



THE ITALIAN DATA PROTECTION AUTHORITY - “GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI”

At today's meeting, which was attended by Prof. Pasquale Stanzone, President, Prof. Ginevra Cerrina Feroni, Vice-President, Mr. Agostino Ghiglia and Mr. Guido Scorza, Members and Fabio Mattei, Secretary-General;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter “GDPR”);

HAVING REGARD TO Legislative Decree No 196 of 30 June 2003 (Personal Data Protection Code, hereinafter ‘the Code’) as amended by Legislative Decree No 101 of 10 August 2018 laying down “Provisions to adapt the national legislation to Regulation (EU) 2016/679”;

HAVING REGARD TO [REDACTED] complaint of 2 November 2021 filed with the Norwegian Data Protection Authority alleging a breach of their personal data by Avis Budget Italia S.p.A.;

CONSIDERING the cooperation mechanism between the European data protection authorities, as provided for in the Regulation (Article 60 et seq.) for cross-border processing of personal data, and in particular the Article 56 IMI procedure opened on 14 January 2022 by the Norwegian authority for the identification of the lead authority in the processing of the procedure;

HAVING EXAMINED the documents in the case file;

HAVING REGARD TO the considerations made by the Secretary-General pursuant to Article 15 of Regulation No 1/2000 of the Garante;

Acting on the report submitted by Mr. Agostino Ghiglia, Member of the Garante’s Panel;

PREAMBLE

1. The complaint and the investigation

By a complaint lodged with the Norwegian Data Protection Authority, two Norwegian nationals ([REDACTED]) complained that they had received, on their return from a journey between Italy and Croatia, a fine for driving in prohibited areas from the “*Italian police*”, as well as a complaint for failure to pay motorway tolls from [REDACTED] (a debt collection company, as subsequently established, on behalf of [REDACTED] the Italian motorway service licensee (concessionaire), even though they had not been in Italy at the time when the road traffic offences were allegedly committed.

They therefore complained of an alleged breach of the rules on the protection of personal data by Avis Budget Italia, from which the complainants had rented a car at Venice airport (the complainants had initially contacted Avis Budget Norway to book the vehicle which was then made available by Avis Budget Italia, part of Avis Budget Group): apparently, the company

incorrectly associated the personal data relating to the complainants with a number plate not corresponding to the car rented by them (as evidenced by documents in the file); as a result, the complainants were notified of administrative penalties by the above-mentioned third parties (“Italian police” and ██████████), however the relevant proceedings were subsequently terminated, at the request of Avis itself. In their complaint, the data subjects also claimed that Avis had “*cause[d] them a long and difficult process, [...and] a lot of work even though we had nothing to do with any of the [notified] violations*”.

The Garante – the lead authority in the cooperation procedure under Article 60 GDPR for the cross-border processing in question, as Avis Budget Italia was found to be the sole controller in the data processing at stake– sent the company, by letter of 16 February 2022, a request for information on what had happened.

Via a note dated 28 March 2022, Avis Budget Italia (hereinafter “Avis”) provided an initial response to the Garante, confirming, in particular, that “*the data relating to the complainants had been communicated to the Carabinieri in relation to a violation of no access and no-parking signs, as well as to the company ██████████ due to the failure to pay a motorway toll*”, adding that “*the erroneous communication is attributable to a mere technical error relating to the association between the identification data of the actual driver and the license plate of the rented vehicle with respect to the period in which, respectively, the violation of the traffic limitation rules and the failure to pay the motorway toll occurred.*”

The company (Avis) also clarified that “*the communication of the personal data of the renting customer by the car rental company is made in accordance with [...] both a legal obligation (combined provisions of Sections 84, 12-a and 196 of the Highway Code) and a duty of collaboration with the competent law enforcement authority [...] or the Authority managing the public motorway concession*”, but that in the case addressed by the complaint “*there appears to have been an error of association between their name as renters and the registration number of the vehicle that was actually liable for non-payment of the toll and violation of road traffic rules*”.

