



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Provvedimento del 6 giugno 2024 [10043007]

VEDI ANCHE: [Newsletter del 9 agosto 2024](#)

[doc. web n. 10043007]

Provvedimento del 6 giugno 2024

Registro dei provvedimenti
n. 341 del 6 giugno 2024

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzone, 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 (di seguito, RGPD);

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 il reclamo presentato ai sensi dell'art. 77 del RGPD dalla signora XX, attraverso l'avvocato XX nei confronti di Drivalia Leasys Rent S.p.A. (in forma abbreviata Leasys Rent S.p.A.) e di CA Autobank S.p.A. (già, FCA Bank S.p.A.);

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 l'avv. Guido Scorza;

PREMESSO

1. Reclamo.

Con reclamo del 25 marzo 2021, l'istante ha rappresentato che Drivalia Leasys Rent S.p.A. (in forma abbreviata Leasys Rent S.p.A., di seguito, la Società) le aveva negato il voucher per il noleggio di un'autovettura in quanto risultava "inserita in una black list".

In particolare, in riscontro alla richiesta di esercizio dei diritti presentata il 28 ottobre 2020 dall'interessata alla Società, quest'ultima comunicava che "in fase prenotativa, [...] procede alla verifica dei dati del contraente attraverso banche dati del Gruppo FCA Bank S.p.A. con lo specifico scopo di prevenzione di truffe ed insolvenze o di altri eventi simili [...] e che ogni richiesta di locazione viene sottoposta ad un esame che si basa su elementi obiettivi che tengono conto di tutti gli elementi presenti nelle banche dati del Gruppo FCA Bank al fine di attribuire un giudizio

sintetico sul grado di affidabilità e solvibilità del richiedente.”

Successivamente, in data 9 dicembre 2020, l'interessata ha inviato alla Società e a CA Autobank S.p.A. (già, FCA Bank S.p.A., di seguito, la Banca), un'ulteriore richiesta volta a conoscere “quali dati e/o informazioni personali avessero in Loro possesso tali da aver causato il diniego di interloquire contrattualmente, l'inserimento della stessa nella "Black List" e per ultima anche l'accusa di essere un "cattivo pagatore" (sebbene non risulti nulla in CRIF)”.

Poiché tale istanza, secondo quanto sostenuto dalla reclamante, sarebbe rimasta priva di riscontro, la stessa ha presentato a questa Autorità il reclamo in esame.

2. L'attività istruttoria.

2.1 Le richieste di informazioni.

In relazione ai fatti richiamati nel reclamo, l'ufficio ha proceduto ad avviare una complessa attività istruttoria sia nei confronti della Società che nei confronti della Banca (con riferimento a quest'ultima, i relativi esiti sono contenuti in un distinto provvedimento, adottato in pari data).

In questo ambito, la Società, con note del 7 luglio 2021 e 15 luglio 2022, è stata invitata a fornire i dovuti chiarimenti in ordine ai fatti oggetto del reclamo.

Con riscontri forniti, rispettivamente, il 26 luglio 2021 e il 3 agosto 2022, la Società ha rappresentato:

- che non risultava “alcun reclamo in data 9.12.2020 da parte Sua o del Suo legale” e che “il DPO [...] non ha ricevuto alcuna richiesta all'indirizzo email [...] indicato nell'informativa di cui [l'interessata] ha preso visione sul sito web della [Società] all'atto della prenotazione”;
- di avere effettuato, come precisato anche nell'informativa resa alla (potenziale) clientela, “[...] la verifica dei Suoi dati attraverso banche dati del Gruppo FCA Bank S.p.A. con lo specifico scopo di prevenire truffe ed insolvenze o altri eventi simili”. Nel medesimo documento è espressamente indicato che “in caso di esito negativo dell'analisi sopra descritta, non sarà possibile erogare il servizio di noleggio richiesto”;
- che “in qualità di società sottoposta a direzione e coordinamento di FCA Bank Spa ex art. 2497 cc, provvede a richiedere, in virtù di rapporti infragruppo, alla medesima la verifica dei dati comunicati dai soggetti interessati nelle banche dati dalla stessa utilizzate”;
- di avere “definito un Data Processing Agreement (di seguito per brevità “DPA”), sottoscritto tra FCA Bank, in qualità di controllante, e le sue controllate, tra cui anche Leasys Rent. La logica sottesa al DPA è quella di regolamentare, in un'ottica di semplificazione, il rapporto tra un Titolare (ciascuna delle società controllate) e un Responsabile (la capogruppo), delegando a quest'ultimo la possibilità sia di gestire determinate tipologie di servizio, per conto del Titolare, che implicassero nel contempo anche attività di trattamento dei personali, quali a titolo esemplificativo e non esaustivo, nei limiti della presente, attività di controllo, servizi amministrativi e di reporting, servizi di contabilità, sia di effettuare le attività di verifica sulla correttezza dei dati personali riferiti a soggetti interessati a noleggiare un autoveicolo presso il Mobility Store di Leasys Rent oppure attraverso modalità online”;
- di richiedere alla clientela nella fase istruttoria di un contratto di autonoleggio: “Anagrafica: Nome, Cognome, Data di nascita, Codice fiscale, Indirizzo di residenza, Indirizzo email, raccolti da Leasys Rent direttamente dall'interessato o in fase di prenotazione o tramite portale web, carta di credito (quest'ultima può essere fornita anche al momento della consegna del veicolo)” e di non raccogliere dati reddituali, ma di svolgere “soltanto verifiche

