dirittifondamentali.it

Tutela della riservatezza e violazione dei dati personali

(GPDP, Provvedimento n. 659 del 2 novembre 2024)

***

Provvedimento del 2 novembre 2024

Registro dei provvedimenti
n. 659 del 2 novembre 2024

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Fabio Mattei, segretario generale;

VISTO il 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 (Regolamento generale sulla protezione dei dati, di seguito "Regolamento");

VISTI in particolare gli articoli 33 e 34 del Regolamento rubricati, rispettivamente, "Notifica di una violazione dei dati personali all'autorità di controllo" e "Comunicazione di una violazione dei dati personali all'interessato";

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali", così come modificato dal decreto legislativo 10 agosto 2018, n. 101 (di seguito "Codice");

VISTE le "Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del RGPD" adottate dal Comitato europeo per la protezione dei dati il 28 marzo 2023 in sostituzione delle "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (di seguito "Linee guida sulla notifica");

VISTE le "Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali" adottate dal Comitato europeo per la protezione dei dati il 14 dicembre 2021 (di seguito "Linee guida sui casi di violazione dei dati personali");

VISTE le "Linee guida per trattamenti dati relativi al rapporto banca-clientela" del 25 ottobre 2007 (pubblicate in G.U. n. 273 del 23 novembre 2007;www.gpdp.it, doc. web n. 1457247);

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali (di seguito, "regolamento 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;
RELATORE il prof. Pasquale Stanzione;

PREMESSO

L'Autorità è venuta a conoscenza, attraverso la notifica di violazione dei dati personali del 17 luglio 2024 (fasc. DB006866), effettuata, in via definitiva ai sensi dell'art. 33 GDPR dalla Intesa Sanpaolo S.p.A. (di seguito "Titolare", "Banca" o "Società"), di una perdita di riservatezza di dati personali determinata dall'accesso non autorizzato da parte di un dipendente ai dati bancari di alcuni clienti.
In particolare, nella citata notifica di violazione di dati personali la Società rappresentava che "Nel mese di febbraio 2024, la Funzione Privacy, incaricata dei controlli di secondo livello in merito a potenziali anomalie negli accessi ai dati bancari da parte dei dipendenti rilevate dai sistemi di alert adottati da questo Titolare, ha analizzato le interrogazioni eseguite dal dipendente interessato (assegnato alla Filiale Agribusiness di Barletta - Distaccamento di Bisceglie con l'incarico di Gestore Agribusiness) sulla movimentazione della carta di credito di una cliente fra il 1° ottobre 2023 e il 12 ottobre 2023. Il sistema di alert ha inoltre intercettato nello stesso periodo (ottobre - novembre 2023) altri potenziali accessi anomali su due ulteriori clienti…" e che "…Sulla base dell'esito di tutte le verifiche condotte si ritiene che il perimetro dei clienti effettivamente impattati dall'accertata anomala operatività effettuata dal dipendente coinvolto sia di 9 persone fisiche."
Con riferimento alla valutazione del rischio della violazione, la Banca ha ritenuto che l'evento presentasse un rischio medio per i diritti e le libertà delle persone fisiche, in ragione del fatto che "Gli interventi effettuati dalla competente funzione di Audit Interno e di Risorse Umane con diretto contatto del dipendente autore della violazione e la sua successiva sospensione dal servizio, hanno consentito di interrompere definitivamente gli accessi ai dati personali della clientela interessata. Il comportamento compulsivo ed esteso del dipendente interessato su clienti estranei al proprio portafoglio e le graduali valutazioni svolte, fanno ritenere plausibile la motivazione dallo stesso addotta (ovvero la curiosità) nella consultazione dei dati personali di tali clienti, limitando, di conseguenza, i potenziali impatti per gli interessati tenuto anche conto dell'assenza di segnali di esfiltrazione delle informazioni visualizzate".
Avuto riguardo alla comunicazione agli interessati, ex art. 34 del Regolamento, la Banca ha rappresentato di voler comunicare l'evento ai nove interessati coinvolti: "pur non rilevando rischi elevati per i diritti e le libertà delle persone, questo Titolare procederà, al fine di fornire tutte le informazioni pertinenti in merito alla vicenda occorsa e consentire un pronto riscontro alle eventuali richieste di ulteriori delucidazioni, ad informare i 9 interessati (tra i quali rientrano anche conoscenti e parenti del dipendente coinvolto) oggetto del numero più consistente di accessi, mediante colloquio effettuato da parte dei Responsabili delle Filiali di radicamento dei rapporti".
Con riferimento alla notifica di una violazione di dati personali all'autorità di controllo prevista dall'art. 33 del Regolamento, la Banca ha ritenuto di aver fornito tutte le informazioni necessarie con la notifica presentata il 17 luglio 2024, che infatti è stata indicata come "completa".
In data 30 agosto 2024, la Banca ha comunque provveduto a integrare la notifica precedentemente presentata, per informare l'Autorità di aver proceduto al licenziamento del dipendente in questione.

