Provvedimento del 19 dicembre 2024 [10106904]

VEDI ANCHE Newsletter del 28 febbraio 2025

[doc. web n. 10106904]

Provvedimento del 19 dicembre 2024

Registro dei provvedimenti
n. 802 del 19 dicembre 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 dott. Claudio Filippi, vice segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito, "Regolamento");

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

VISTO l'accertamento ispettivo effettuato in data 13 giugno 2023 presso la sede operativa di Studio Riabilitazione Creditizia s.r.l.s. (di seguito "Studio Riabilitazione" o "la Società");

ESAMINATA la documentazione in atti;

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

RELATORE la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. L'attività ispettiva nei confronti della società.

Nell'ambito dell'esercizio dei poteri di controllo di cui all'art. 58, par. 1 del Regolamento (v. anche artt. 157 e 158 del Codice), sono stati effettuati dalla scrivente Autorità accertamenti ispettivi nei confronti di Studio Riabilitazione Creditizia s.r.l.s..

L'attività di controllo è originata da una segnalazione ricevuta dalla Banca d'Italia che ha rilevato che il Sig. XX (rappresentante legale dell'anzidetta società) aveva effettuato numerose richieste di accesso ai dati della Centrale rischi della Banca medesima, per conto di persone fisiche, in assenza di una effettiva legittimazione, con conseguente rischio di un utilizzo improprio di dati personali di carattere finanziario indebitamente acquisiti.

All'esito dell'accertamento ispettivo (v. verbale di operazioni compiute del 13/6/2023, nonché note

del 28/6/2023 e del 3/7/2023 con le quali la Società, a scioglimento delle riserve effettuate in sede ispettiva, ha trasmesso la documentazione integrativa), l'Ufficio, avendo riscontrato alcuni profili di criticità meritevoli di una più approfondita analisi, ha formulato una richiesta di informazioni, ai sensi dell'art. 157 del Codice, che tuttavia è rimasta inevasa (v. note del 4/12/2023 e 23/1/2024); a fronte del mancato riscontro, il citato Nucleo speciale, su delega dell'Ufficio (v. nota del 6/3/2024), ha notificato alla Società l'anzidetta richiesta di informazioni - unitamente all'atto di avvio del procedimento sanzionatorio, ai sensi dell'art. 166, comma 5, del Codice, in relazione alla violazione dell'art. 157 del Codice - e ha acquisito le informazioni richieste (v. verbali di operazioni compiute del 15 e 17/4/2024).

Dall'attività istruttoria anzi descritta, sulla base delle dichiarazioni rese dal rappresentante legale della Società, è emerso che:

1. la Società "si occupa principalmente di cancellazione delle segnalazioni nelle centrali creditizie operate dalle banche". La clientela individua i contatti della Società prevalentemente "attraverso il sito www.studioucp.it", ove sono riportate anche le "informazioni sui servizi offerti";

2. nel momento in cui "il cliente contatta telefonicamente la società", lo stesso "riceve un'informativa sul trattamento dati mediante una voce pre-registrata" che gli "fornisce alcune informazioni generali sui servizi offerti"; quindi, "se il cliente accetta, la centralinista acquisisce i dati del cliente (nome, cognome, indirizzo, mail, ecc.) nella banca dati aziendale (Customer Relationship Management, c.d. CRM). In tale CRM vengono memorizzati anche ulteriori dati che nel proseguo del rapporto consulenziale il cliente fornisce, ovvero i moduli firmati e inviati via posta elettronica". La Società, una volta ottenute le deleghe da parte degli interessati, effettua "istanze di accesso o visure presso le centrali rischi private e pubbliche (Banca d'Italia e Camera di commercio) onde meglio definire la posizione debitoria del cliente" e valutare "la fattibilità della cancellazione o della limitazione del trattamento dei dati personali del cliente presso le centrali rischi". Nel caso in cui non rilevi "alcun elemento per procedere alla cancellazione, invia al cliente un ulteriore "questionario" per ottenere maggiori dettagli sulle circostanze lamentate"; quindi "se dall'analisi degli ulteriori dati forniti la Società intravede la suddetta fattibilità, emette un preventivo di spesa che viene trasmesso al cliente tramite e-mail. Se questo accetta la prestazione offerta dalla Società, gli viene inviata via posta ordinaria la documentazione contrattuale comprensiva degli allegati, affinché egli la restituisca, sempre a mezzo corriere, firmata per accettazione. Quindi si avvia l'attività presso gli uffici competenti per richiedere, ad esempio, la cancellazione delle segnalazioni";

3. l'informativa di cui agli artt. 13 e 14 del Regolamento (di cui è stata acquisita copia, v. all. 1 al verbale del 13/6/2023 e, tra gli allegati, v. pag. 43), oltre ad essere pubblicata sul sito www.studioucp.it (cfr. all. 9 al verbale anzidetto), viene resa agli interessati sia telefonicamente, al momento del primo contatto con la Società, sia successivamente, in occasione della sottoscrizione del "modulo di mandato" e della delega ad operare, per loro conto, presso le centrali rischi pubbliche e private (v. contratto di mandato, delega e informativa pagg. 9, 20-22 e 43 del verbale di operazioni compiute del 13/6/2023, nonché all. 8, tra cui, pag. 157). Con la stessa, il cliente viene reso edotto che la base giuridica del trattamento dei dati personali risiede nell'art. 6, lett. b) del Regolamento e che gli stessi sono conservati "per tutta la durata del rapporto contrattuale e, dopo la cessazione del rapporto, limitatamente ai dati a quel punto necessari, per l'estinzione delle obbligazioni contrattualmente assunte e per l'espletamento di tutti gli eventuali adempimenti di legge e per le esigenze di tutela anche contrattuale connessi o da esso derivanti";