di legittimità sulla correttezza delle informazioni rese dalla clientela ed in generale sull'assenza di potenziali pregiudizi nel rispetto degli ordinari presidi di controllo tipici e caratterizzanti un gruppo con prevalente componente bancaria e ciò anche al fine di prevenire truffe, furti o altri eventi simili”;

- che i dati reddituali “sono stati verificati da FCA Bank Spa che ha fornito parere negativo alla Scrivente, rispetto all'erogazione del servizio di noleggio richiesto. In particolare, dalle analisi svolte da FCA Bank è risultato un output negativo relativamente ai Documenti di Reddito dall'applicativo Scipafi (Sistema Centralizzato Informatico di Prevenzione Amministrativa Furto di Identità, strumento del Ministero dell'Economia e Finanza). Tale circostanza ha impedito di poter accogliere la Sua richiesta” ed è stata ulteriormente confermata dalla stessa Società sia nella comunicazione del 26 luglio 2021, sia nell'integrazione del successivo 3 agosto 2022, nella quale ha rappresentato che: “è indubbio che Leasys Rent, nel corso dell'istruttoria svolta in fase di prenotazione del veicolo, si è avvalsa dei controlli effettuati per il tramite di FCA Bank, dai quali, come già alla Vs. Autorità comunicato in data 26 luglio 2021, “è risultato un output negativo relativamente ai Documenti di Reddito dall'applicativo Scipafi (Sistema Centralizzato Informatico di Prevenzione Amministrativa Furto di Identità, strumento del Ministero dell'Economia e Finanza)”;

- che il “trattamento dei dati della [reclamante] è stato, quindi, realizzato per le finalità e secondo le modalità presenti nell' Informativa che prevede testualmente che “In fase preliminare Leasys Rent procederà alla verifica dei Suoi dati attraverso banche dati del Gruppo FCA Bank S.p.A. con lo specifico scopo di prevenzione di truffe ed insolvenze o di altri eventi simili.”

2.2 La richiesta di chiarimenti avanzata al Ministero Economia e Finanze.

L'ufficio ha chiesto chiarimenti al Ministero dell'Economia e delle Finanze (MEF) circa l'accesso ai dati reddituali della reclamante contenuti nel Sistema SCIPAFI, effettuato dalla Banca per conto della Società, al fine di valutare se accogliere la richiesta di noleggio.

Il MEF, nel riscontro fornito, ha rappresentato che la Banca, ai sensi dell'art. 30-ter, comma 5, lett. a) del d.lgs. 141/2010, è tenuta a partecipare, quale aderente diretto, al sistema di prevenzione delle frodi,

Il Ministero ha anche rappresentato di avere autorizzato, con nota del 6 luglio 2022, la stessa Banca “ad effettuare interrogazioni sul Sistema SCIPAFI per conto di Leasys Rent S.p.A. [...], in virtù della previsione al comma 7-bis dell'art. 30-ter del d.lgs. 141/2010: ciò in quanto Leasys Rent S.p.A., società di noleggio a lungo termine, non è una società compresa tra le aziende che partecipano al Sistema di prevenzione del furto di identità ai sensi dell'art. 30-ter, comma 5. del suddetto decreto legislativo”.