Having taken note of what the controller has stated as well as of the proactive stance taken by the latter, which had requested the aforementioned third parties to rectify the data and to cancel the proceedings wrongly involving the complainants, this Authority still found it necessary to obtain clarifications from Avis in order to better understand the process that gave rise to the communication to third parties of incorrect personal data referring to the complainants and to verify any violations of the rules on the protection of personal data.

This Authority therefore sent a new request for information to the data controller, pursuant to Section 157 of the Italian DP Code (also following the submission of additional documents by the Norwegian authority) requesting further clarifications, while representing the company the legal consequences in case of false declarations, exhibitions or documentation to the Garante (Article 168 of the Code).

The controller, in providing new feedback to the Garante, stated that “*as regards the facts dating back to 2019 [...] Avis has made any necessary corrections, taking charge of any necessary communication activities to the interested parties and without any consequences for the customer concerned*”, specifying, inter alia, that:

- “*the data are provided to Avis on the initiative of the requesting customer as part of the conclusion of a vehicle rental contract [...].*”
- “*The provision of customer data also allows AVIS to fulfil specific regulatory obligations to identify and communicate to the authorities (“Questure”) the relevant data [...of the] drivers of a motor vehicle (with reference to [Decree-Law No 113 of 2018, converted by] Law 132/2018 and related Ministerial Decree of 29 October 2021) [...]. In the event of infringements or omissions to be attributed to the persons concerned, the public authorities responsible for road traffic control and motorway service licensees shall, in*

any event, notify Avis (being the car rental company which owns the vehicle) of requests for driver identification [...];

- the data relating to the customer and the related rental are therefore processed and stored on the AVIS IT system for contractual, legal and administrative purposes [...]. Furthermore, with regard to the specific circumstances of the case in question, the retention of rental data also allows AVIS to respond to requests for driver identification from public authorities in relation to claims of violation of traffic rules provided for by the Highway Code or local regulations, as well as requests from motorway service concessionaires in the event of a dispute over non-payment of the toll, as indicated above;
- the requests for identification of drivers of rental vehicles, upon receipt of notifications (in the form of a paper report or communication via certified e-mail) by AVIS, are subsequently managed by the company ██████████, which is an outsourcee of AVIS (on the basis of a service contract) and has been appointed as processor, [...], by searching for the relevant data corresponding to the notifications on the IT system and communicating them to the authorities and concessionaire bodies. As previously communicated, this is based both on a legal obligation for AVIS (pursuant to the combined provisions of Sections 84, 126-a and 196 of the Highway Code) and on the duty by AVIS to cooperate with the requesting authorities and concessionaires to provide such identification data upon reasoned request, as resulting from the relevant findings in the AVIS system on the basis of correspondence with the license plate number and date of the disputed violation.
- In the case in question, however, what was subsequently ascertained both following the customer's report and following internal verification that led to the cancellation of the related requests for administrative infringements and non-payment of motorway tolls, with the closure of the related files [...], it appears that the data provided did not correspond to those of the customer who had actually rented the vehicle [...] and to whom they should therefore have been correctly attributed.
- In fact, after having carried out every appropriate check (as is the case whenever – which seldom happens - a possible anomaly is reported on the consistency of the rental data pending such disputes), it was found that the incorrect association of the above data occurred as a result of a clerical error attributable to the manual entry of data for the purpose of rental registration by the operators on duty at the rental station, [...] resulting in the incorrect identification of the complainant as the driver of the vehicle itself on the dates on which those violations had occurred;
- It is also possible that the customer requests and obtains a different type of vehicle than the one assigned by the system according to the specifications previously provided by the customer himself or that a vehicle already pre-assigned is returned late or early [...] leading to a reallocation of the vehicle. In these cases, in spite of the care taken by the operator in inserting the necessary correction, there is the possibility, although absolutely infrequent, that there is an overlap of dates or rental time [...].
- As a rule, however, in these cases the system signals an anomaly, which is therefore promptly corrected, but it cannot be absolutely excluded that a temporary permanence in the data system for so-called 'void' rentals may occur (i.e. a rental that is closed suddenly on request or because of changed customer needs [...] or for technical reasons) with the resulting very rare incorrect associations of rental dates or times with respect to a vehicle [...], which are then systematically ascertained and corrected ex post in the shortest time technically possible, as part of internal controls or upon customer reporting, and in all cases without any consequence for the customer himself in terms of

