Relazione del Responsabile della Protezione dei Dati

Anno 2025

Roma, Maggio 2026

BANCA D'ITALIA
EUROSISTEMA

INDICE

1. Quadro d'insieme

L'azione di sorveglianza e consulenza sull'applicazione del GDPR da parte del Responsabile della Protezione dei Dati (RPD) si colloca all'interno di un quadro caratterizzato da crescente complessità delle normative applicabili e dalla pervasività dell'evoluzione tecnologica, anche sostenuta dalla diffusione di applicativi basati sull'intelligenza artificiale.

L'intensificarsi della produzione normativa europea nei diversi settori legati al trattamento e alla diffusione dei dati personali e delle tecnologie digitali ha comportato un aumento del livello di complessità e il rischio di sovrapposizioni e incoerenze che, oltre a essere fonte di incertezze applicative e di maggiore onerosità amministrativa, sono suscettibili, soprattutto nello sviluppo di sistemi di intelligenza artificiale, di portare a una perdita di competitività delle imprese europee a vantaggio degli operatori extra UE. Per far fronte a questa situazione è stata promossa, a livello europeo, un'azione di semplificazione normativa.

In questo contesto, l'azione del RPD è stata orientata a promuovere momenti di confronto con l'esterno al fine di favorire il continuo allineamento della Banca con le indicazioni dell'Autorità Garante e con le migliori pratiche emergenti a livello nazionale ed europeo. E' stato rafforzato il ruolo di interfaccia stabile e qualificata con le altre Istituzioni grazie alla partecipazione del RPD alle sedi di cooperazione con il Garante della Privacy, rispettivamente in ambito bancario e assicurativo, nonché alle riunioni dei Network dei RPD nazionali ed europei.

Allo stesso tempo, all'interno dell'Istituto, sono stati intensificati il dialogo e le occasioni di coordinamento con le Strutture in modo da anticipare, il più possibile, il momento della valutazione degli impatti per la *privacy* e delle relative misure di mitigazione dei rischi all'interno dei progetti che trattano dati personali.

Infine, in un contesto nel quale la maggiore esposizione degli individui a una raccolta massiva e automatizzata di informazioni personali trasforma le persone nel principale vettore d'attacco delle minacce cyber, è stata promossa un'azione di sensibilizzazione a favore del personale volta ad accrescere stabilmente la consapevolezza sui rischi connessi al trattamento dei dati personali, consolidare una cultura diffusa della protezione della riservatezza delle informazioni e favorire comportamenti sempre attenti, responsabili e coerenti con le misure di sicurezza previste.

2. Evoluzione del quadro normativo

Il 19 novembre 2025, la Commissione Europea ha presentato un disegno regolamentare denominato "*Digital Omnibus*", comprensivo di 3 proposte di regolamento, con l'obiettivo di razionalizzare e semplificare le regole dell'Unione su circolazione dati e tecnologie digitali[1]. La proposta interviene anche sulle disposizioni del GDPR, con l'obiettivo di semplificarne alcuni aspetti sulla base delle problematiche applicative emerse nei sette anni dalla sua entrata in vigore[2] nonché di tener conto degli aspetti legati all'applicazione del Regolamento (UE) 2024/1689 sull'intelligenza artificiale (*AI Act*).

Sul versante nazionale, il 10 ottobre 2025 è entrata in vigore la legge sull'intelligenza artificiale (legge 23 settembre 2025 n. 132), volta ad armonizzare l'ordinamento nazionale alle disposizioni dell'*AI Act*, individuando in particolare specifici presidi per l'utilizzo delle nuove tecnologie nel settore delle pubbliche amministrazioni, con l'obiettivo di coniugare le opportunità offerte dai nuovi strumenti innovativi con l'elevato livello di garanzia da assicurare ai diritti e alle libertà fondamentali dei cittadini.

Nel corpo della normativa in esame, sono state designate Autorità nazionali per l'intelligenza artificiale sia l'Agenzia per l'Italia digitale (AgID), con finalità di promozione dello sviluppo, che l'Agenzia per la cybersicurezza nazionale (ACN), con compiti di supervisione e sanzionatori. Il ruolo di autorità di vigilanza del mercato è stato invece attribuito, ciascuna per i profili di competenza, alla Banca d'Italia, alla Consob e all'IVASS.

Infine si segnala che, a seguito della recente modifica[3] della legge 7 dicembre 2023 n. 193 in tema di parità di trattamento, non discriminazione e garanzia del diritto all'oblio delle persone guarite da patologie oncologiche, la Banca d'Italia e la Consob, nelle materie di rispettiva competenza, saranno chiamate a dettare le disposizioni attuative della legge con riferimento alle operazioni, alla stipulazione o al rinnovo di contratti relativi a servizi bancari, finanziari e di investimento.

---

[1] Il documento "European data union strategy" individua tre aree d'intervento: ampliare l'accesso ai dati per l'intelligenza artificiale; semplificare le norme in materia di dati; salvaguardare la sovranità dell'UE sui dati per rafforzarne la posizione globale.

[2] In sintesi, le principali modifiche riguarderanno:

- la ridefinizione del concetto di dato personale, escludendone la ricorrenza quando la persona interessata non possa ragionevolmente essere identificata da altro soggetto giuridico in base ai mezzi da questo posseduti; corrispondentemente verrebbero ridefiniti i requisiti minimi della pseudonimizzazione;
- l'ampliamento dei casi di esenzione dall'obbligo di informativa;
- la previsione di modalità uniformi per lo svolgimento delle valutazioni di impatto sulla protezione dei dati, sotto il coordinamento dell'European Data Protection Board (EDPB);
- l'armonizzazione della segnalazione di data breach limitata al solo pericolo di alto rischio per gli interessati (tipizzata con provvedimento della Commissione UE) da effettuarsi in un termine poco più ampio (96 ore anziché 72);
- la possibilità di trattare dati personali per sviluppare sistemi di intelligenza artificiale sulla base del legittimo interesse del Titolare del trattamento.