In particolare il MEF ha valutato di ricomprendere la fattispecie del noleggio a lungo termine nel d. lgs. 141/2010, in linea con quanto previsto dalla Circolare emanata il 17 luglio 2014 dalla Direzione V Prevenzione dell'utilizzo del sistema finanziario per fini illegali. Quest'ultima, infatti, stabilisce che, fermo restando l'ambito soggettivo di applicazione della normativa (come definito dall'art. 30-ter del d.lgs. 141/2010), il comma 7-bis del citato art. 30-ter del decreto, vada interpretato nel senso di ampliare l'ambito oggettivo di applicazione della norma, consentendo, in tal modo, ai soggetti aderenti di avvalersi del sistema di prevenzione anche al di fuori delle fattispecie previste dal comma 7 della stessa disposizione normativa.

2.3. L'attività ispettiva.

Nell'esercizio dei poteri di controllo di cui all'art. 58, par. 1 del RGPD (v. anche artt. 157 e 158 del Codice) e al fine di un compiuto esame della vicenda, l'Autorità ha svolto un'attività di accertamento presso la Società (v. verbale operazioni compiute del 3 aprile 2023), nel corso del quale i rappresentanti della stessa hanno dichiarato che:

- "Drivalia ha cambiato nome da ottobre 2022 da Leasys rent in vista dell'acquisizione del 100% di FCA Bank, controllante diretto di Drivalia, da parte di Credit Agricole Consumer Finance. La precedente capogruppo Leasys, prima controllata da FCA Bank, che si occupa di noleggio a lungo termine, è stata ceduta ad una società posseduta da Credit Agricole CF e da Stellantis. Drivalia si occupa di noleggio a breve termine, in abbonamento, noleggio a lungo termine, in fase di avvio e car sharing";
- "fra Drivalia e FCA bank è stato stipulato un contratto per la prestazione di servizi per l'outsourcing di alcune funzioni, fra cui, ad esempio, la funzione del DPO o l'internal audit. L'ultimo rinnovo del contratto risale a dicembre 2020. In tale contesto, FCA può trattare dati personali di titolarità di Drivalia, in qualità di responsabile del trattamento, in base al DPA intercorrente, dal 2019, fra WinRent (precedente denominazione della società) e FCA Bank";
- "quando un cliente chiede a Drivalia un servizio di noleggio, recandosi presso un mobility store o tramite voucher Amazon, deve fornire i propri dati personali, creando un proprio account, prendendo visione dell'informativa privacy attraverso la scansione di un apposito QR code. I dati anagrafici e i dati relativi allo strumento di pagamento (carta di credito) vengono censiti e confrontati con le banche dati di Drivalia, per verificare la presenza di elementi ostativi al noleggio";
- "FCA Bank effettua periodicamente attività di individuazione dei soggetti indesiderati, a fini antifrode, anche attraverso l'interrogazione di SCIPAFI. Qualora tali verifiche automatizzate evidenzino anomalie, gli analisti di FCA provvedono a verificare tale esito. La lista dei soggetti indesiderati, c.d. watchlist, viene messa a disposizione di Drivalia per i controlli in fase di accettazione delle richieste di noleggio", precisando "che tali verifiche vengono effettuate su tutti i noleggi in abbonamento, che ammontano a circa 12.000 l'anno. A tal fine FCA bank tratta i dati e li conserva secondo quanto indicato dal contratto di servizio";
- in relazione alla posizione della reclamante, la Società ha rappresentato di avere proceduto a cancellare "definitivamente i dati personali dell'interessata dalla watchlist in uso a Drivalia stessa e fornita da FCA Bank dal dicembre 2021, facendo altresì richiesta di cancellazione dalla watchlist di FCA bank" (e-mail di cancellazione di cui la Società ha allegato copia).

In data 21 aprile 2023, la Società, nell'inviare la documentazione integrativa a scioglimento delle riserve, ha:

- presentato il "riepilogo rapporti intercorsi fra la reclamante [...] e le società del Gruppo CA Auto Bank S.p.A.", con il quale (nel rinviare alla ricostruzione della vicenda effettuata dalla Capogruppo) si precisa che "il rifiuto della prenotazione è avvenuto in quanto il nominativo della Reclamante era presente nella Watch List di FCA Bank S.p.A. (oggi "CA Auto Bank S.p.A.") correlato al codice "10" ovvero sia "documentazione reddituale contraffatta" anche in relazione alla ditta individuale" facente capo all'interessata. "Tale Watch List era ed è messa a disposizione di Drivalia per finalità di prevenzione di truffe e insolvenze e altri eventi simili, così come specificato nell'informativa privacy pubblicata sul sito e resa disponibile in fase di prenotazione, come regolamentato dal Data Processing Agreement (DPA) tra Drivalia (Titolare del trattamento) e FCA Bank (Responsabile del trattamento)";
- rappresentato che "il DPA era stato redatto per regolamentare i rapporti relativi al trattamento dei dati tra la società Capogruppo e le società controllate: in altri termini