4. la Società, nello svolgimento della sua attività, si avvale della collaborazione di diversi soggetti (persone fisiche e giuridiche) rispetto ai quali non sono stati correttamente individuati e/o disciplinati i ruoli privacy, ai sensi dell'art. 28 del Regolamento. In particolare,

dal complesso degli elementi acquisiti, risulta che:

a. la società “Centro Realizzazioni informatiche e finanziarie S.r.l.s.” (v. verbale del 13/6/2023, pag. 5) – il cui rappresentante legale è sempre XX - pone in essere trattamenti di dati personali, per conto e nell’interesse di Studio Riabilitazione creditizia, in assenza di un qualunque atto che, valutati i requisiti di professionalità della società e tenuto conto delle garanzie dalla stessa offerte per la tutela dei diritti degli interessati, la vincoli al titolare definendone gli obblighi e i diritti, nonché i termini e le condizioni dei trattamenti dei dati personali effettuati;

b. ulteriori soggetti intervengono “nel processo di trattamento dei dati dei clienti (…)” in qualità di responsabili del trattamento ex art. 28 del Regolamento; si tratta della società "Ufficio Cattivi Pagatori S.r.l.", anch’essa riconducibile al Sig. XX (socio unico della stessa) e di “alcuni professionisti esterni, consulenti legali o fiscali”, la cui attività “consiste nel ricevere in modalità cartacea la delega firmata dal cliente e le istruzioni delle attività da svolgere, per il singolo caso specifico, presso i diversi uffici pubblici interessati (ad es. presso la camera di commercio, vengono forniti al professionista i protesti e le cambiali) (cfr. all. 3, 4 e 5 al verbale del 13/6/2023). Rispetto a ciascuno di questi soggetti la Società ha predisposto una “Lettera di incarico a responsabile del trattamento” che contiene espresso rinvio a un “contratto di cui costituisce parte integrante”; purtuttavia, a specifica richiesta dell’Ufficio di produrre copia dei contratti in questione “o altro atto giuridico di cui all’art. 28, par. 3 del Regolamento”, la Società non ha fornito alcuna documentazione integrativa (v. verbale 17/4/24, pag. 4).

5. nel corso dell’ispezione è stata acquisita copia del registro dei trattamenti, predisposto ai sensi dell’art. 30 del Regolamento (v. all. 9); inoltre, su richiesta dell’Ufficio, la Società ha confermato di avere designato il dott. XX quale “Responsabile della protezione dei dati personali” ai sensi dell’art. 37 del Regolamento (come si rinviene anche nell’informativa resa ai clienti), precisando di non avere tuttavia effettuato la dovuta comunicazione all’Autorità (v. verbale del 13/6/2023, pag. 6);

6. in merito al sistema informativo, la Società ha dichiarato che il sistema in esercizio è composto da 10 postazioni client e un server, operante nei locali della Società medesima. Alle postazioni, si accede mediante immissione di una username e di una password. Il server opera un sistema informatico di tipo CRM (Customer relationship management) per la gestione del database dei clienti, un prodotto personalizzato e sviluppato da un fornitore esterno.

Dagli accessi effettuati in loco è emerso, fra l’altro, che:

- il “Gestionale CRM” contiene posizioni corrispondenti a n. 74.214 clienti. Per ciascun “record cliente” i dati presenti riguardano nome, cognome, luogo e data di nascita, codice fiscale, dati di contatto (telefono, indirizzo fisico e-mail) un numero identificativo (“NRG”), lo “status” (ovvero se si tratta di un soggetto “già cliente” o “nuovo”, oppure “in esercizio” o “concluso”) nonché altre informazioni relative allo stato della pratica, ivi compresi eventuali appunti in forma testuale e sintetica e lo stato dei pagamenti delle fatture emesse dalla Società, a seguito della lavorazione della pratica;

- in ciascuna scheda cliente, sono presenti anche i report forniti, dalle società e dagli istituti bancari, in riscontro alle istanze di accesso avanzate dagli interessati per il tramite del delegato, dott. XX o XX (v. verbale del 13/6/23, all. 7).

- l’accesso al CRM avviene tramite inserimento di una componente di autenticazione oscurata (password) (v. all. 3 al verbale del 13/6/2023) ed è possibile unicamente dai

locali della Società e senza alcuna possibilità di collegamento, via internet, ai sistemi informatici dall'esterno, "mediante software c.d. di "remote desktop""; la Società ha peraltro dichiarato che la "manutenzione delle postazioni e del software CRM viene effettuata da un soggetto esterno, designato amministratore di sistema, che si reca in loco presso la sede all'occorrenza" (v. verbale 13/6/2023, pag. 6);

- nel CRM "sono stati convogliati anche i dati personali la cui titolarità era delle diverse società che negli anni si sono succedute nell'esercizio dei medesimi servizi; tali dati vengono consultati di volta in volta per la funzionalità di recupero delle insolvenze per i servizi prestati dalle seguenti società: Ufficio cattivi pagatori srl, UCP srl, Centro realizzazioni informatiche e finanziarie, Insurance Global service srl".