[3] D. Lgs. 31 dicembre 2025, n. 212, artt. 3 e 6. Le nuove norme affidano alle due istituzioni anche la vigilanza sull'applicazione delle disposizioni adottate nell'ambito dei rispettivi ordinamenti.

3. L'azione del Responsabile Protezione Dati

Nel corso del 2025 l'azione del RPD si è svolta nel quadro degli orientamenti espressi dal Garante della Protezione dei Dati Personali a livello nazionale e dall'European Data Protection Board (EDPB) a livello europeo. Sono stati anche tenuti in considerazione i risultati degli approfondimenti svolti all'interno di consessi istituzionali ai quali il RPD partecipa quale rappresentante dell'Istituto: Network Data Protection Officers (DPO) del Sistema Europeo Banche Centrali (SEBC) e del Single Supervisory Mechanism (SSM), Rete nazionale dei RPD delle Authority, Sedi di cooperazione con l'Autorità Garante della Protezione dei Dati Personali per il settore bancario e per quello assicurativo (cfr. infra par. 3.1, 3.2, 3.3).

La funzione di sorveglianza e consulenza è stata orientata a rafforzare in modo sostanziale i livelli di *compliance* e *accountability*. In particolare, sono stati ampliati i canali di coordinamento e le occasioni di interlocuzione con le Strutture della Banca con l'obiettivo di anticipare sempre di più il coinvolgimento del RPD nei progetti con impatti su dati personali, così da garantire valutazioni tempestive e integrate sui trattamenti e mitigare i rischi prima della messa in esercizio. La capacità di "*giocare d'anticipo*", soprattutto con riferimento ai processi di digitalizzazione in corso e alla crescente esternalizzazione dei servizi, può contribuire a rendere più efficiente l'integrazione dei principi di protezione dei dati personali fin dalle fasi iniziali di progettazione e ridisegno dei processi nonché a promuovere l'adozione delle migliori pratiche che tengano conto dei progressi tecnologici e dei più aggiornati standard di sicurezza e organizzativi.

In questa prospettiva, la partecipazione del RPD alle riunioni del Comitato per le Tecnologie dell'Informazione e ai lavori del Sottocomitato per l'IA assume un rilievo centrale e, allo stesso tempo, testimonia una sensibilità a 360° della Banca verso la tematica della tutela dei diritti fondamentali. Inoltre, con la conclusione dell'accordo[4] tra il RPD e il Servizio Organizzazione - che svolge i compiti del Titolare del trattamento e ha la responsabilità di promuovere le linee di sviluppo organizzativo della Banca - si è completato il riassetto organizzativo per la gestione della privacy, avviato nel 2024 con la collocazione del RPD e del Nucleo di supporto presso il Dipartimento Pianificazione, Organizzazione e Bilancio.

Tale assetto, ulteriormente rafforzato con la nomina di *referenti privacy* all'interno dei Servizi, ha contribuito a migliorare l'efficace applicazione del principio di *privacy by design* consentendo di tener conto, sin dalla fase progettuale, delle implicazioni per la protezione dei dati personali derivanti da interventi su assetti, normative e processi di lavoro determinati da cambiamenti organizzativi e dall'avanzamento delle tecnologie. La più intensa interazione con il Servizio Organizzazione e con le altre Strutture della Banca ha permesso di imprimere maggiore efficacia all'attività di monitoraggio sul Registro dei trattamenti che, nel corso dell'anno, ha registrato un sensibile miglioramento della qualità informativa (cfr. infra par. 3.5).

Con particolare riferimento all'attività di consulenza (cfr. infra par. 3.4), che si attesta su livelli di poco superiori a quelli dell'anno precedente, si segnala il crescente impegno derivante dalle attività legate ai lavori di preparazione dell'euro digitale e alla ripresa del coinvolgimento nei *team* di supporto ai progetti vincitori della *Call for proposal* di Milano Hub.

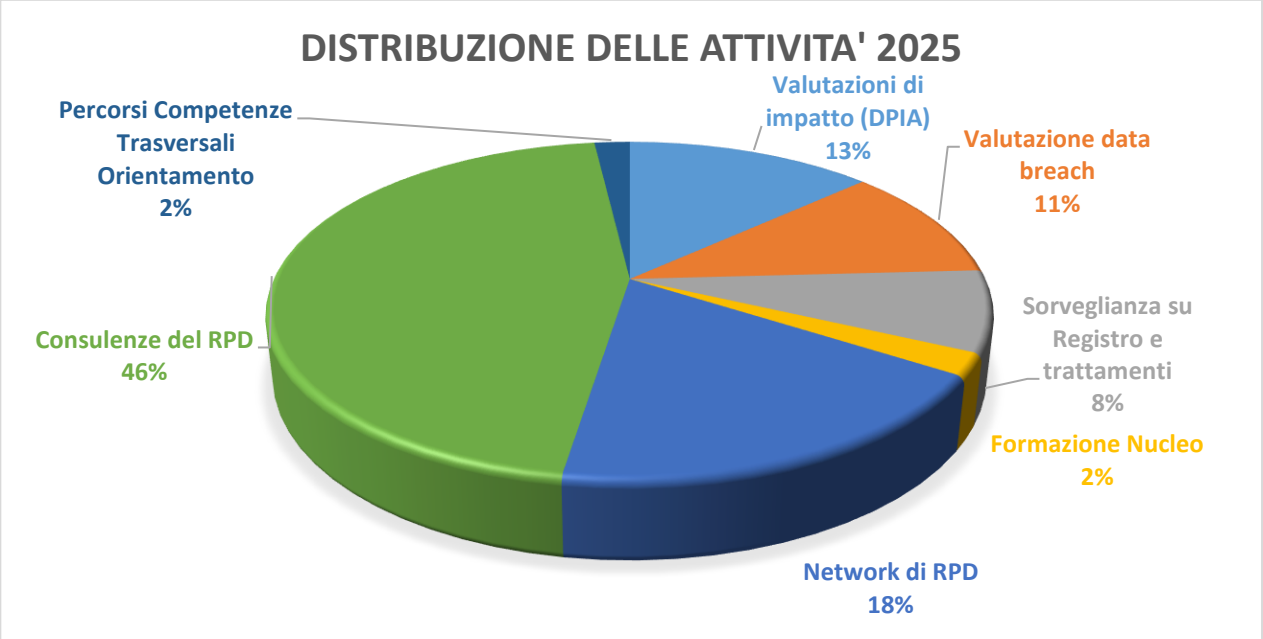
[4] Accordo ORG-RPD e Nucleo di supporto n. 700776 del 1° aprile 2025 che integra il precedente accordo n. 1885049 del 30 settembre 2024 adottato a seguito della riforma organizzativa che ha interessato il RPD e il relativo Nucleo di supporto.