Successivamente, il 10 ottobre 2024, l'Autorità ha appreso, da notizie di stampa, che un dipendente di Intesa Sanpaolo avrebbe avuto accesso, al di fuori della corretta operatività connessa allo svolgimento del proprio lavoro, a "…depositi di politici e militari, tra cui la sorella della premier, l'ex compagno e i ministri Crosetto e Santanchè. Ma anche Ignazio La Russa e il procuratore della Direzione nazionale antimafia, Giovanni Melillo…" (cfr. https://www.agi.it/cronaca/news/2024-10-10/spiati-conti-correnti-di-giorgia-meloni-e-sorella-inchiesta-su-ex-dipendente-intesa-sanpaolo-28202220/).

In particolare, gli accessi "…sarebbero stati quasi settemila, realizzati tra il 21 febbraio del 2022 e il 24 aprile del 2024, e avrebbero più in particolare riguardato gli oltre tremilacinquecento clienti portafogliati di 679 filiali di Intesa Sanpaolo, sparse in tutta Italia" (cfr. https://www.ansa.it/puglia/notizie/2024/10/10/spiati-i-conti-correnti-di-meloni-giambruno-la-russa_cb03fa8d-6456-4f78-9fb5-5eb7895cee00.html) e sarebbero stati scoperti dall'Istituto, grazie alla denuncia di un correntista.

In merito, l'Autorità, con nota prot. 118325 del 10 ottobre 2024, ha inviato una richiesta di informazioni a Intesa Sanpaolo allo scopo di verificare se i fatti riportati dalle notizie di stampa fossero riconducibili all'evento di violazione di dati personali descritto nella notifica del 17 luglio 2024 e per conoscere l'effettiva portata degli eventi a suo tempo notificati in termini di assai minore portata in relazione al numero di interessati coinvolti e alle loro categorie (titolari di cariche elettive e pubbliche, personaggi politici e pubblici).

La Banca ha risposto, con nota n. 121551 del 17 ottobre 2024, precisando che:

l'evento di violazione di dati personali descritto nella notifica del 17 luglio 2024 è il medesimo riportato sulle notizie di stampa;

la violazione è consistita nella "…perdita di riservatezza, dovuta unicamente ad accessi apparentemente non giustificati da ragioni di servizio compiuti da un dipendente";

la Banca ha avuto contezza, per la prima volta, di un accesso anomalo da parte del dipendente il 9 ottobre 2023, a seguito dell'attivazione dell'alert F23.2acc – Alert Privacy "Carte e CRIF", facente parte dei controlli impostati da Intesa Sanpaolo, in ottemperanza del Provvedimento dell'Autorità n. 192/2011. Tale alert ha segnalato una potenziale anomalia in merito all'interrogazione da parte del dipendente dei movimenti, relativi al bimestre precedente, della carta di credito di un cliente;

a seguito dell'attivazione di altri alert in tempi successivi e all'esito di controlli e verifiche interne, effettuati anche attraverso l'analisi dei log degli accessi complessivamente effettuati dal dipendente e conservati per 24 mesi ai sensi del citato Provvedimento del Garante n. 192/2011, in data 4 luglio 2024, la Banca avviava un procedimento disciplinare nei confronti del dipendente;

il numero di interessati coinvolti risulta, allo stato "…non determinabile – ossia, per essere determinato con ragionevole certezza, richiede l'impiego di uno sforzo sproporzionato. Il numero reso noto dalla stampa di 3.572 clienti, a cui corrispondono 6.637 accessi effettuati dal Dipendente e indicato nel report della funzione di Audit del 21 maggio 2024 ("Report Audit", allegato sub Allegato 1), corrisponde ai clienti non radicati presso la Filiale Agribusiness di Barletta e presso i relativi distaccamenti di Bisceglie e Ruvo di Puglia (Filiale e distaccamenti di pertinenza del Dipendente) i cui dati sono stati oggetto di accesso da parte del Dipendente in 460 giornate tra il 21 febbraio 2022 e il 24 aprile 2024";