Al riguardo, il titolare del trattamento, a cui è stato chiesto di precisare quali siano le società che attualmente accedono — e a quale titolo — alla banca dati aziendale e se esiste, all'interno della stessa, una compartimentazione o una funzionalità che consenta di risalire, rispetto a ciascun cliente, alla società che, in qualità di titolare, ha raccolto e quindi trattato i dati personali del cliente medesimo, è stato specificato che: "attualmente al CRM accede come società solo la "Studio riabilitazione creditizia S.r.l.s", attraverso le persone menzionate. All'interno del CRM negli anni sono confluiti i dati di tutte le società che si sono avvicendate. Ho negli anni avvicendato le diverse società per ragioni fiscali e di opportunità lavorative. Per ognuna delle stesse ho provveduto a raccogliere il consenso da ogni cliente con il quale intrattenevamo rapporti di lavoro. Il consenso veniva raccolto in maniera cartacea. La documentazione concernente i consensi ad oggi, per lo spostamento in diverse sedi, è riposta in una cantina e conservata in un apposito locale. Tengo a precisare che per tutte le società che si sono avvicendate sono sempre stato io l'amministratore unico e quindi il titolare del trattamento. Preciso che il mandato conferito da ogni cliente è riconducibile ad un'unica società e le altre non hanno mai interagito con quel cliente, nonostante i dati siano confluiti tutti in un unico CRM. Anche se negli anni le società si sono succedute nei medesimi servizi, il mandato da ogni singolo cliente è stato conferito ad un'unica società e solo quella società ha avuto rapporti lavorativi con lui. Non c'è una funzionalità nel CRM che ci consente di risalire, per ogni cliente, alla società che ha raccolto i dati. Tutti i dati confluiscono nel CRM in un'anagrafica generale. Chiarisco che nel CRM in argomento sono presenti i dati non solo delle persone che poi sono diventate nostri clienti, ma sono presenti anche dati di persone che attraverso il form sul nostro sito, www.ufficiocancellazioneprotesti.it, hanno semplicemente richiesto delle informazioni e poi non hanno voluto continuare nel rapporto. Quindi non essendo clienti i loro dati presenti nel CRM sono minimi (nome — cognome — telefono). Per quanto di mia conoscenza, e come confermato dalla mia collaboratrice (…), i clienti nel database sono circa 46.000" (v. verbale del 17/4/2024, pag. 9);

8. in merito alla conservazione dei dati, sia quelli in formato digitale sia quelli custoditi in forma cartacea, la Società ha dichiarato che:

- "non sono previste procedure sistematiche di periodica cancellazione dei dati risalenti e, pertanto, la società conserva i fascicoli cartacei e record digitali completi, anche se con detti soggetti la stessa non ha più da tempo rapporti contrattuali in essere; in particolare, "per ciascun cliente vi è un fascicolo cartaceo custodito in un armadio ubicato nella medesima sede. Le pratiche più vecchie sono spostate in un apposito locale ad uso deposito" (v. verbale 13/6/23, pagg. 5-6);

- in ordine alla richiesta di chiarire la congruenza delle dichiarazioni sopra riportate con quanto indicato nell'informativa che viene resa ai clienti ai sensi degli artt. 13 e 14 del Regolamento e riportato nel registro dei trattamenti acquisito agli atti (allegati 1 e 9 al verbale del 13/6/2023), la Società, nel precisare che "il nostro CRM non ha scopi

commerciali e nessun dato che riguarda i clienti viene utilizzato per ricontattarli una volta che il nostro rapporto lavorativo si esaurisce. Manteniamo solo una banca dati complessiva, nella quale sono confluiti negli anni la totalità dei dati", ha altresì dichiarato che provvederà, "quanto prima, a cancellare dal CRM aziendale tutti i dati che non hanno più motivo di permanere nello stesso avendo esaurito le tempistiche fiscali o legali che ci consentono di mantenere il dato"

2. L'avvio del procedimento per l'adozione dei provvedimenti correttivi e sanzionatori.

Nell'ambito del procedimento, la Società è stata destinataria di due distinte notifiche di violazione, ai sensi dell'art. 166, comma 5 del Codice:

la prima, con nota del 6 marzo 2024, in relazione alla violazione dell'art. 157 del Codice, per il mancato riscontro, nei termini, alla richiesta di informazioni avanzata il 23/1/2024 e regolarmente notificata alla stessa dal Nucleo della Guardia di finanza in data 15 aprile 2023;

la seconda, con nota del 3 settembre 2024, in relazione alle violazioni del Regolamento riscontrate, all'esito della documentazione acquisita in sede istruttoria, con riferimento agli artt. 5, par. 1, lett. a), e) e par. 2, 14, 24, 28, 37, 38 del Regolamento, notificata via pec, in data il 3 settembre 2024.

La Società, pur invitata a presentare i propri scritti difensivi o documenti entro 30 giorni dal ricevimento delle citate note (art. 166, commi 6 e 7 del Codice, art. 18 l. 689/1981) - che risultano correttamente notificate – non ha fatto pervenire alcun elemento.

