gli istituti bancari al rispetto rigoroso del GDPR e della normativa nazionale sulla privacy e obbligandoli ad informare anche i singoli Interessati.

Il provvedimento sottolinea l'obbligo delle banche di implementare misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio, con particolare attenzione alla protezione dei dati finanziari.

Provvedimento del Garante relativo a prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011 n. 192

REQUISITO NORMATIVO	RIFERIMENTO LEGISLATIVO	•SANZIONI PREVISTE
Sicurezza del trattamento	Art. 32 GDPR	Fino a 20 milioni € o 4% fatturato* del Gruppo
Registro delle attività	Art. 30 GDPR	Fino a 20 milioni € o 4% fatturato* del Gruppo
Notifica violazioni	Art. 33 GDPR	Fino a 20 milioni € o 4% fatturato* del Gruppo
Valutazione d'impatto	Art. 35 GDPR	Fino a 20 milioni € o 4% fatturato* del Gruppo

* Si applica la sanzione con il maggior effetto deterrente oltre alla sanzione è necessario calcolare il danno reputazionale

MISURE TECNICHE E ORGANIZZATIVE PER LA TRACCIATURA DEGLI ACCESSI



Autenticazione Multifattoriale

Implementazione di sistemi MFA per l'accesso ai dati sensibili dei clienti, richiedendo più fattori di verifica dell'identità degli operatori.



Segregazione dei Dati

Limitazione degli accessi in base al principio del "need-to-know", garantendo che ogni dipendente possa visualizzare solo i dati necessari per le proprie mansioni.



Log di Controllo Avanzati

Registrazione dettagliata di ogni accesso ai dati dei clienti, con informazioni su chi ha effettuato l'accesso, quando, da quale postazione e per quale motivo operativo.

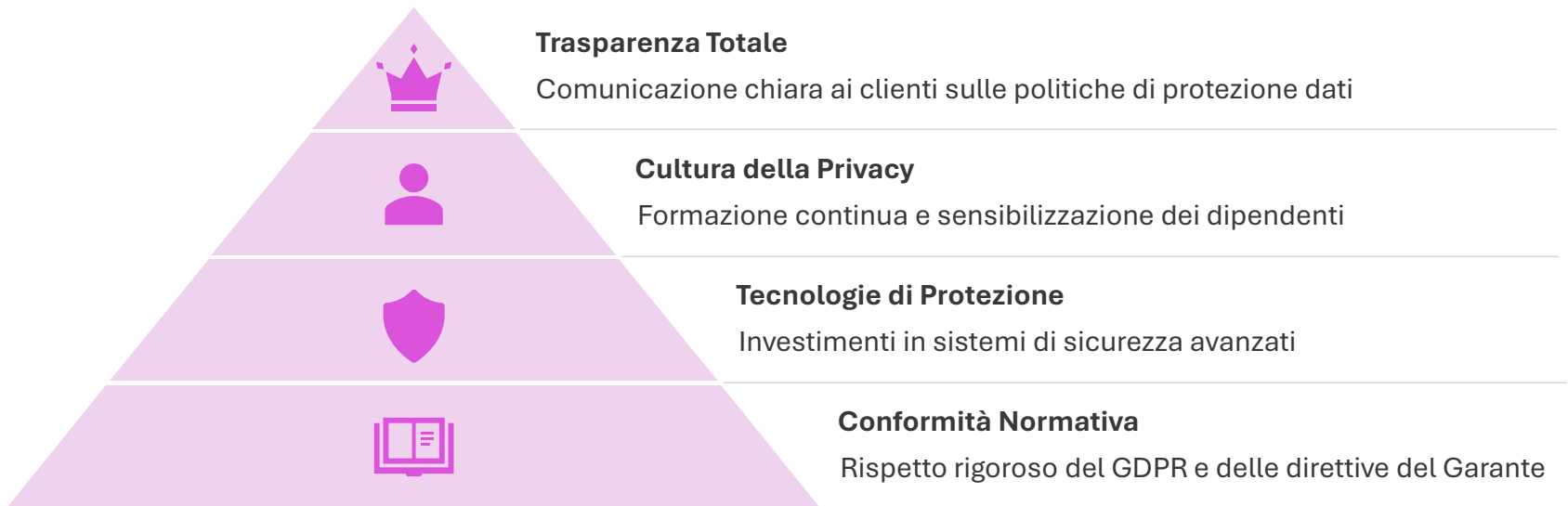


Sistemi di Allerta in Tempo Reale

Monitoraggio continuo che segnala automaticamente comportamenti anomali o accessi sospetti, attivando immediati controlli di sicurezza.

L'Autorità Garante ha specificato che queste misure devono essere oggetto di revisioni periodiche e test di efficacia, con particolare attenzione alla formazione continua e sensibilizzazione del personale sulle politiche di riservatezza e sicurezza dei dati.

IMPLICAZIONI FUTURE E BEST PRACTICE



Le banche che operano in Italia devono adottare un approccio proattivo alla protezione dei dati, anticipando i rischi e implementando soluzioni che vadano oltre la semplice conformità normativa. Questo rappresenta non solo un obbligo legale, ma un vantaggio competitivo in un mercato dove la fiducia dei clienti è fondamentale.





CONSILIA BUSINESS MANAGEMENT S.r.l.

• Corso Europa, 13 – 20122 Milano

• **TEL:** +39 02 873 89 370 | **Fax:** +39 02 873 89 371

• **Sito web:** www.consiliabm.com

• **MAIL:** segreteria@consiliabm.com

info@consiliabm.com