venivano delegate dai Titolari (ciascuna delle società controllate) al Responsabile (la capogruppo) le attività relative alla gestione di determinate tipologie di servizi. Nel suddetto DPA Intercompany vengono, infatti, elencate a titolo esemplificativo e non esaustivo, le attività di controllo, servizi di contabilità, attività relative al credito queste ultime, limitatamente alle attività di verifiche sulle società di fleet management e non riferite, come più volte precisato, ad attività istruttorie su persone fisiche relative alle offerte di servizio di short term”;

3. L'avvio del procedimento.

Con nota prot. 134255 del 28 settembre 2023, l'Ufficio, sulla base delle dichiarazioni rese dalle parti e degli elementi acquisiti nel corso dell'istruttoria, ha notificato alla Società l'atto di avvio del procedimento per l'adozione dei provvedimenti di cui agli artt. 58, par. 2, e 83 del Regolamento, in conformità a quanto previsto dall'art. 166, comma 5, del Codice, in relazione alla violazione delle disposizioni di cui agli artt.5, par. 1, lett. a), 13 e 28 del RGPD.

In particolare è stato oggetto di contestazione:

- la liceità dell'attività di controllo effettuata dalla Società sui dati dei potenziali clienti al fine di verificare la presenza di cause ostative alla conclusione del contratto di autonoleggio, in quanto effettuata attraverso l'accesso al Sistema SCIPAFI (sistema pubblico di prevenzione del furto di identità istituito dal d.lgs. n. 141/2010, il cui funzionamento è disciplinato dal decreto del Ministero dell'Economia e delle Finanze del 19 maggio 2014, n. 95), attraverso la Banca per conto della Società, nonché l'acquisizione e il relativo trattamento di tali dati (inclusi, per quanto di interesse nel caso di specie, quelli dell'interessata) al dichiarato “scopo di prevenzione di truffe e insolvenze o di altri eventi simili” (v. “Informativa privacy - servizio di noleggjo breve termine Leasys Rent” aggiornata al 13.03.2020 e in atti). Ciò in quanto gli accessi a SCIPAFI effettuati dalla Banca, per conto della Società, al fine di valutare la posizione della reclamante, sono avvenuti in un periodo (tra il 2019 e il 2020) nel quale il Ministero non aveva ancora autorizzato la Banca a interrogare il Sistema SCIPAFI anche per conto della Società che, pertanto, non poteva trattare i relativi dati (ancorché rielaborati e resi disponibili mediante la watchlist creata dalla Banca) al fine di valutare se stipulare o meno contratti di autonoleggio;

- la circostanza che l'informativa fornita all'interessata (v. all.1 alla nota della Società del 3 agosto 2022, sopra richiamata) non contenesse alcuno specifico riferimento alle finalità e relative modalità di trattamento dei dati personali effettuato per il tramite della Banca attraverso l'utilizzo del Sistema SCIPAFI, limitandosi a un generico richiamo alla “verifica dei dati [dell'interessato] attraverso banche dati del gruppo FCA Bank”, risultando in tal modo in violazione dell'art. 13 del RGPD. Al riguardo, si rileva, altresì, che tale richiamo era formulato in termini tali da non consentire di individuare né le banche dati consultate, né se l'accesso a queste ultime fosse effettuato dalla stessa Società o da altre Società del gruppo (ed eventualmente quali), non specificando neppure se queste ultime agissero in veste di titolari o responsabili del trattamento.

- la circostanza che dalla documentazione prodotta in sede istruttoria non emergesse quanto dichiarato, anche in sede ispettiva, circa il ruolo di responsabile del trattamento ricoperto dalla Banca nell'accesso a SCIPAFI per conto della Società. In particolare, se è vero che in base al DPA intercorrente dal 2019, tra WinRent (precedente denominazione della Società) e la Banca, quest'ultima rivestirebbe il ruolo di responsabile del trattamento in relazione ad alcuni trattamenti definiti peraltro come “esemplificativi e non esaustivi”, occorre rimarcare che ciò si porrebbe in violazione dell'art. 28, par. 3 del RGPD, dal momento che attiene a un trattamento dei dati degli interessati che la Banca non poteva effettuare, quale responsabile del trattamento, per conto della Società, non rientrando quest'ultima tra i soggetti che

possono accedere a SCIPAFI né direttamente, né tramite i soggetti aderenti al Sistema.