3. Esito del procedimento.

3.1. Osservazioni sulla normativa in materia di protezione dei dati personali rilevante nel caso di specie e violazioni accertate.

All'esito dell'esame delle dichiarazioni rese all'Autorità nel corso del procedimento (della cui veridicità l'autore risponde ai sensi e per gli effetti di cui all'art. 168 del Codice), nonché della documentazione acquisita, risulta che Studio Riabilitazione Creditizia s.r.l.s., in qualità di titolare del trattamento, ha posto in essere trattamenti dei dati personali dei clienti non conformi alla disciplina in materia di protezione dei dati personali, in relazione ai diversi profili di seguito rappresentati.

In generale si evidenzia che il trattamento dei dati personali deve avvenire nel rispetto dei principi indicati nell'art. 5, par. 1, del Regolamento, fra cui quelli di "liceità, correttezza e trasparenza" e di "limitazione della conservazione", ai sensi dei quali i dati personali devono essere – rispettivamente – "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato", nonché "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati" (art. 5, par. 1, lettere a) ed e), del Regolamento).

In particolare, il principio di trasparenza si traduce nell'obbligo, da parte del titolare del trattamento, di fornire all'interessato tutte le informazioni inerenti al trattamento dei dati personali che lo riguardano, in modo accessibile e comprensibile, rendendolo edotto, nel momento i cui i dati personali sono ottenuti, anche delle finalità e delle modalità del trattamento e della base giuridica dello stesso, nonché di tutte le ulteriori informazioni necessarie per garantire che il trattamento sia corretto e trasparente nel rispetto di quanto previsto dagli artt. 13 e 14 del Regolamento (v. anche Cons. 39 del Regolamento).

L'art. 14, par. 1 e 2 del Regolamento dispone inoltre che, nel caso in cui i dati personali "non siano

ottenuti presso l'interessato", il titolare del trattamento è tenuto a fornire allo stesso le informazioni cui ai paragrafi 1 e 2 "entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati" ovvero, "nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali" (art. 14, par. 3 del Regolamento).

Le disposizioni del Regolamento individuano poi specificamente i soggetti – titolare, responsabile – che, a diverso titolo, possono trattare i dati personali degli interessati, stabilendone anche le relative attribuzioni.

In particolare, il titolare è il soggetto sul quale ricadono le decisioni circa le finalità e le modalità del trattamento dei dati personali degli interessati nonché una "responsabilità generale" (accountability) sui trattamenti posti in essere dallo stesso o da altri che effettuino tali trattamenti "per suo conto", ovvero i responsabili del trattamento (cons. 81, artt. 4, punto 8) e 28 del Regolamento).

Il rapporto tra titolare e responsabile deve essere regolato "da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento" (art. 28, par. 3, Regolamento).

Il titolare è altresì competente per il rispetto della disciplina di protezione dei dati personali, dovendo, a tal fine, mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento; ciò "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (artt. 5, par. 2 e 24, del Regolamento).

L'art. 37 del Regolamento ("Designazione del responsabile della protezione dei dati"), nel prevedere i casi in cui la designazione del responsabile della protezione dei dati (RPD) è obbligatoria, stabilisce altresì che, in ogni caso, anche laddove lo stesso sia individuato in via volontaria dal titolare, l'RPD "può essere un dipendente del titolare (o del responsabile) oppure assolvere ai suoi compiti in base a un contratto di servizi".

Le "Linee guida sui Responsabili della protezione dei dati ("RPD")" adottate dal Gruppo di lavoro Art. 29 il 13 ottobre 2016 (emendate il 5 aprile 2017) prevedono infatti che laddove "un'organizzazione designa un DPO su base volontaria, i requisiti di cui agli articoli da 37 a 39 si applicheranno alla sua designazione, posizione e compiti, come se la designazione fosse stata obbligatoria" (v. punto 2.1).

Il RPD, dipendente o meno del titolare del trattamento, dovrebbe infatti poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente (Cons. 97). Il titolare del trattamento è inoltre tenuto a pubblicare i dati di contatto dell'RPD e a comunicarli all'autorità di controllo. (art. 37, parr. 6 e 7 Regolamento).

A norma dell'art. 38 del Regolamento ("Posizione del responsabile della protezione dei dati"), il RPD deve infatti essere un soggetto designato dal titolare (o dal responsabile del trattamento) per assolvere, nei confronti dello stesso, a funzioni di supporto e di controllo, consultive, formative e informative relativamente all'applicazione della normativa di protezione dei dati personali, in piena indipendenza e autonomia, in assenza di conflitti di interessi e senza ricevere istruzioni in ordine all'esecuzione dei suoi compiti, sui quali riferisce direttamente al vertice gerarchico del titolare.

3.2. Violazioni accertate.

3.2.1. Violazione dell'art. 5, par. 1, lett. a) e dell'art. 14 del Regolamento.

In base agli elementi acquisiti nel corso delle verifiche sopra descritte, è risultato che la Società detiene un database nel quale sono registrati i dati personali di oltre 70.000 clienti acquisiti dalle diverse società, facenti capo al Sig. XX, che negli anni si sono avvicendate nei medesimi servizi alla clientela.