charging errors, for which AVIS bears full responsibility;

- *it is possible that [following the forwarding of notifications by Avis] “relating to disputes on infringements of road traffic rules or failure to pay motorway tolls by the authorities and bodies in charge [...] to ██████████ [...] a date different than that relating to the alleged violation may have been manually entered, at the time of the search by ██████████ ██████████ to follow up on the requests for identification of drivers [and] data different from those of the actual driver concerned and, in particular, those of the customer who subsequently reported the circumstance as incorrect were returned.*
- *an incorrect association between the reference date and time for the alleged infringements and the vehicle number plate, resulting from one of the above circumstances, has unfortunately led to incorrect communication of the driver’s data, which has, however, been corrected. It is therefore reiterated that the events at issue did not result from an IT system shortcoming or from an inconsistency in the matching of data operated by the system, but only from a human error made by the operator [...] in the data entry phase [...] probably due to last minute changes requested by the customer or else to the management of early or delayed vehicle returns.*
- *It should also be noted that the facts at issue date back to 2019, whereas our systems have in the meantime been periodically and significantly updated also by way of the adoption of technical solutions that were intended, among other things, to reduce the risk that data entry [...] or any other] manual intervention by an operator [...] may incidentally lead to a mismatch or a lack of consistency in the rental records, also with the help of appropriate preventive reporting or monitoring tools.*
- *AVIS remains committed to constantly improving its systems precisely to minimize these risks as much as possible [...]; as part of its accountability as Data Controller [Avis] undertakes to devote its best technical resources to the aforementioned [regular] updating of the systems regarding the detection and reporting of anomalies in order to further reduce the already remote possibility that similar accidental mismatches, however rare, may recur in the future.*
- *AVIS responds to notifications received in compliance with legal obligations and in a spirit of collaboration, but it plays essentially a "vicarious" role with respect to the requirements for identification of alleged offenders and fining injunctions for public interest purposes [...] in terms of dutiful collaboration in the management of a driver identification request; however, all of this is in itself alien to the purposes of its processing activities as Data Controller (i.e., the provision of rental services, as opposed to the notification of alleged violations);*
- *In conclusion, [...] a mere clerical and human error in entering data temporarily gave rise to subsequent incorrect communications to the requesting motorway authorities and bodies, however as mentioned above this error was fully addressed following the complaint and subsequently led to requests [for] correction on the initiative of AVIS which were granted by those authorities and bodies;*
- *there are currently no relevant cases or reports relating to the processing of the data of rental customers [...].”*

2. Assessment of the Authority and conclusions

According to Regulation (EU) 2016/679 on data protection (“GDPR”), the processing of personal data must be carried out in accordance with the fundamental principles set out in Article 5 (e.g. lawfulness, fairness, transparency, purpose limitation, minimisation, accuracy, integrity and confidentiality of data) and, in order to be lawful, it must rely on one of the legal bases referred to in Article 6 GDPR (including: consent of the data subject, performance of a contract,

fulfilment of a legal obligation, performance of a task carried out in the public interest, legitimate interest of the controller). The basis for processing data for compliance with a legal obligation must be determined by the law of the Union or of the Member State to which the controller is subject (Article 6(3)).