"…le inquiry effettuate dal Dipendente nel Biennio di Analisi su 3.572 clienti potevano, teoricamente, essere coerenti con la specifica operatività di un Gestore Agribusiness (qualifica ricoperta dal Dipendente), che può dover interrogare "in circolarità" anche clientela non radicata presso la propria Filiale di appartenenza…". In merito, "…il Dipendente ha eccepito la legittimità di parte dei 6.637 accessi…";

dal Report di Audit emerge che, con riferimento ai clienti oggetto di accesso da parte del dipendente: "…34 sono politici nazionali, appartenenti sia a forze politiche del centro destra, sia del centro sinistra. In totale, nel Biennio di Analisi, le interrogazioni del Dipendente relative a tali soggetti sono state 102 (pari all'1,54% del complesso dei 6.637 accessi citati nel Report Audit). In particolare, per 15 dei 34 politici, il Dipendente ha effettuato una sola inquiry e, per altri 11 soggetti, ne ha effettuate due e, dei 34 politici, è risultato come 10 non avessero – al tempo dei fatti – alcun rapporto in essere con la Banca (con risultato scheda vuota); 43 sono personaggi di fama nazionale del mondo dello spettacolo, dello sport e della cronaca; 73 sono dipendenti e manager della Banca, inclusi alcuni soggetti apicali; i rimanenti 3.422 clienti consistono, prevalentemente, in soggetti della piazza di residenza del Dipendente o radicati in altre piazze che ruotano intorno alla sua sfera personale e professionale. In particolare, circa 2.450 di tali soggetti sono delle piazze di Bari e limitrofe al comune di residenza del Dipendente; gli accessi hanno riguardato 1) posizioni contrattuali/SICLI (NJ00 - scheda cliente), 2) movimentazione di rapporti (IY11 - e/c ad uso interno) e carte di pagamento (ZAFI - consente di interrogare il mondo "carte di pagamento"), talora anche con dettagli di operazioni, e 3) attività finanziarie (DAPY – investimenti).";

la Banca ha dichiarato di non avere avuto evidenza di estrazione dei dati oggetto di accesso da parte del proprio dipendente tramite i sistemi informativi interni;

la Banca ha ribadito di non aver proceduto ad effettuare la comunicazione agli interessati ex art. 34 del Regolamento "Coerentemente a quanto concluso dal Responsabile della protezione dei dati, la Banca (titolare del trattamento) non ha a sua volta ritenuto che la violazione dei dati personali in commento fosse "suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 34.1 GDPR) e, quindi, non ha provveduto alla comunicazione della medesima violazione dei dati personali a tutti i soggetti potenzialmente coinvolti";

la Banca starebbe comunque "…valutando di inviare alla nostra intera base clienti, costituita da circa 13 milioni di soggetti interessati, una comunicazione di client caring dedicata a descrivere come si è effettivamente svolta la vicenda e quali possono essere le sue possibili conseguenze, ma anche le misure che abbiamo adottato e quelle che stiamo valutando di adottare";

rispetto a quanto descritto nella notifica del 17 luglio 2024, la Banca ha inteso precisare che: "…La notifica depositata in data 17 luglio 2024 è solo la prima comunicazione all'Autorità sulla vicenda di interesse…" e, con riferimento all'indicazione di 9 interessati coinvolti "sicuramente le posizioni di 9 clienti della Banca (7 NDG5 + 2 cointestatari) siano stati oggetto di accessi anomali da parte del Dipendente in considerazione della numerosità di tali accessi" e che, inoltre, "Si tratta, nello specifico, di clienti che sono stati oggetto di complessivamente 1.333 accessi sul totale di 6.637 accessi estratti nel Biennio di Analisi ai fini di cui alle verifiche della Banca".