Nessuna funzionalità del CRM in questione consente di individuare, rispetto a ciascun cliente, quale sia la società che ha provveduto alla raccolta dei dati personali; i medesimi dati sono altresì conservati, in maniera parimenti indifferenziata, in fascicoli cartacei custoditi nei locali della società oppure, con riferimento ai fascicoli più risalenti, in un magazzino.

In ordine a tale circostanza, si rileva che, relativamente ai dati personali dei clienti i cui dati non sono stati raccolti direttamente da Studio Riabilitazione, ma da una o più delle altre società comunque riconducibili al Sig. XX (e successivamente confluiti nel CRM di Studio Riabilitazione), quest'ultima, nella sua qualità di titolare del trattamento, non è stata in grado di dimostrare – nel corso dell'istruttoria - di aver informato gli interessati di tale passaggi fornendo agli interessati le informazioni previste dall'art. 14, paragrafi 1 e 2 del Regolamento, secondo i termini stabiliti dal successivo paragrafo 3 del medesimo articolo.

La condotta della Società è stata pertanto posta in essere in violazione del principio di "lealtà, correttezza e trasparenza" di cui all'art. 5, par. 1, lett. a) e dell'art. 14 del Regolamento (cfr. par. 3.1).

3.2.2. Violazione dell'art. 5, par. 1, lett. e) del Regolamento.

È stato inoltre accertato che, nel momento in cui il cliente si rivolge alla Società per avvalersi dei servizi della stessa, riceve un'informativa ai sensi dell'art. 13 del Regolamento nella quale risultano esplicitate le caratteristiche essenziali del trattamento, ivi comprese le informazioni relative ai tempi di conservazione dei dati oggetto di trattamento (v. pag. 43 del verbale del 13/6/2023).

Nel modello di informativa acquisita agli atti è riportato che "i dati personali saranno conservati per un periodo di tempo non superiore a quello strettamente necessario al conseguimento delle finalità indicate. I dati personali dei quali non è necessaria la conservazione o per cui la conservazione non sia prevista dalla vigente normativa, in relazione agli scopi indicati, saranno cancellati o trasformati in forma anonima. Si evidenzia che i sistemi informativi impiegati per la gestione delle informazioni raccolte sono configurati, già in origine, in modo da minimizzare l'utilizzo dei dati".

Al contrario, però, dalle verifiche effettuate -e dalle stesse dichiarazioni rese a verbale dalla parte (v. verbale 13/6/23 pagg. 5-6)-, è emerso che, di fatto, la Società non ha individuato precise tempistiche di conservazione dei dati personali trattati, sia con riferimento a coloro che, sottoscrivendo un contratto di mandato, si sono avvalsi dei servizi della Società, sia con riferimento a quanti hanno invece semplicemente richiesto informazioni, senza poi instaurare alcun rapporto contrattuale.

In particolare, la Società, diversamente da quanto riportato nell'informativa resa agli interessati, non ha mai provveduto, dopo la cessazione del rapporto contrattuale, alla cancellazione dei dati personali la cui conservazione non risulti necessaria. Ciò, vale in particolare per i dati di coloro che, dopo aver contattato la Società, non hanno usufruito dei servizi della stessa (che ammontano a diverse migliaia).

Tale condotta risulta pertanto posta in essere in violazione del principio di “limitazione della conservazione”, di cui all’art. 5, par. 1, lett. e), del Regolamento, secondo cui i dati personali devono essere conservati in modo da consentire l’identificazione dell’interessato per un arco di tempo non superiore a quello necessario a conseguire le finalità del trattamento.

Il principio in questione infatti impone al titolare l’onere di valutare la durata del trattamento, in necessaria correlazione con le specifiche finalità prefissate a monte, all’atto della raccolta; ciò al fine di “assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario” (v. Cons. 39 del Regolamento).

Seppure in sede di accertamento ispettivo, la Società si è impegnata a provvedere alla cancellazione, “dal CRM aziendale” di “tutti i dati che non hanno più motivo di permanere nello stesso avendo esaurito le tempistiche fiscali o legali che ci consentono di mantenere il dato", non è stata fornita alcuna assicurazione al riguardo.

3.2.3. Violazione dell’art. 28 del Regolamento.

In sede di accertamento, è emerso altresì che taluni trattamenti sono effettuati, per conto della Società, da alcuni soggetti - persone fisiche e giuridiche – senza che la stessa abbia provveduto, come tenuta, a disciplinarne il rapporto, in conformità a quanto previsto dall’art. 28 del Regolamento.
Il titolare, infatti, può legittimamente decidere di affidare l’effettuazione del trattamento, per suo conto, ricorrendo a responsabili (cfr. art. 28 e Cons. 81 del Regolamento).

In tal caso però l’esecuzione dei trattamenti, da parte di un responsabile del trattamento, dovrebbe essere disciplinata da un contratto (o da altro atto giuridico a norma del diritto dell’Unione o degli Stati membri) che vincoli il responsabile del trattamento al titolare del trattamento e in cui siano specificati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il responsabile del trattamento è pertanto legittimato a trattare i dati degli interessati “soltanto su istruzione documentata del titolare” (v. art. 28, par. 3, lett. a); cfr. anche provvedimento del Garante del 14 gennaio 2021 [doc. web n. 9542113] e, più diffusamente, sul rapporto tra il titolare del trattamento e il responsabile del trattamento, v. le “Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR”, adottate dal Comitato per la protezione dei dati personali il 7 luglio 2021.

Spetta dunque al titolare del trattamento, in virtù della responsabilità generale che su di lui incombe (art. 24 del Regolamento) provvedere alla corretta regolazione dei rapporti tra i diversi soggetti che intervengono nel trattamento (v. artt. 5, par. 2, c.d. “accountability” e 24 del Regolamento).

Nel caso di specie, in sede di ispezione, è emerso invece che il titolare del trattamento si è avvalso della collaborazione di alcuni soggetti in assenza dei presupposti previsti dall’art. 28 del Regolamento. In particolare, come sopra evidenziato (cfr. par. 1, punto 4, lett. a) e b)), si tratta di persone fisiche e giuridiche che effettuano trattamenti di dati personali, per conto di Studio Riabilitazione Creditizia, senza che questa attività sia stata adeguatamente disciplinata da un contratto o altro atto giuridico, o sulla base di una “lettera di incarico” priva però di un alcun reale ed effettivo contenuto, che si limita a riportare formule astratte, prese per lo più dalle disposizioni del Regolamento, senza individuare, in modo specifico, i compiti, gli obblighi e gli ambiti di competenza di ciascun responsabile, come invece previsto dall’art. 28, par. 3, del Regolamento.

Per le ragioni suesposte, ne consegue la violazione, nel caso di specie, sulla base degli elementi acquisiti e di quanto confermato dalla stessa Società nei termini di cui sopra, dell’art. 28 del

Regolamento.

3.2.4. Violazione degli artt. 37 e 38 del Regolamento.

Dalla documentazione acquisita nel corso del procedimento, risulta inoltre che la Società, ha ritenuto di provvedere alla designazione del Responsabile per la protezione dei dati personali (di seguito, "RPD") e ha individuato lo stesso nel dott. XX, rappresentante legale della società medesima.

Di tale designazione, ne è stata data evidenza agli interessati attraverso l'informativa (sia quella pubblicata sul sito della Società, sia quella resa ai clienti medesimi unitamente al modulo di contratto, v. pag. 43 degli allegati al verbale del 13/6/2023), mentre non ne è stata data comunicazione alcuna all'Autorità, come invece disposto dall'art. 37, par. 7 del Regolamento.

Al riguardo occorre evidenziare che "Linee guida sui Responsabili della protezione dei dati ("RPD")" adottate dal Gruppo di lavoro Art. 29 il 13 ottobre 2016 (emendate il 5 aprile 2017) prevedono che laddove "un'organizzazione designa un DPO su base volontaria, i requisiti di cui agli articoli da 37 a 39 si applicheranno alla sua designazione, posizione e compiti, come se la designazione fosse stata obbligatoria" (v. punto 2.1 Linee guida citate).

Si rileva inoltre che l'art. 37, par. 6 del Regolamento prevede espressamente che il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

Come previsto dal considerando 97, "tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".

È di tutta evidenza che il ruolo di RPD è pertanto del tutto incompatibile con quello di rappresentante legale della società presso la quale è designato, in quanto il medesimo soggetto che determina i mezzi e le finalità dei trattamenti non può avere la necessaria indipendenza per esercitare anche i compiti di sorveglianza, sull'osservanza della disciplina e sulle politiche del titolare in materia di protezione dei dati personali, previsti dall'art. 39, par. 1, lett. b), del Regolamento e affidati appunto a un soggetto (anche interno) a cui deve essere tuttavia assicurata una condizione di indipendenza (vedi considerando 97).

Ciò, trova conferma ulteriore anche nel complesso delle disposizioni di cui all'art. 38 del Regolamento, con riferimento alla posizione del responsabile della protezione dati, laddove, tra l'altro, si prevede che il titolare e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione, per quanto riguarda l'esecuzione dei propri compiti, e riferisce direttamente al vertice gerarchico del titolare o del responsabile del trattamento

La valutazione circa l'eventuale sussistenza di incompatibilità connesse allo svolgimento di incarichi che comportano poteri decisionali in ordine ai trattamenti di dati personali (come nel caso del rappresentante legale della società) avrebbe dovuto comportare l'impossibilità del perfezionamento della designazione che, anche ove effettuata, come nel caso di specie, risulta comunque nulla.

L'aver poi inoltre omesso di comunicare all'Autorità i dati del RPD designato, come previsto dall'art. 37, par. 7 del Regolamento, ha peraltro impedito alla stessa di rilevare e segnalare al titolare del trattamento la predetta incompatibilità.

Risulta pertanto accertato che la Società ha designato, quale RPD, un soggetto incompatibile (rappresentante legale), in violazione degli artt. 37, par. 6 e 38 del Regolamento e non ha provveduto a comunicare all'Autorità i dati di contatto dell'RPD, in violazione dell'artt. 37, par. 7 del

Regolamento.

3.2.5. Violazione degli artt. 5, par. 2 e 24 del Regolamento.

Dall'insieme delle violazioni sopra esposte emerge, inoltre, che le misure tecniche e organizzative complessivamente adottate dal titolare al fine di conformare i trattamenti al Regolamento, non sono risultate adeguate alla natura, al contesto, alle finalità e ai rischi dei trattamenti in questione, configurando, in capo al titolare, la violazione del principio di "accountability" di cui agli artt. 5, par. 2 e di quanto previsto dall'art. 24 del Regolamento.