Furthermore, according to Article 24 GDPR, taking into account the nature, context and purposes of the processing, as well as the risks to the rights and freedoms of individuals, the controller shall implement appropriate technical and organisational measures to ensure, and be able to demonstrate, that the processing complies with the GDPR; those measures shall be reviewed and updated where necessary.

Article 32 GDPR specifies security obligations, stipulating that: “the controller and the processor shall put in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk [...]. When assessing the appropriate level of security, special account shall be taken of the risks presented by the processing resulting in particular from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

With regard to the legal basis of data processing in the present case, it is apparent from the documents gathered that Avis initially processed the data relating to the complainants for the performance of a contract (Article 6 para. 1, (b)) and that, likely, due to a clerical error at the *data entry* stage, the data of the complainants were associated with the registration plate of a vehicle not attributable to them.

Following requests for the identification of the driver by the Italian public authority and the concessionaire for motorway services, in relation to claims of infringement of the Highway Code and non-payment of motorway tolls, Avis itself, in line with Article 6(1)(c) and (f), provided those third parties with the data relating to the complainants – as presumably resulting from the activity of managing the requests for identification of the drivers of the vehicles. As also indicated in the information provided by Avis, the latter may, in fact, be required to perform such communication by law, as well as for a legitimate interest (in particular in the event of any disputes, for the defense of their rights).

More specifically, it was found that, in the context of the communication of driver data by Avis to the aforementioned entities (Carabinieri and motorway service concessionaire-[REDACTED]), which activities are in principle lawful on the basis of the European and national regulatory framework (Article 6(1)(c), (f) and para. 3 GDPR; Sections 126a, 176, 196, *inter alia*, of Legislative Decree No 285/1992, the Italian Highway Code), in the specific case *a personal data breach occurred, i.e. ‘the breach of security leading to accidental or unlawful destruction, loss, modification, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed’* (Article 4(12) of the GDPR) on account of the undue communication of personal (non-sensitive) data, given that the complainants are not the actual offenders.

However, the analysis of the documentation gathered showed that the cause of that breach was a human error, which occurred during the data entry phase, and not an IT or operational problem with the system used by Avis. The data controller promptly corrected the data in its internal systems and requested their correction to the aforementioned entities and it also had the offences for violation of the highway code cancelled, as also confirmed by the data subjects. Furthermore, the controller stated that it had updated the technical and organisational measures used during the proceeding, in particular regarding the detection and reporting of anomalies in order to further reduce the possibility of such errors (see also the EDPB “Guidelines 9/2022 on personal data breach notification under GDPR, Adopted 28 March 2023”).

As also pointed out in the EDPB Guidelines no. 01/2021 on examples regarding the notification of a personal data breach, para. 78, “*In this case, the infringement does not result from deliberate action by an employee, but from accidental human error caused by inattention. This type of infringement can be prevented or made less frequent [...]*” by a series of technical

and organisational measures referred to therein. In such cases, moreover, the Guidelines do not provide, among the necessary actions to be taken on the basis of the risks identified, either for notification to the supervisory authority or to the data subject within the meaning of Articles 33 and 34 GDPR.

Furthermore, it should be borne in mind that, under Article 57(1)(d) of the GDPR, the DP Authority has, inter alia, the task of promoting data controllers' awareness of their obligations under the GDPR.

The Garante, the lead supervisory authority, informed the concerned supervisory authorities of the investigation and shared its position on the matter.

In particular, having taken note of the reply provided by the Company, also pursuant to Section 168 of the Privacy Code and in line with the EDPB Guidelines 02/2022 on the application of Article 60 of the GDPR, adopted by the EDPB on 14 March 2022 (paragraph 232, 233, 234), this Authority proposed not to take any corrective action pursuant to Article 58 para. 2 GDPR against the controller, and to rather adopt a decision pursuant to Art. 60 para. 7, in order to close the procedure, while inviting the data controller to constantly check the adequacy of the technical and administrative measures relating to data processing operations (including adequate training of staff) to avoid (or promptly detect) similar errors in the future (Article 57 para. 1, letter d) GDPR).