* * *

Nelle more della definizione di una più ampia istruttoria, tuttora in corso, finalizzata all'approfondimento di quanto sopra illustrato e alla definizione di tutti gli aspetti connessi

all'evento occorso, si rende necessario valutare la conformità delle iniziative fin qui intraprese dalla Banca a tutela degli interessati, con particolare riferimento al pieno ed efficace assolvimento degli obblighi di comunicazione di cui all'art. 34 del Regolamento, alla luce sia delle dichiarazioni rese dal Titolare che degli elementi autonomamente acquisiti dall'Ufficio.

Al riguardo, il Regolamento indica che, nella valutazione del rischio, siano prese in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati, e che tali rischi siano determinati in base a una valutazione oggettiva (cfr. cons. nn. 75 e 76).

In particolare, le Linee guida sulla notifica individuano i seguenti fattori da considerare – a fronte di una violazione dei dati personali – nella valutazione del rischio per i diritti e le libertà degli interessati: il tipo di violazione; la natura, il carattere sensibile e il volume dei dati personali; la facilità di identificazione degli interessati; la gravità delle conseguenze per gli interessati; le caratteristiche particolari dell'interessato; le caratteristiche particolari del Titolare del trattamento dei dati; nonché il numero di interessati coinvolti.

Diversamente da quanto valutato dal Titolare, l'Autorità ritiene che la violazione dei dati personali in questione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto della natura della violazione dei dati personali – che alle condizioni previste dal Codice penale, art. 615-ter, può configurare un'ipotesi di reato – delle categorie dei dati personali oggetto di violazione, della gravità e persistenza delle possibili conseguenze per le persone fisiche che potrebbero derivare dalla violazione (quali, a titolo di mero esempio, la divulgazione di notizie riguardanti lo stato patrimoniale, il danno reputazionale) nonché del settore di attività del Titolare, che richiede un elevato grado di responsabilizzazione da parte dei propri incaricati, al fine di garantire la fiducia nei propri confronti da parte dei clienti, soddisfacendo, in particolare, le loro legittime aspettative di riservatezza e di sicurezza del trattamento.

L'art. 34, par. 1, del Regolamento che stabilisce che "quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo", fatti salvi i casi in cui tale comunicazione non è richiesta in quanto risulta essere soddisfatta una delle condizioni previste al par. 3 del medesimo articolo, non applicabile al caso in specie.

Le citate Linee guida sulla notifica ricordano che "in linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia" (cfr. art. 34, par. 3, lett. c), del Regolamento), richiamando le "Linee guida sulla trasparenza ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29, fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018. Queste ultime Linee guida chiariscono che il titolare dovrebbe "effettuare una valutazione mettendo sulla bilancia, da un lato, lo sforzo […] e, dall'altro, l'impatto e gli effetti […] sull'interessato".

Al riguardo, le Linee guida sulla notifica richiamano l'attenzione dei titolari del trattamento su quanto previsto dall'art. 34, par. 3, del Regolamento, facendo presente che "conformemente al principio di responsabilizzazione, il titolare del trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più […] condizioni" per le quali non è richiesta la comunicazione della violazione dei dati personali direttamente agli interessati coinvolti.

La comunicazione agli interessati rappresenta, peraltro, una delle misure che il titolare del trattamento può adottare per attenuare i possibili effetti negativi della violazione dei dati personali per gli interessati e ha come obiettivo principale quello di fornire informazioni specifiche sulle misure che gli stessi interessati possono adottare per proteggersi dalle possibili conseguenze negative di una violazione (cfr. cons. n. 86 del Regolamento).

In ogni caso, le Linee guida sulla notifica raccomandano al titolare del trattamento di "scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate" evidenziando che "si potrebbe altresì prevedere l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, soluzione questa che potrebbe rivelarsi utile per le persone fisiche che potrebbero essere interessate da una violazione ma che il titolare del trattamento non può altrimenti contattare".