Ai sensi del predetto principio, infatti, il titolare è il soggetto cui è attribuita la "responsabilità generale" del trattamento, gravando, pertanto, sullo stesso l'onere di attuare un sistema organizzativo e gestionale contraddistinto da misure reali ed efficaci di protezione dei dati nonché comprovabili (v. anche cons. 74 del RGPD).

Ciò, in primo luogo, mediante la corretta e puntuale predisposizione degli adempimenti imposti dal Regolamento (informativa, definizione dei rapporti con i soggetti terzi a cui è affidato il trattamento per conto del titolare -responsabili del trattamento-, corretta designazione del responsabile per la protezione dei dati) nonché attraverso l'implementazione di procedure e prassi organizzative atte a conformare i trattamenti alla disciplina di riferimento (quali ad esempio definizione dei tempi di conservazione dei dati e di procedure per la cancellazione automatica dei dati, nonché di procedure per la gestione delle richieste di esercizio dei diritti e dei reclami cfr. Gruppo art. 29, WP 173 del 13 luglio 2010- Opinion 3/2010 on the principle of accountability, pagg. 11-12).

3.2.6. Violazione dell'art. 157 del Codice.

Nell'ambito dell'istruttoria, la Società ha anche omesso di fornire riscontro a una richiesta di informazioni formulata dall'Autorità, ai sensi dell'art. 157 del Codice e regolarmente notificata.
Si evidenzia in proposito che la violazione in questione ha reso necessario il coinvolgimento del Nucleo privacy della Guardia di finanza, incaricato di provvedere alla notifica degli atti e di raccogliere gli elementi istruttori, con conseguente aggravio del procedimento in termini di costi e di tempi.

La violazione dell'art. 157 comporta, ai sensi dell'art. 166, comma 2, del Codice, l'applicazione della sanzione amministrativa di cui all'art. 83, par. 5 del Regolamento.

4. Conclusioni: dichiarazione di illiceità del trattamento. Provvedimenti correttivi ex art. 58, par. 2, del Regolamento.

Per i suesposti motivi l'Autorità, prendendo atto anche che la Società non ha fatto pervenire alcuna osservazione difensiva rispetto ai rilievi notificati dall'Ufficio con gli atti di avvio del procedimento, ritiene che non vi sono elementi che consentano di superare i rilievi medesimi e di disporre l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Il trattamento dei dati personali effettuato da Studio Riabilitazione Creditizia s.r.l.s. risulta pertanto illecito, nei termini su esposti, in quanto posto in essere in violazione degli artt. 5, par. 1, lett. a), ed e) e par. 2, 14, 24, 28, 37 e 38 del Regolamento e dell'art. 157 del Codice.

La violazione, accertata nei termini di cui in motivazione, non può essere considerata "minore", tenuto conto della natura e della gravità della violazione stessa che ha riguardato, tra l'altro, i principi generali, la responsabilità del titolare del trattamento, la definizione dei rapporti con i responsabili del trattamento e la designazione del responsabile della protezione dati, nonché del grado di responsabilità e della maniera in cui l'autorità di controllo ha preso conoscenza della violazione (v. Considerando 148 del Regolamento).

L’Autorità ha altresì ritenuto che il livello di gravità della violazione sia elevato, alla luce di tutti i fattori rilevanti nel caso concreto e, in particolare, la natura, la gravità e la durata della violazione, tenendo in considerazione il numero di soggetti interessati i cui dati personali sono stati trattati dalla Società nel tempo.

Visti i poteri correttivi attribuiti dall’art. 58, par. 2, del Regolamento, alla luce delle circostanze del caso concreto, si ritiene necessario prescrivere le seguenti misure correttive:

- predisporre una procedura in materia di conservazione dei dati personali dei clienti, che ne definisca i termini in relazione alle finalità dei trattamenti e i criteri per la loro cancellazione;

- provvedere alla cancellazione dei dati personali dei clienti la cui conservazione non risulti più necessaria, con particolare riguardo ai dati di coloro che, dopo aver contattato la Società, non hanno usufruito dei servizi della stessa;

- provvedere altresì, ove non già effettuato, alla cancellazione di tutti i dati personali rispetto ai quali la Società si è impegnata in tal senso nel corso del procedimento, essendo decorsi i termini di conservazione consentiti dalla legge;

- provvedere a disciplinare correttamente il rapporto con i soggetti a cui la Società affida il trattamento dei dati personali, per suo conto, mediante l’adozione di un idoneo contratto (o di un altro atto giuridico vincolante) nel rispetto di quanto previsto dall’art. 28, par. 3 del Regolamento;

- provvedere - laddove la Società intenda designare il Responsabile per la protezione dei dati

- a conferire l’incarico a un soggetto idoneo, in possesso dei requisiti previsti dall’art. 37, par. 5, nel rispetto di quanto previsto dagli artt. 38 e 39 del Regolamento.

5. Adozione dell’ordinanza ingiunzione per l’applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i), e 83 del Regolamento; art. 166, comma 7, del Codice).

All’esito del procedimento risulta che Studio Riabilitazione Creditizia s.r.l.s. ha violato gli artt. 5, par. 1, lett. a), ed e) e par. 2, 14, 24, 28, 37 e 38 del Regolamento e l’art. 157 del Codice. Per la violazione delle predette disposizioni è prevista l’applicazione della sanzione amministrativa pecuniaria prevista dall’art. 83 del Regolamento.