The Authority reached that conclusion taking into account all the circumstances of the case and, in particular, that the mix-up appeared to be due to human error of an occasional nature and that the data controller (which, in principle, is required under Italian law to share driver's data with the aforementioned requesting entities) proactively took steps to reduce or eliminate the impact of what happened on the data subjects.

This is also in line with the provisions of EDPB Guidelines 2/2022, according to which, in the light of the result obtained and the specific circumstances of the case, *'the supervisory authority may consider that the most appropriate decision in relation to the complaint in question is to close the procedure, taking note of the solution reached and without taking any action against the controller'* and after *'a careful assessment of the circumstances of the complaint as a whole [...]*' (EDPB Guidelines 2/2022 on the application of Article 60 para. 232, 233).

According to Article 60 para. 4-6, as no objections were raised by the authorities concerned within the four-week deadline, the draft decision became binding on the authorities concerned and on the Garante (lead authority).

Therefore, this Authority finds that the procedure in question should be finalised, pursuant to Article 60(7) of GDPR, without the adoption of corrective/fining measures pursuant to Article 58(2) of GDPR, given that the breach entailed a level of risk to the rights and freedoms of data subjects that can be considered low (see EDPB Guidelines 01/2021, *cit.*). However, this Authority considers it appropriate, pursuant to the aforementioned Article 57 para. 1, letter *d*) GDPR, to invite the data controller to constantly check the data security measures (and in particular, technical and organizational measures) to prevent similar human errors, also in the light of what is highlighted by the EDPB Guidelines 01/2021: *"It is important to identify first how human error could have occurred and, where appropriate, how it could have been avoided. In the specific case, the risk is low, since no special categories of personal data have been involved, or other data the misuse of which could have significant adverse effects, the breach does not result from a systemic error on the part of the controller and only two persons are affected"* (para. 107 Guidelines 01/2021).

The Garante, therefore, adopts this decision and notifies it to the data controller, pursuant to Article 60 para. 7, GDPR, in the light of its role as lead supervisory authority being *"the sole interlocutor of the controller who is the subject of the complaint in question"*. Data subjects will be informed through the complaint-receiving authority – in this case, the Norwegian authority

(Guidelines 2/2022 EDPB, para. 234).

BASED ON THE ABOVE PREMISES, THE GARANTE

Pursuant to Article 60(7) of the GDPR and Section 143(3) of the Italian DP Code, Section 14 and 18 of Regulation No 1/2019 of the Italian Data Protection Authority on internal procedures with external relevance for the performance of the tasks and exercise of the powers delegated to the Italian Data Protection Authority, orders the closure of the procedure in question, without the adoption of corrective and fining measures, for the reasons set out above and in line with the EDPB Guidelines 2/2022 on the application of Article 60 of the General Data Protection Regulation, adopted on 14 March 2022, paras. 232, 233, 234;

In accordance with Article 57(1)(d) of the GDPR, Avis Budget Italia S.p.A. is invited to constantly check the adequacy of the technical and administrative measures relating to data processing operations (including adequate staff training) in order to avoid (or promptly detect) similar errors in the future.

This decision is notified to the data controller and communicated to the persons concerned through the Norwegian authority which received the complaint.

Pursuant to Article 78 of the Regulation and Section 152 of the Code, this decision may be challenged before a judicial authority by filing an appeal either with the court of the place where the data controller resides or is established or with the court of the complainant's place of residence within 30 days from the date of communication hereof, or else within 60 days if the appellant resides abroad.

Rome, 17 July 2024

THE PRESIDENT

THE RAPPORTEUR



GHIGLIA AGOSTINO
signed



PASQUALE STANZIONE
signed

THE SECRETARY-GENERAL



FABIO MATTEI
Signed