In secondo luogo, occorre rilevare che il “rinnovo” di tale accordo, stipulato tra la Società e la Banca nel mese di dicembre 2020, dà conto, all’art.10.1, che “con riguardo ai dati che verranno forniti nell’espletamento dei Servizi, Ognuna delle Parti, in qualità di titolare autonomo del trattamento si impegna al pieno rispetto della normativa in materia di protezione dei dati personali [...]”. Dalla lettura del testo emerge, pertanto, l’autonoma titolarità di entrambi i soggetti.

Il 27 ottobre 2023, la Società ha presentato i propri scritti difensivi con i quali ha:

- confermato che l’autorizzazione del MEF all’accesso (indiretto) della Società “a SCIPAFI sia avvenuto in data posteriore all’effettivo accesso da parte di quest’ultima alle informazioni [...], presenti nella watchlist messa a disposizione dalla Banca”.

- ribadito di non avere mai proceduto al trattamento delle specifiche informazioni personali presenti in SCIPAFI riferite alla Reclamante, ma di avere potuto soltanto prendere visione, mediante consultazione della watchlist messa a disposizione dalla Banca, di un codice numerico corrispondente a “documentazione reddituale contraffatta”;

- precisato, in merito ai ruoli (titolare e responsabile del trattamento) da attribuire alla Società e alla Banca in ordine al trattamento dei dati in esame, la qualificazione come “esemplificativi e non esaustivi” dei profili elencati nel Data Processing Agreement (DPA) del 2019, contenuta nella comunicazione datata 3 agosto 2022 in riscontro alla richiesta di informazioni inviata dall’Autorità il 15 luglio 2002, aveva il solo “fine di evitare di riportare tutte le fattispecie elencate, invece, tassativamente nel DPA 2019”, pertanto la Società “pur perfettamente consapevole del fatto che il DPA 2019 era indiscutibilmente migliorabile” ritiene “che tali carenze informative [non] possano addirittura inficiare i requisiti sanciti dall’articolo 28(3) GDPR con conseguente carenza de facto di una regolamentazione in tal senso. Infatti, i requisiti di cui al succitato articolo 28(3) non possono non considerarsi presenti: nelle premesse, oltre alle specifiche finalità del trattamento, sono presenti e/o deducibili, altresì, la materia disciplinata e la natura del trattamento; le categorie degli interessati e il tipo di dati personali sono riportati, rispettivamente, agli articoli 2 e 3; gli obblighi e i diritti del titolare sono rinvenibili in numerosi articoli tra cui, a titolo esemplificativo, nell’articolo 5 relativo ai sub-responsabili”;

- specificato che “il rinnovo del suddetto DPA 2019 non è, in realtà, un rinnovo e nemmeno un accordo ai sensi dell’articolo 28 GDPR, bensì un vero e proprio contratto per prestazione di servizi (in seguito, anche, “Contratto di servizi”) a cui il predetto DPA, necessariamente, si accosta ancorché non esplicitamente richiamato”;

- richiamato l’art.10.1 del citato Contratto che statuisce che “con riguardo ai dati che verranno forniti nell’espletamento dei Servizi, ognuna delle Parti, in qualità di titolare autonomo del trattamento si impegna al pieno rispetto della normativa in materia di protezione dei dati personali [...]”, e confermato “l’ambiguità della citata dicitura [...] in relazione alla titolarità autonoma delle parti, precisando che “detta disposizione deve necessariamente interpretarsi in ossequio ai principi in materia di interpretazione contrattuale di cui agli articoli 1362 e ss. del Codice Civile. Dette disposizioni impongono una lettura organica che tenga conto non solo del DPA 2019, ma anche, e soprattutto, del comma successivo del medesimo articolo 10 il quale recita che la Banca è “autorizzata ad effettuare il trattamento dei dati personali esclusivamente in esecuzione degli obblighi previsti nel presente contratto e, in particolare, per l’esecuzione dei servizi oggetto del medesimo”. La presenza di tale previsione risulta un lampante indicatore dell’impossibilità” di attribuire autonoma titolarità ad ognuna delle parti e confermerebbe, invece, “un rapporto tra titolare (Drivalia) e responsabile del trattamento (Banca) in esecuzione del già citato DPA

2019;

- confermato “il coinvolgimento del responsabile per la protezione dei dati personali in relazione ai succitati contratti. Tuttavia, non è presente un parere formale di quest’ultimo in quanto non prescritto dalla normativa;