Si è altresì registrata un'intensificazione della partecipazione ai Network, nazionali ed europei, ai quali partecipa istituzionalmente il RPD.

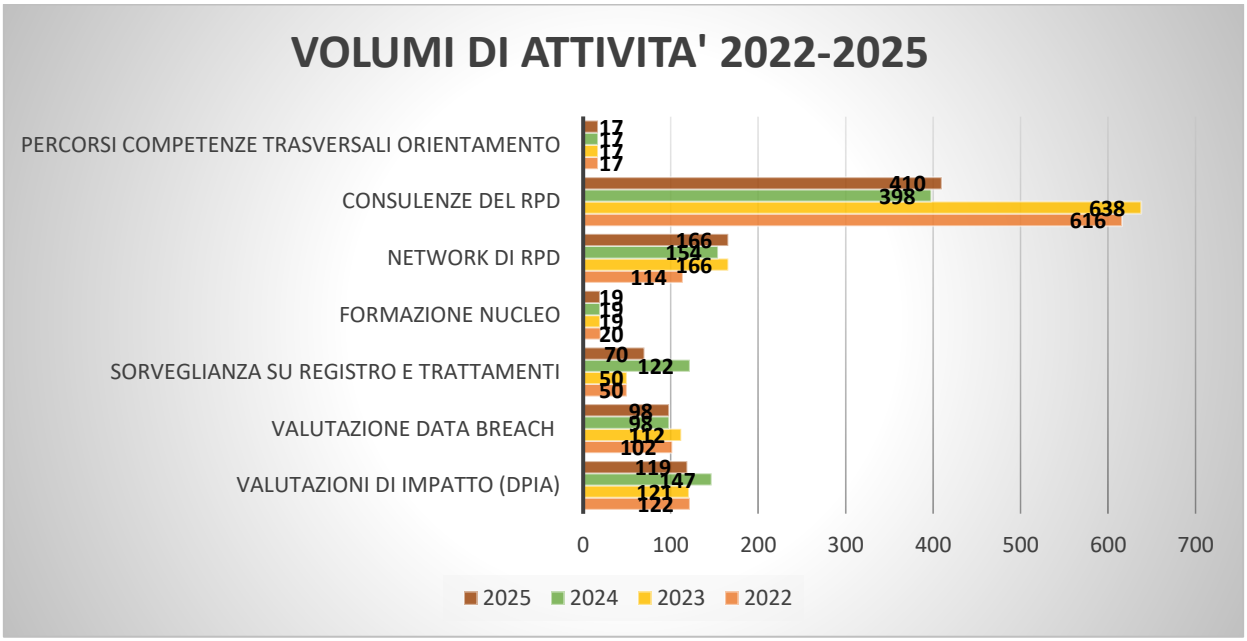
Per quanto riguarda l'attività di promozione della consapevolezza del personale sulla protezione dei dati personali, il RPD ha svolto alcune iniziative di sensibilizzazione, differenziate in funzione delle esigenze delle diverse fasce di personale. Gli interventi sono stati orientati ad attirare l'attenzione sui possibili impatti delle attività quotidiane sulla riservatezza delle informazioni e sulla tutela dei dati personali degli individui, rafforzando la percezione dei pericoli derivanti da comportamenti inconsapevoli nella circolazione dei dati o da condotte esterne malevole (cfr. infra par. 3.8).

Nel giugno del 2025, Banca d'Italia e IVASS, ai sensi dell'art. 37, par. 3, del GDPR, hanno designato un unico RPD. Tale designazione si prefigge di realizzare importanti sinergie tra le due Istituzioni in relazione alle analogie tra i processi, le metodologie e le procedure operative in materia di protezione dei dati, insieme con la condivisione dei valori improntati al riconoscimento e al rispetto dei diritti fondamentali dell'individuo, fra cui quello alla *privacy*. In prospettiva, la nomina di un unico RPD, oltre a mettere a fattor comune le esperienze maturate negli specifici settori di competenza di ciascuna Istituzione, favorirà il continuo allineamento delle prassi di gestione della privacy, con benefici in termini di minore onerosità amministrativa e maggiore efficienza.

Nei grafici seguenti si fornisce la distribuzione delle attività svolte nel 2025 nonché il raffronto tra i volumi di attività registrati nel periodo 2022-2025.



[§] La quantificazione delle attività è stata effettuata sulla base dell'elaborazione dei dati segnalati in procedura ASTRA.



Il lavoro svolto dal RPD e dal Nucleo di supporto è descritto, in maniera analitica per i diversi ambiti di competenza, nei paragrafi che seguono.

3.1 La partecipazione al Network dei DPO del SEBC/SSM

Nel corso del 2025 negli incontri, in streaming e in presenza presso la Bundesbank, del Network dei DPO delle Banche Centrali del SEBC e delle Autorità Nazionali Competenti (NCA) per la supervisione bancaria del SSM, coordinato dal DPO della BCE, sono stati analizzati, anche attraverso procedure scritte, principalmente i seguenti temi comuni:

- le attività di coordinamento tra il Legal Committee (LEGCO) e il Network dei DPO per la Governance della protezione dei dati personali in ambito europeo a seguito delle risultanze del rapporto del Comitato di audit interno;
- le riflessioni sui primi anni di applicazione del GDPR/EUDPR raccolte in un rapporto che evidenzia quanto già realizzato nell'applicazione della normativa europea e come affrontare le sfide future per il coordinamento e l'armonizzazione dell'azione dei DPO;
- l'analisi delle implicazioni per la privacy delle soluzioni di sviluppo delle diverse componenti dell'euro digitale;
- il progetto per una piattaforma accentrata delle informazioni (CDM - Common Data Management) elaborato in ambito SEBC;
- l'esame di un accordo di *Joint controllership* relativo al trattamento dei dati personali nell'ambito del nuovo sistema European Collateral Management System (ECMS);
- i ruoli privacy assunti dalla BCE e dalle Banche Centrali Nazionali nel *framework* integrato (IReF) concernente un progetto di piattaforma statistica unica del SEBC;
- il confronto sulle modalità di implementazione di sistemi di intelligenza artificiale all'interno delle banche centrali nazionali e delle NCA con l'obiettivo di condividere *best practice* e promuovere una più stretta collaborazione all'interno del SEBC;

- la proposta di uno schema di accordo di *Joint controllership* da utilizzare nei casi che coinvolgono il SEBC e/o il SSM.

3.2 La partecipazione alla rete nazionale dei RPD delle *Authority*

Il RPD della Banca partecipa alle riunioni del Network dei RPD delle Autorità indipendenti nazionali[5] che rappresenta la sede di confronto inter-istituzionale sui temi di protezione dei dati personali.

Grazie agli approfondimenti svolti da funzionari del Garante e di altre Autorità, nelle riunioni mensili sono stati trattati temi di attualità di interesse comune per le Istituzioni, riguardanti lo svolgimento dell'attività di sorveglianza e consulenza del RPD e, in particolare:

- il Parere dell'Autorità nazionale anticorruzione del 30 gennaio 2025 relativamente alle misure che possono limitare la raccolta di dati personali su Internet, effettuata (da terzi) con lo scopo di addestrare i modelli di intelligenza artificiale generativa (c.d. *web scraping*);
- i principali contenuti delle Linee guida AgID, poste in consultazione per l'adozione dell'intelligenza artificiale nella PA dal punto di vista tecnico e organizzativo;
- gli approfondimenti sul Portale Nazionale del reclutamento della PA, disciplinato con decreto ministeriale 3 novembre 2023;
- le linee guida per il rafforzamento della resilienza delle PA in coerenza con quanto disposto dall'articolo 8 della legge 28 giugno 2024, n.90;
- il seminario a cura del Garante relativo al trattamento dei dati dei lavoratori dipendenti su alcuni aspetti quali la gestione delle mail dei dipendenti cessati, i tempi di conservazione dei dati, dei *log* e dei metadati, i controlli a distanza sui lavoratori in *smart working*/telelavoro, il trattamento dei *log* di navigazione in Internet dei dipendenti, l'impatto dell'intelligenza artificiale sul trattamento dati dei dipendenti (selezione e gestione del rapporto di lavoro).

Il Network si è fatto promotore di un seminario sul tema *Intelligenza Artificiale e pubblica amministrazione* al quale hanno partecipato i Presidenti del Garante, dell'Agenzia per l'Italia Digitale, dell'Agenzia nazionale per cibersicurezza, della *Commissione sull'IA della Presidenza del Consiglio dei Ministri* oltre a docenti universitari ed esponenti delle professioni.

3.3 Cooperazione e interlocuzione con l'Autorità Garante della privacy

L'anno in rassegna ha fatto segnare significativi momenti di confronto nell'ormai stabile sede di cooperazione con l'Autorità Garante della privacy su tematiche di comune interesse, che

[5] Al Network partecipano, oltre al RPD (coadiuvato dal Nucleo di Supporto), gli RPD dell' Autorità di Regolazione per Energia Reti e Ambiente (ARERA), dell'Autorità di Regolazione dei Trasporti (ART), dell'Autorità Garante della Concorrenza e del Mercato (AGCM), della Commissione Nazionale per le Società e la Borsa (CONSOB), dell'Autorità Nazionale anticorruzione, (ANAC), dell'Autorità per le Garanzie nelle Comunicazioni (AGCOM), della Commissione di Vigilanza sui fondi Pensione (COVIP), della Commissione di Garanzia nei servizi pubblici essenziali (CGSSE), del Garante privacy (GPDP), dell'Istituto di Vigilanza sulle Assicurazioni (IVASS), dell'Agenzia per la Cybersicurezza Nazionale (ACN), della Cassa per i Servizi Energetici e Ambientali (CSEA), dell'Acquirente Unico S.p.a. (AU) e del Garante per l'Infanzia e l'adolescenza; vi prendono parte, in qualità di osservatori, anche i RPD dell'Istituto Nazionale di Statistica (ISTAT), dell'Agenzia per l'Italia Digitale (AgID) e della Centrale di acquisto nazionale (Consip spa).

vede la partecipazione del RPD della Banca alla Rete dei RPD del settore bancario, dell'ABI e di Federcasse, con il coordinamento del Garante.

Tale Network costituisce la sede istituzionale per approfondire la conoscenza dei fenomeni di rilevanza privacy per il comparto bancario e per quello assicurativo nonché per coordinare le previsioni normative che possono avere impatti sulla protezione dei dati personali.