Le Linee guida sui casi di violazione dei dati personali evidenziano come la comunicazione agli interessati sia una buona pratica e un fattore di mitigazione in presenza di un attacco ransomware con esfiltrazione poiché "la violazione riguarda non solo la disponibilità dei dati, ma anche la riservatezza, in quanto l'autore dell'attacco può aver modificato e/o copiato i dati dal server. Pertanto, il tipo di violazione comporta un rischio elevato" e che "la natura, la sensibilità e il volume dei dati personali aumentano ulteriormente i rischi, poiché il numero di persone interessate è elevato, così come la quantità complessiva di dati personali compromessi" (cfr. parr. 42 e 43) e, laddove coinvolga dati di diversa natura, fra cui quelli finanziari, può causare un danno più elevato: "Le violazioni che coinvolgono dati sanitari, documenti di identità o dati finanziari come i dettagli della carta di credito possono causare danni di per sé, ma se utilizzate insieme potrebbero essere utilizzate per il furto di identità. Una combinazione di dati personali è in genere più sensibile di un singolo dato personale." (cfr. par. 108).

Alla luce di quanto sopra, pertanto, il Titolare del trattamento è tenuto a comunicare la violazione agli interessati, considerata la particolare delicatezza dei dati personali oggetto di violazione, obbedendo a un principio di precauzione che, pur nella incertezza sugli effettivi utilizzi ulteriori dei dati cui il dipendente ha avuto accesso (che non è dato sapere, al momento, se siano stati oggetto di acquisizione come dati informatici o come immagini o siano stati semplicemente consultati e, possibilmente, trascritti manualmente su supporti cartacei o elettronici), impone di adottare comunque le maggiori cautele possibili a fronte della potenzialità lesiva recata dalle ripetute azioni poste in essere dal dipendente e che sono tuttora al vaglio dell'Autorità giudiziaria competente.

Inoltre, si rileva che la decisione del Titolare di non effettuare la comunicazione agli interessati non consente loro di assumere gli idonei comportamenti cautelativi in considerazione della natura dei dati personali oggetto di violazione che li riguardano (cons. n. 86 del Regolamento; cfr. anche Provv. n. 264 del 10 dicembre 2020, doc. web n. 9557555).

Ciò, tenuto anche conto del fatto che, nel corso dell'istruttoria fin qui svolta, il Titolare non ha comprovato in alcun modo la sussistenza della condizione di cui all'art. 34, par. 3, del Regolamento in relazione allo sforzo sproporzionato che la predetta comunicazione richiederebbe.

Pertanto non si ritiene applicabile al caso di specie la condizione prevista alla lettera c) del par. 3, anche in ragione del fatto che i clienti le cui posizioni bancarie sono state oggetto di accesso da parte del dipendente sono certamente noti alla Banca così come sono noti i recapiti di ciascuno di essi, e

tenuto conto del tempo intercorso e delle analisi effettuate dalla Banca, anche in contraddittorio con il dipendente.

La comunicazione non appare, inoltre, comportare uno sforzo sproporzionato in ragione del numero di interessati a cui si dovrebbe rivolgere, numero che, per ammissione della stessa Banca, rappresenta "…un numero esiguo di interessati rispetto – per la Banca – al totale della clientela".

Ciò anche considerando che la comunicazione che il Titolare ha dichiarato di voler inviare a tutta la base clienti avrebbe contenuti e scopi diversi da quella necessariamente più specifica richiesta dall'art. 34 del Regolamento, che, invece, deve essere effettuata nei confronti di coloro i cui dati personali siano stati oggetto di un accesso indebito, ovvero in assenza di documentate ragioni di servizio, suscettibile di presentare un rischio elevato per i loro diritti e libertà fondamentali.

L'art. 34, par. 4, del Regolamento, stabilisce infine che "nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda".

* * *

Alla luce dell'esame delle circostanze portate all'attenzione dell'Autorità e delle considerazioni svolte si ravvisano la necessità e l'urgenza di ingiungere al Titolare del trattamento , ai sensi del combinato disposto degli artt. 34, par. 4, e 58, par. 2, lett. e) del Regolamento, di comunicare individualmente la violazione dei dati personali a tutti gli interessati i cui dati personali e bancari siano stati oggetto di accesso non riconducibile con certezza all'ordinaria attività lavorativa del dipendente, fornendo almeno le informazioni di cui all'art. 34, par. 2, del Regolamento, "senza ingiustificato ritardo" e, in ogni caso, entro venti giorni dalla data di ricezione del presente provvedimento, al fine di assicurare un'efficace tutela agli interessati, in particolare descrivendo la natura della violazione e le sue possibili conseguenze, fornendo i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto appositamente istituito presso cui ottenere maggiori informazioni nonché fornendo notizie sulle misure adottate per porre rimedio alla violazione e per attenuarne i possibili effetti negativi.

Tale comunicazione dovrà essere effettuata attraverso un contatto individuale, preferibilmente attraverso personale appositamente istruito della filiale di radicamento del cliente, nelle modalità che il Titolare riterrà più opportune, individuando un ordine di priorità e un calendario eventualmente differenziato, secondo una tempistica proporzionata al rischio.

La comunicazione deve essere rivolta individualmente e personalmente a ciascun interessato cui si riferiscano i dati oggetto di accesso indebito, quando non vi siano evidenze in merito ad accessi effettuati per esigenze di servizio.

Si richiede, altresì, che le attività di contatto della clientela coinvolta siano dettagliatamente registrate e che vengano documentate in forma scritta, nelle modalità di svolgimento e negli esiti del contatto, nel rispetto del principio di responsabilizzazione.

Dovranno essere altresì documentati gli accessi giustificati da ragioni di servizio del dipendente, esclusi evidentemente dall'azione di comunicazione, nonché gli accessi che, proprio a seguito dell'azione di comunicazione, dovessero essere riconosciuti come legittimi dai clienti perché effettuati nel loro interesse e comunque per ragioni di servizio.

Resta salva ogni altra determinazione all'esito della definizione dell'istruttoria avviata sul caso, anche con riferimento, tra gli altri, agli obblighi in materia di idonee misure tecniche e organizzative volte a garantire la protezione dei dati fin dalla progettazione e per impostazione predefinita, nonché notifica delle violazioni dei dati personali di cui agli artt. 24, 25 e 33 del Regolamento, e che, in ogni caso, ai sensi dell'art. 19, comma 6 del regolamento 1/2019, è fatta salva l'attività di controllo in caso di sopravvenuti elementi di fatto o di diritto ovvero di diversa e ulteriore valutazione del Garante.
Inoltre, si ricorda, ai sensi del combinato disposto degli artt. 58, par. 1, lett. a) del Regolamento e 157 del Codice, che il Titolare del trattamento deve dimostrare all'Autorità di aver adempiuto alle prescrizioni impartite mediante la trasmissione di documentati riscontri al Garante entro il termine di 30 giorni ritenuto congruo nel caso specifico.
Si ricorda, infine, che, ai sensi dell'art. 83, par. 6, del Regolamento, "l'inosservanza di un ordine da parte dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore".

TUTTO CIÒ PREMESSO, IL GARANTE

1) ai sensi del combinato disposto degli artt. 34, par. 4 e 58, par. 2, lett. e) del Regolamento, ingiunge a Intesa Sanpaolo S.p.A. di comunicare la violazione dei dati personali in esame agli interessati coinvolti, nei termini specificati in motivazione, senza ritardo e, comunque, entro venti giorni dalla data di ricezione del presente provvedimento, nei termini di cui in premessa, fornendo almeno le informazioni di cui all'art. 34, par. 2, del Regolamento;
2) ai sensi del combinato disposto degli artt. 58, par. 1, lett. a) del Regolamento e 157 del Codice, ingiunge altresì alla società di trasmettere all'Autorità, entro trenta giorni dalla data di ricezione del presente provvedimento, un riscontro adeguatamente documentato in merito alle iniziative intraprese al fine di dare attuazione a quanto disposto al punto 1);
3) ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019 del 4 aprile 2019, dispone l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2, del Regolamento nel registro interno dell'Autorità, previsto dall'art. 57, par. 1, lett. u) del Regolamento;
4) ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, dispone la pubblicazione del presente provvedimento sul sito internet dell'Autorità.
Si ricorda che il mancato riscontro alla presente richiesta è punito con la sanzione amministrativa ai sensi del combinato disposto degli artt. 83, par. 5, lett. e) del Regolamento e 166 del Codice.
Ai sensi dell'art. 78 del Regolamento, nonché degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il Titolare del trattamento dei dati, entro il termine di trenta giorni dalla data della sua comunicazione.

Roma, 2 novembre 2024

per IL PRESIDENTE
LA VICEPRESIDENTE
Cerrina Feroni

per IL RELATORE
LA VICEPRESIDENTE
Cerrina Feroni
IL SEGRETARIO GENERALE
Mattei