- comunicato di avere proceduto alla cancellazione del nominativo della reclamante dalla watchlist;

- quanto all’inidoneità dell’informativa resa agli interessati, nel concordare con l’Autorità circa “la non esaustività della predetta informativa e, in particolare, la mancata menzione delle banche dati consultate”, ha sottolineato che, “in detta informativa la finalità del trattamento in questione era espressamente specificata quale “prevenzione di truffe ed insolvenze o di altri eventi simili” e che, “seppur vero che non viene specificato se l’accesso avviene per il tramite della Banca o direttamente da Drivalia o i ruoli delle stesse, il requisito normativo relativo all’indicazione dei “destinatari” o delle “categorie di destinatari” dei dati personali” è comunque presente all’interno della stessa informativa.

4. Il quadro normativo di riferimento.

4.1. Il sistema Scipafi: art. 30-ter del d.lgs. 13 agosto 2010, n. 141.

Il sistema SCIPAFI, istituito presso il Ministero dell’Economia e delle Finanze -che ne ha affidato la gestione a Consap S.p.A-, è un sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo e dei pagamenti dilazionati o differiti, con specifico riferimento al furto di identità (v. d.lgs. n. 141/2010 e decreto del Ministero dell’Economia e delle Finanze del 19 maggio 2014, n. 95).

Al Sistema e alle informazioni in esso contenuto sono tenuti ad accedere solo i soggetti tassativamente individuati dalla normativa, qualificati aderenti (art. 30-ter, comma 5 e 5-bis, d.lgs. cit.).

Il trattamento dei dati personali degli interessati all’interno dell’archivio (sia da parte del MEF, sia da parte della Consap e dei soggetti aderenti) è consentito per le sole finalità individuate dall’art. 2, comma 2 del d.m. 95/2014, ovvero la verifica dell’autenticità o meno dei dati contenuti nella documentazione fornita dalle persone fisiche (quali interessati), che richiedono una dilazione o un differimento di pagamento, un finanziamento o altra analoga facilitazione finanziaria, un servizio a pagamento differito e “nei casi in cui ritengono utile, sulla base della valutazione degli elementi acquisiti, accertare l’identità delle medesime” (art. 30-ter commi 7 e 7-bis del d.lgs. 141/2010 cit.).

4.2. Le disposizioni rilevanti in materia di protezione dei dati personali.

Il trattamento dei dati personali deve avvenire nel rispetto dei principi indicati nell’art. 5, del RGPD, fra cui quelli di “liceità, correttezza e trasparenza” (art. 5, par. 1, lettere a) del RGPD).

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 anche in relazione ad eventuali responsabili nel rispetto di quanto previsto dall’art. 13 del Regolamento (v. anche cons. 39 del RGPD).

La normativa in materia di protezione dei dati personali individua i soggetti -titolare e responsabile- che, a diverso titolo, possono trattare i dati personali degli interessati, stabilendone anche le

relative attribuzioni.

In tale ambito, 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 titolare 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 è regolato da un contratto, o da altro atto giuridico stipulato per iscritto, che, oltre a vincolare reciprocamente le due figure, fornisce istruzioni al responsabile e prevede in dettaglio (e in maniera esaustiva e non esemplificativa) quale sia la materia disciplinata, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare.

5. Le valutazioni dell’Autorità e l’esito dell’istruttoria.

All’esito dell’esame delle dichiarazioni rese dalla Società nel corso del procedimento (della cui veridicità l’autore risponde ai sensi e per gli effetti di cui all’art. 168 del Codice “Falsità nelle dichiarazioni al Garante e interruzione dell’esecuzione dei compiti o dell’esercizio dei poteri del Garante”) nonché della documentazione acquisita agli atti, si rappresenta quanto segue.

In particolare:

a. in relazione al profilo della liceità del trattamento dei dati dell’interessata tratti da SCIPAFI, la Società, nel confermare che l’autorizzazione del MEF all’accesso effettuato dalla Banca per conto della Società al Sistema SCIPAFI risulta rilasciata il 6 luglio 2022 e, pertanto, in data successiva a quella in cui è avvenuto il trattamento dei dati dell’interessata, ha altresì precisato di non avere mai “proceduto al trattamento delle specifiche informazioni personali presenti in SCIPAFI riferite alla Reclamante”, avendo esclusivamente preso visione del codice numerico (presente nella watchlist sopra menzionata messa a disposizione dalla Banca alle società del gruppo) che indicava come “contraffatta”, la documentazione reddituale dalla stessa presentata.