Il Garante, ai sensi dell’art. 58, par. 2, lett. i) del Regolamento e dell’art. 166 del Codice, ha il potere di infliggere una sanzione amministrativa pecuniaria prevista dall’art. 83 del Regolamento, mediante l’adozione di una ordinanza ingiunzione (art. 18. L. 24 novembre 1981 n. 689), in relazione al trattamento dei dati personali posto in essere da Studio Riabilitazione Creditizia s.r.l.s. di cui è stata accertata l’illiceità, nei termini sopra esposti.

Ritenuto di dover applicare il paragrafo 3 dell’art. 83 del Regolamento laddove prevede che “se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave”, l’importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5.

Con riferimento agli elementi elencati dall’art. 83, par. 2, del Regolamento ai fini dell’applicazione della sanzione amministrativa pecuniaria e la relativa quantificazione, tenuto conto che la sanzione deve “in ogni caso [essere] effettiva, proporzionata e dissuasiva” (art. 83, par. 1 del

Regolamento), si rappresenta che, nel caso di specie, sono state tenute in considerazione le circostanze sotto riportate:

- in relazione alla natura, gravità e durata delle violazioni, è stata considerata rilevante la natura delle stesse in quanto concernenti l'inosservanza dei principi generali del trattamento e, in particolare, il principio di liceità e trasparenza e di limitazione della conservazione nonché il generale principio di "accountability";

- con riferimento al carattere doloso o colposo della violazione e al grado di responsabilità del titolare, è stata presa in considerazione la condotta della Società e il grado di responsabilità della stessa che ha violato l'obbligo di diligenza previsto dall'ordinamento non dando seguito alle comunicazioni inviate dall'Autorità nel corso del procedimento;

- il rilevante numero di interessati i cui dati sono oggetto di trattamento da parte della Società e su cui si riflettono gli effetti delle violazioni contestate (circa 74.000);

- la scarsa collaborazione con l'Autorità dimostrata dalla Società nel corso del procedimento che ha determinato un aggravio del procedimento, in termini di costi e di tempi;

- a favore della parte si è tenuto conto dell'assenza di precedenti specifici.

Si ritiene inoltre che assumano rilevanza nel caso di specie, tenuto conto dei richiamati principi di effettività, proporzionalità e dissuasività ai quali l'Autorità deve attenersi nella determinazione dell'ammontare della sanzione (art. 83, par. 1, del Regolamento), in primo luogo le condizioni economiche del contravventore, determinate in base al volume d'affari della Società, di cui al bilancio di esercizio per l'anno 2023.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti di Studio Riabilitazione Creditizia S.p.A. la sanzione amministrativa del pagamento di una somma pari ad euro 70.000 (settantamila).

In tale quadro si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito internet del Garante vista la natura e la numerosità delle violazioni che riguardano inosservanze dei principi generali nel trattamento dei dati di migliaia di interessati.

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, rileva l'illiceità del trattamento effettuato da Studio Riabilitazione Creditizia s.r.l.s., in persona del legale rappresentante pro tempore, con sede legale in Roma, Piazzale Clodio n. 22 - P.I. 14339591001, per la violazione degli artt. 5, par. 1, lett. a), ed e) e par. 2, 14, 24, 28, 37 e 38 del Regolamento e dell'art. 157 del Codice;

ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, prescrive alla Società di conformarsi, entro 90 giorni dalla data di notifica del presente provvedimento alle prescrizioni formulate al par. 4 della presente decisione, richiedendo al contempo di fornire, ai sensi dell'art. 157 del Codice ed entro il predetto termine, un riscontro adeguatamente documentato delle iniziative intraprese; si rappresenta che l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. e) del Regolamento;

ORDINA

ai sensi dell’art. 58, par. 2, lett. i) del Regolamento alla medesima Società di pagare la somma di euro 70.000 (settantamila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

INGIUNGE

quindi alla medesima Società di pagare la predetta somma di euro 70.000 (settantamila), secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l’adozione dei conseguenti atti esecutivi a norma dell’art. 27 della legge n. 689/1981.

Si rappresenta che ai sensi dell’art. 166, comma 8 del Codice, resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento - sempre secondo le modalità indicate in allegato - di un importo pari alla metà della sanzione irrogata entro il termine di cui all'art. 10, comma 3, del d. lgs. n. 150 del 1° settembre 2011 previsto per la proposizione del ricorso come sotto indicato.

DISPONE

ai sensi dell’art. 166, comma 7, del Codice e dell’art. 16, comma 1, del Regolamento del Garante n. 1/20129, la pubblicazione dell’ordinanza ingiunzione sul sito internet del Garante;

ai sensi dell’art. 154-bis, comma 3, del Codice e dell’art. 37 del Regolamento del Garante n. 1/20129, la pubblicazione del presente provvedimento sul sito internet del Garante;

ai sensi dell’art. 17 del Regolamento n. 1/2019, 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.

Ai sensi dell’art. 78 del Regolamento, nonché degli articoli 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo individuato nel medesimo art. 10, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 19 dicembre 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL VICE SEGRETARIO GENERALE
Filippi