Con specifico riferimento alla promozione della privacy *compliance* dell'attività delle banche è stata avviata una ricognizione delle disposizioni di supervisione vigenti con implicazioni sugli accessi ai dati personali con l'obiettivo di sollecitare riflessioni e proposte condivise per rafforzare la conformità degli accessi dei dipendenti ai dati bancari dei clienti e per individuare soluzioni di mitigazione dei rischi. Inoltre, è stato presentato anche uno specifico contributo di studio dell'ABI per la revisione e l'aggiornamento del provvedimento del Garante n. 192/2011 relativo alla circolazione delle informazioni e al tracciamento delle operazioni bancarie.

Per quanto riguarda il trattamento dei dati dei clienti effettuato per finalità di antiriciclaggio e antiterrorismo (adeguata verifica della clientela), è stata affrontata la tematica della legittimità della raccolta di dati personali da parte di operatori commerciali che gestiscono banche dati. L'analisi ha anche riguardato le modalità di acquisizione delle informazioni e di utilizzo da parte delle banche per le verifiche nei confronti della propria clientela.

In vista dell'attuazione dell'art. 75 del Regolamento (UE) 1624/2024 ("AML *Regulation* - AMLR") è stata avviata una riflessione sui partenariati per lo scambio di informazioni (cd. *partnership for information sharing* - PIS), accordi di cooperazione tra soggetti privati e/o pubblici finalizzati anche alla condivisione di dati relativi ai clienti degli intermediari che partecipano all'accordo, nonché alle operazioni da questi effettuate[6].

3.4 Le consultazioni del Responsabile Protezione Dati

L'attività di consulenza è condotta dal RPD principalmente mediante pareri formali (cfr. par. 3.6 e 3.7) resi obbligatoriamente, ai sensi degli artt. 33 e 35 del GDPR, prima dell'avvio o della modifica di processi strutturati che comportano trattamenti di dati personali (DPIA) nonché a seguito di segnalazioni di incidenti che possono comportare violazioni dei dati personali (c.d. *data breach*).

A questa consultazione formalizzata si affianca, in misura rilevante, l'attività di consulenza sull'applicazione uniforme della normativa privacy che si estrinseca mediante suggerimenti e raccomandazioni, resi in modo informale, in risposta a quesiti o problemi posti dalle Strutture.

[6] La norma, che avrà applicazione dal 10 luglio 2027, individua i requisiti sostanziali e procedurali cui tali partenariati devono conformarsi e attribuisce alle autorità di vigilanza antiriciclaggio (per l'Italia, la Banca d'Italia sul settore finanziario) il compito di verificarne il rispetto, prevedendo inoltre la consultazione, ove necessario, delle autorità competenti in materia di protezione dei dati personali.

Rientra nell'attività di consulenza, l'esame delle clausole privacy di accordi o protocolli da perfezionare con istituzioni pubbliche e, in particolare:

- una convenzione tra Banca d'Italia e Unioncamere, per la condivisione di informazioni finalizzata alla realizzazione di progetti di ricerca economica di interesse comune, mediante aggregazioni rispettose della riservatezza delle persone e dei diritti di privativa;
- un accordo tra Banca d'Italia e Guardia di Finanza per lo scambio informativo e la cooperazione per la protezione e il contrasto delle minacce cyber;
- un accordo tra Dipartimento per la Trasformazione Digitale, Associazione Nazionale Comuni Italiani e Banca d'Italia volto a condurre indagini congiunte sullo stato del processo di digitalizzazione delle PA e a pubblicarne i risultati;
- una convenzione tra Banca ed Ente Veneto Lavoro relativa a una collaborazione diretta all'analisi del sistema di politiche attive del lavoro e allo studio delle caratteristiche dei disoccupati e dell'evoluzione delle carriere lavorative;
- una convenzione tra Banca e Unione Nazionale Rivenditori Auto Estere (UNRAE) finalizzata a contribuire alla produzione di statistiche e analisi tempestive sull'evoluzione del quadro economico congiunturale;
- un accordo di cooperazione tra Banca d'Italia e Consob a supporto delle indagini da espletare nel quadriennio 2025 - 2028 da ciascuna Istituzione sull'Alfabetizzazione finanziaria e le competenze di finanza digitale dei Giovani (IAFG);
- un accordo di collaborazione, nell'ambito delle attività di Milano Hub, con la Central Bank of Ireland (CBI) per il coordinamento di una iniziativa di ricerca aperta a studenti e ricercatori universitari (Innovation Data Challenge, IDC), sul tema "*The use of data to promote innovation in the retail payment market*".

Per la verifica della privacy *compliance* sono state prestate consulenze nei seguenti ambiti: la Circolare 318 recante il nuovo Manuale della gestione documentale; la piattaforma informatica costituita da EBA, ESMA ed EIOPA (ESA Information System) per lo scambio di informazioni pertinenti alle rispettive aree di supervisione; il processo di adeguata raccolta delle evidenze digitali a scopo difensivo (*Digital Forensic Readiness*); l'apertura dell'Archivio Storico della Banca d'Italia per la consultazione pubblica dei Diari dell'ex Governatore Paolo Baffi relativi agli anni 1949 – 1980. Inoltre, nell'ambito del *risk assessment* previsto dall'*Operational Risk Management,* è stata prestata consulenza con riferimento alla stima del potenziale impatto patrimoniale di sanzioni inflitte per violazione della privacy.

Nell'ambito dei contratti stipulati dalla Banca sono stati approfonditi aspetti di *compliance* nei ruoli e nelle clausole privacy riguardanti servizi di primo soccorso, fornitura di brokeraggio assicurativo, servizio di gestione del piano di *flexible benefits* per il personale.

È stato avviato un confronto con la Cassa di Sovvenzioni e Risparmio fra il personale della Banca d'Italia (CSR) per la verifica e l'eventuale aggiornamento della privacy *compliance* nelle aree di intersezione tra le rispettive attività e processi di lavoro.

Con riferimento al progetto dell'euro digitale, è proseguito l'impegno del RPD e del Nucleo di supporto nel fornire i propri contributi all'esame di profili privacy emersi nell'attività dell'*High Level Task Force* e durante il negoziato presso la Commissione europea volto a definire l'impianto normativo della *Proposal for a Regulation on the establishment of the digital euro*.

3.5 La sorveglianza sul Registro delle attività di trattamento

L'attività di sorveglianza sul Registro delle attività di trattamento si estrinseca, principalmente, attraverso il monitoraggio periodico delle informazioni iscritte nel Registro[7] che ha l'obiettivo di verificare la pertinenza, la coerenza, la completezza e l'efficacia della rappresentazione della generalità o di gruppi di trattamenti inseriti dalle Strutture competenti e promuoverne le eventuali rettifiche e integrazioni**.**

Raffrontando la situazione del Registro al 31 dicembre 2025[8] con quella risultante dalla precedente Relazione, si rileva il complessivo aumento dei trattamenti di dati personali (235 a fronte di 223 dell'anno precedente), ascrivibile all'introduzione di attività di trattamento frutto dello svolgimento di nuovi compiti ovvero della crescente articolazione e informatizzazione dei processi di lavoro.

In linea con le raccomandazioni espresse dai revisori interni a seguito dell'*audit* sul sistema di protezione dati della Banca[9], il monitoraggio del Registro è stato improntato a una maggiore focalizzazione e specificità delle indicazioni fornite al Titolare del trattamento, al fine di favorire un'efficace azione di indirizzo e di coordinamento nei confronti delle Strutture. I suggerimenti contenuti nel monitoraggio sono stati puntualmente riscontrati dal Servizio Organizzazione con l'indicazione delle iniziative intraprese che hanno riguardato l'aggiunta di elementi rappresentativi del trattamento ovvero l'affinamento di quelli già censiti (basi giuridiche, criteri e termini di cancellazione, informative privacy, indicazione dei destinatari esterni e delle ulteriori finalità del trattamento).

Tale rinnovata dialettica tra RPD e Titolare del trattamento, oltre a comportare un sensibile miglioramento della qualità informativa del Registro, consentirà, in linea con le raccomandazioni

---

7 La tenuta del Registro è prevista dall'art. 30 del GDPR tra gli adempimenti principali del Titolare (e del Responsabile) del trattamento. Il Registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. Secondo quanto previsto dalle Linee Guida europee (WP Art. 29, *Guidelines* 5 aprile 2017, par. 4.1 e 4.5), il RPD conduce con regolarità il monitoraggio del Registro con l'obiettivo di valutare complessivamente l'efficacia informativa dei trattamenti censiti.

8 Per conseguire vantaggi di efficienza, a partire dal 2025, l'arco temporale oggetto del monitoraggio coincide con il semestre dell'anno solare, in modo da allinearlo con il periodo di riferimento delle altre valutazioni relative all'attività aziendale.

9 Nel periodo ottobre - dicembre 2024 sono stati sottoposti a revisione l'adeguatezza del sistema adottato dalla Banca per la protezione dei dati personali e dei processi di lavoro posti a presidio dei relativi rischi nonché l'efficacia dei meccanismi di coordinamento tra la struttura incaricata degli adempimenti di competenza del Titolare del trattamento e il Nucleo di supporto al Responsabile della Protezione dei Dati (RPD).

del Garante[10], di migliorare la tracciabilità delle attività di trattamento e la verifica del livello complessivo di *compliance*.

3.6 Le valutazioni di impatto sulla protezione dei dati (DPIA)

Nel corso del 2025 il RPD ha fornito il suo parere per otto *Data Protection Impact Assessment* (DPIA) legati alla realizzazione di progetti informatici o procedure di lavoro oggetto di studio o revisione[11] che, comportando una potenziale esposizione a rischio per i dati personali delle persone fisiche interessate, hanno richiesto di implementare presidi di protezione adeguati. Tra le valutazioni di maggior rilievo si segnalano:

- il progetto volto a introdurre, nel quadro dei servizi di comunicazione e collaborazione in uso nell'Istituto e in IVASS, gli applicativi Microsoft Copilot 365 e Microsoft Copilot Chat, integrati con specifici agenti Copilot, al fine di supportare le attività lavorative del personale tramite strumenti di intelligenza artificiale generativa configurati sullo schema del *language learning model*;
- la manutenzione evolutiva dell'applicativo Microsoft Teams tramite l'introduzione delle funzionalità di registrazione e trascrizione delle riunioni classificate con un profilo di riservatezza inferiore ad "alto";
- l'iniziativa volta a implementare una nuova procedura, denominata S.I.M.B.A. (sistema integrato missioni *budget* e agenzia), tramite acquisizione di una soluzione in *public cloud* per agevolare l'integrazione dei profili gestionali del *budget* e delle missioni del personale nonché per semplificare il relativo processo di liquidazione del trattamento economico;
- l'integrazione tra i dati contenuti nelle bollette doganali, acquisiti dall'Agenzia delle dogane e dei monopoli, e il patrimonio informativo gestito dall'Istituto all'interno dell'*enterprise data lake*, al fine di potenziare le basi di dati messe a disposizione per finalità di analisi statistica e ricerca economica con tecniche e metodologie innovative;
- la configurazione dei presidi di sicurezza privacy adottati dalla piattaforma *online* finalizzata all'erogazione dei servizi di *welfare* aziendale (c.d. piano di *flexible benefits*) fruibili dal personale in servizio e in quiescenza dell'Istituto nonché dagli altri beneficiari;
- la manutenzione evolutiva del servizio di "*contact centre*" della Banca d'Italia (c.d. numero verde), tramite assistenza affidata in modalità mista a una società esterna, per la gestione del contatto telefonico e le informazioni relative ai servizi offerti dall'Istituto, e alla Banca per la risoluzione dei quesiti di maggiore complessità;
- il progetto volto a introdurre in via sperimentale la piattaforma *online* "Concorsi *smart*", gestita da una società esterna, per consentire lo svolgimento tramite *tablet* delle prove scritte nei concorsi esterni e interni dell'Istituto con successivo caricamento degli elaborati

[10] Provvedimento 29 aprile 2021, Documento di indirizzo sul Responsabile della protezione dei dati (RPD) in ambito pubblico, par. 8.

[11] L'art. 35 del GDPR prevede che: «*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. ..... Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati* ...». Le valutazioni di impatto si rendono necessarie quando l'acquisizione e la gestione delle informazioni implicano un trattamento di dati personali di rilevanza particolare o su larga scala o con l'utilizzo di tecnologie innovative e in tutte le fattispecie individuate dal Garante *ex* art. 35.4 GDPR (cfr. Provv. n. 467 dell'11 ottobre 2018).

concorsuali nella suddetta piattaforma, dotata di presidi di sicurezza privacy e accessibile soltanto ai componenti della commissione;

- l'integrazione della valutazione di impatto, a suo tempo effettuata riguardo ai vari trattamenti di dati personali aggregati nel "Portale dei servizi per il personale in servizio e in quiescenza", per l'inserimento di un nuovo servizio di comunicazione per i dipendenti e i pensionati.

3.7 La valutazione dei data breach

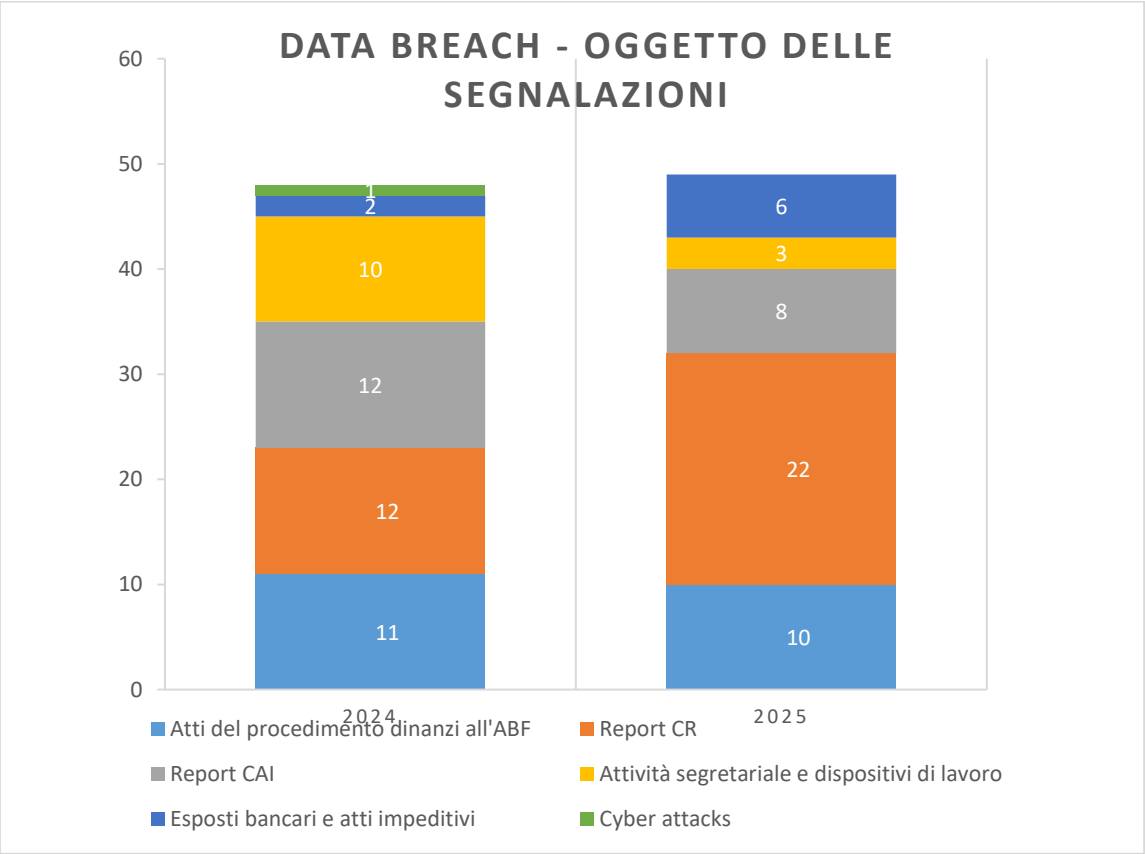
Nel 2025, le potenziali violazioni dei dati personali rilevate e sottoposte alla valutazione del RPD (c.d. *data breach*) sono state 49 (a fronte delle 48 registrate nel 2024): su ciascun evento il RPD ha fornito al Titolare del trattamento il proprio parere sulla qualificazione del fatto segnalato come violazione dei dati personali e sulla ponderazione del conseguente rischio per i diritti e le libertà delle persone fisiche, ai fini delle eventuali determinazioni previste dal GDPR[12].

Il livello di rischio per i soggetti interessati nelle varie fattispecie alla luce delle circostanze fattuali e delle cautele adottate è stato ritenuto trascurabile. In due casi il RPD ha proposto di effettuare la segnalazione all'Autorità Garante prevista dall'art. 33 del GDPR: nel primo caso, la segnalazione è stata effettuata in via cautelativa sebbene l'evento concernesse un potenziale furto di identità digitale cui la Banca era estranea; nel secondo caso, riguardante un furto di un supporto informatico in uso a un dipendente della Banca, sono state effettuate nei primi giorni del 2026 la segnalazione e la comunicazione ai diretti interessati.

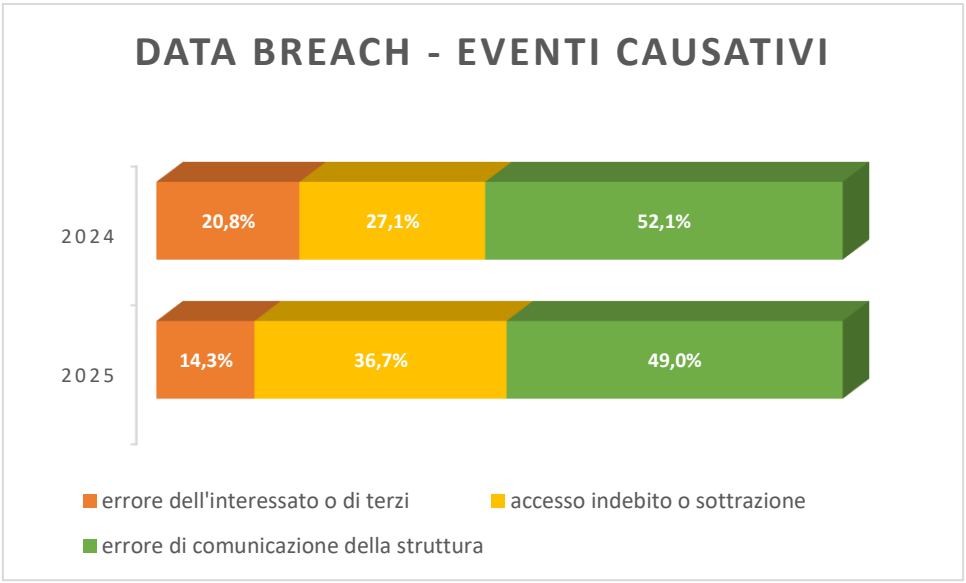
Gli ambiti nei quali si sono concentrate maggiormente le segnalazioni di violazione dei dati personali sono quelli inerenti agli accessi alla Centrale dei Rischi (C.R.), alla gestione dei procedimenti dinanzi all'Arbitro Bancario e Finanziario (A.B.F.) e alla comunicazione dei tabulati contenuti nella Centrale di Allarme Interbancaria (C.A.I).

Nel grafico seguente vengono posti a raffronto il numero di *data breach* registrato nel 2024 e nel 2025 per ciascun ambito di attività.

[12] Il RPD fornisce al Titolare del trattamento un parere nei casi di perdita, alterazione o sviamento (accidentali o illeciti) di dati personali configurabili come *data breach*. Il GDPR (art. 33), qualora si verifichino i presupposti di un *data breach*, impone al Titolare del trattamento dei dati di darne notifica all'Autorità Garante, entro 72 ore dal momento in cui ne ha avuto conoscenza (salvo giustificazione dei motivi del ritardo, ove la notifica non possa essere effettuata entro tale stringente termine), a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche; qualora, poi, la violazione presenti un rischio elevato per i diritti e le libertà degli interessati, il Titolare del trattamento deve darne comunicazione, senza ingiustificato ritardo, anche agli interessati (art. 34).



Poco più della metà delle violazioni è imputabile a condotte negligenti o malevole poste in essere dagli stessi interessati o da parte di terzi. La restante quota è determinata da errori operativi nelle comunicazioni all'esterno da parte di dipendenti della Banca. Al fine di contenere la diffusione del fenomeno, nel corso delle iniziative di sensibilizzazione illustrate nel paragrafo successivo sono state richiamate le raccomandazioni e buone prassi per la tutela della riservatezza dei dati personali.



3.8 Le iniziative di sensibilizzazione del Responsabile Protezione Dati

Nell'esercizio dei propri compiti di sorveglianza sull'applicazione della normativa privacy, il RPD promuove, di propria iniziativa o congiuntamente con altre funzioni, attività dirette a sensibilizzare su adempimenti e iniziative per rafforzare la *compliance* complessiva delle strutture.

In questo ambito, il RPD ha promosso una campagna di sensibilizzazione, organizzata d'intesa con il Dipartimento Informatica, sull'evoluzione dello scenario della minaccia cyber e sulla difesa dei dati personali nell'era digitale, portando l'attenzione sull'importanza di tenere comportamenti consapevoli e sulla centralità della protezione dei dati personali fin dalla progettazione di piattaforme e sistemi informatici.

Le iniziative hanno coinvolto i Capi dei Servizi e delle unità di base, e i loro sostituti e sono state finalizzate a consolidare comportamenti quotidiani coerenti con le misure organizzative e tecniche adottate e ad accrescere la capacità del personale di riconoscere segnali di anomalia e tentativi di inganno. In questo ambito, sono state esplicitate raccomandazioni e buone prassi da seguire per la tutela della riservatezza delle informazioni e per la privacy *compliance*.

Si sono poi tenuti alcuni incontri, che hanno coinvolto il personale di alcune Strutture e dell'IVASS, nel corso dei quali sono stati esposti i principi della normativa sulla privacy e le cautele in grado di limitare i possibili rischi di violazioni dei dati personali nell'ambito delle attività di lavoro.

Proseguendo lungo questa linea, nei primi mesi del 2026, la Banca, con una comunicazione rivolta a tutti i dipendenti, ha ulteriormente richiamato l'attenzione sulla tutela dell'integrità del patrimonio informativo e sulla necessità di adottare comportamenti attenti e consapevoli, pienamente rispettosi delle norme organizzative e tecniche poste a salvaguardia dei dati personali e della riservatezza delle informazioni.