Nel caso specifico, dunque, risulta comprovato che gli accessi a SCIPAFI effettuati dalla Banca, per conto della Società, al fine di valutare la posizione della reclamante, sono avvenuti tra il 2019 e il 2020, periodo nel quale, come risulta dalla documentazione in atti, la Società (che non rientra tra gli aderenti al Sistema SCIPAFI, specificamente individuati dall’art. 30-ter, comma 5, d.lgs. n. 141/2010 cit.), non risultava autorizzata, neanche attraverso la Banca, ad accedere a SCIPAFI e ad acquisire e trattare i dati ivi presenti e riferiti all’interessata (ancorché rielaborati e resi disponibili alla Società mediante la c.d. watchlist creata dalla Banca), al fine di valutare se stipulare o meno il contratto di autonoleggio. Tale trattamento risulta, pertanto, illecito.

Si osserva, altresì, che il sistema SCIPAFI consente la verifica dell’autenticità dei dati contenuti nei documenti (di identità o reddituali) presentati dall’interessato ai fini della valutazione di una richiesta. Esso, pertanto, presuppone che l’aderente effettui un riscontro puntuale rispetto a uno specifico documento presentato per ottenere la prestazione richiesta;

Nel caso di specie, l’accesso effettuato dalla Banca per conto della Società è illecito in quanto avvenuto senza avere effettuato tale riscontro; risulta, infatti che non sia mai stata acquisita la dichiarazione dei redditi della reclamante, documento indispensabile per effettuare il confronto con le informazioni reddituali riferite alla medesima contenute in SCIPAFI.

b. in relazione al ruolo soggettivo (di titolare o responsabile) ricoperto dalla Società e dalla

Banca, con riferimento all'accesso ai dati dell'interessata tratti da SCIPAFI e oggetto di successiva elaborazione e inserimento nella watchlist, la Società medesima, pur dichiarandosi consapevole che la documentazione prodotta (in particolare, il DPA 2019 e il successivo atto denominato "rinnovo" del 2020), risulti poco chiara sul punto, ritiene, tuttavia, che tali carenze non inficino i requisiti previsti dall'art. 28, par. 3 del RGPD e che emergerebbe comunque dagli atti un rapporto di titolare e responsabile rispettivamente in capo alla Società e alla Banca.

A tal riguardo si rileva che all'epoca dei fatti, la Banca, in qualità di autonomo titolare del trattamento, era tenuta ad accedere a SCIPAFI esclusivamente nell'ambito dello svolgimento della propria specifica attività (art. 30-ter, commi 7 e 7-bis, d.lgs. 141/2010, cit.); diversamente, nel caso di specie, l'accesso è stato effettuato per valutare la posizione dell'interessata ai fini della stipula di un contratto di noleggio (che esula dalle attività proprie della Banca) con la Società (che costituisce un soggetto diverso dalla Banca, ancorché appartenente allo stesso gruppo).

Ne discende che la Società, che non rientrava tra i soggetti che, all'epoca dei fatti, potevano accedere a SCIPAFI né direttamente, né tramite i soggetti aderenti al Sistema, non poteva trattare i dati dell'interessata né in veste di titolare del trattamento né designando a tal fine la Banca quale responsabile, con l'effetto che l'attribuzione di tale ruolo alla Banca da parte della Società si è posto in violazione dell'art. 28 del RGPD;

c. pur confermando l'inidoneità dell'informativa resa all'interessata, in quanto generica e comunque non idonea a consentire a quest'ultima di individuare la tipologia dei dati trattati, l'origine degli stessi, con specifico riferimento alle banche dati consultate e se l'accesso a queste ultime fosse effettuato dalla stessa Società o da altre del gruppo, l'Autorità prende atto di quanto dichiarato e documentato dalla Società in ordine all'intervenuta sostituzione della precedente informativa con quella "presente sul sito internet della Società reperibile al seguente indirizzo: <https://www.drivalia.it/it/customer-service/privacyservizio/>.

6. Conclusioni: illiceità dei trattamenti effettuati.

Alla luce delle valutazioni che precedono, si rileva che le dichiarazioni rese dal titolare del trattamento negli scritti difensivi della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice non consentono di superare tutti i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentirne l'archiviazione, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del regolamento del Garante n. 1/2019, concernente le procedure interne all'Autorità aventi rilevanza esterna.

I trattamenti posti in essere dalla Società risultano illeciti nei termini sopra esposti, in relazione agli artt. 5, par. 1, lett. a), 13 e 28 del RGPD.

La violazione delle disposizioni sopra richiamate comporta l'applicazione della sanzione amministrativa prevista dall'art. 83, par. 4, lett. a); par. 5, lett. a) e b), del RGPD.

7. 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).

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, par. 5, del Regolamento, mediante l'adozione di una ordinanza ingiunzione (art. 18. legge 24 novembre 1981 n. 689).

La violazione, accertata nei termini di cui in motivazione, non può essere considerata "minore",

tenuto conto della natura, della gravità, del grado di responsabilità e della maniera in cui l'autorità di controllo ha preso conoscenza della violazione (cons. 148 del Regolamento).

Con riferimento agli elementi elencati dall'art. 83, par. 2, del Regolamento ai fini della 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 considerate le seguenti circostanze:

- in relazione alla natura e gravità della violazione, sono stati considerati rilevanti la natura della violazione che ha riguardato l'organizzazione dell'intero trattamento con riferimento ai ruoli rispettivamente ricoperti dalla Società e dalla Banca al tempo in cui è avvenuto il fatto e, nello specifico, la liceità del trattamento dei dati riferiti all'interessata;
- in relazione al carattere doloso o colposo delle violazioni va tenuto conto della condotta della Società che -pur essendo consapevole dell'assenza di autorizzazione del MEF a conoscere, anche mediante la Banca, le informazioni contenute in SCIPAFI- ha ritenuto di accedere alla watchlist messa a disposizione dalla Banca nella quale erano contenute informazioni tratte anche dal suddetto Sistema, ancorché successivamente rielaborate;
- la cooperazione fornita dalla Società nel corso dell'istruttoria e gli adeguamenti disposti nel rispetto del principio di accountability (attraverso l'instaurazione di un nuovo assetto contrattuale più strutturato, avendo siglato un nuovo contratto di servizi con annesso un nuovo accordo ai sensi dell'articolo 28 del RGPD) e dei principi di privacy by design e privacy by default mediante l'implementazione di misure volte ad eliminare la visibilità della motivazione pregiudiziale collegata alla causale numerica così come trasmessa dalla Banca mediante la watchlist;
- l'assenza di precedenti pronunce da parte dell'Autorità nei confronti della Banca rispetto alla medesima fattispecie, nonché di reclami analoghi a quello oggetto del presente provvedimento.

Si prende atto, infine, che, nel corso del procedimento la Società ha aggiornato l'informativa in conformità alle previsioni contenute negli artt. 5, par. 1, lett. a) e 13 del RGPD, non sussiste, pertanto, il presupposto di ingiungere di conformare il trattamento alle disposizioni del RGPD rispetto a tale profilo.

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), si ritiene che assumano rilevanza nel caso di specie, le condizioni economiche del contravventore, determinate in base ai ricavi conseguiti dalla Società con riferimento al bilancio ordinario d'esercizio per l'anno 2022.

Ritenuto, altresì, di dover applicare il paragrafo 3 dell'art. 83 del Regolamento che 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, lett. a), del Regolamento.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene di dovere adottare, nei confronti di Drivalia Leasys Rent S.p.A. (in forma abbreviata Leasys Rent S.p.A.) - C.F./P.I. 05406791003, con sede legale in Torino, Corso Orbassano 367, la sanzione amministrativa del pagamento di una somma pari a euro 250.000,00 (euro duecentocinquantamila,00).

In tale quadro si ritiene, altresì, in considerazione della tipologia delle violazioni accertate, 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 provvedimento sul sito Internet del Garante e che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO, IL GARANTE

rileva l'illiceità del trattamento effettuato da Drivalia Leasys Rent S.p.A. (in forma abbreviata Leasys Rent S.p.A.) - C.F./P.I. 05406791003 - in persona del legale rappresentante pro tempore, con sede legale in Torino, Corso Orbassano 367, ai sensi dell'art. 143 del Codice, per la violazione degli artt. 12, par. 3, e 15 del Regolamento;

ORDINA

ai sensi dell'art. 58, par. 2, lett. i), del Regolamento, a Drivalia Leasys Rent S.p.A. (in forma abbreviata Leasys Rent S.p.A.), di pagare la somma di euro 250.000,00 (euro duecentocinquantamila,00) 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 250.000,00 (euro duecentocinquantamila,00) 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 ricorda che 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 dell'1.9.2011 previsto per la proposizione del ricorso come sotto indicato (art. 166, comma 8, del Codice);

DISPONE

la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, e ritiene che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

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, 6 giugno 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei