[doc. web no. 9023986]

Injunction against Autosat S.p.A. - May 31, 2018

Register of measures

no. 371 of 31 May 2018

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, in the presence of Dr. Antonello Soro, president, of dott.ssa Augusta Iannini, vice president, of dott.ssa Giovanna Bianchi Clerici and of prof.ssa Licia Califano, members and of dott. Giuseppe Busia, general secretary;

NOTING that the Guardia di Finanza, special privacy unit, with minutes nos. 86 and 87 of 25 July 2016 (both notified on 9 August 2016), and no. 8 of 25 January 2017 (notified on 13 February 2017) which must be understood as fully reported here, contested the company Autosat S.p.A., in the person of its pro-tempore legal representative, with registered office in Surbo (LE), via Unità d'Italia no. . 1, tax code 03575990753, the violations foreseen by the articles 26, 33, 37, 38, 162, paragraph 2-bis and 163 of the Code regarding the protection of personal data (legislative decree no. 196 of 30 June 2003, hereinafter referred to as the "Code");

NOTING that from the examination of the documents of the sanctioning procedure initiated with the contestation of administrative violation, the following emerged, in summary:

- The special privacy unit of the Guardia di Finanza carried out inspections against Autosat S.p.A., on 24, 25 and 26 May 2016, as part of the six-monthly inspection program established by the Guarantor;

- during the audit, checks were carried out on the computer workstations in use at the company, the operating methods of the video surveillance system and the nature of the data processed for the performance of commercial activities;

- with reference to the computer workstations, it was possible to ascertain that to access the computer used by one of the company's employees, which contained documents containing the customers' personal data, it was necessary to enter a password of only 4 alphanumeric characters;

- with reference to the video surveillance system, it was found that the device in which the images taken by the system used by the company were stored was accessible without passing an IT authentication procedure;

- with reference to the nature of the data processed, it was noted that in the event that a customer belonging to the categories of disabilities indicated in law no. 104/1992 requests the application of the VAT regime with a reduced rate for the purchase of

a car, the company collects information and documents suitable for detecting the state of health of the applicant; however, for the processing of sensitive data, suitable for revealing the state of health of the interested parties, the company has not acquired the required written consent from the interested parties;

- with reference to the processing of data collected through the website www.autosat-spa.it and for profiling purposes, as represented in the information on the website, the company does not appear to have submitted the notification to the Guarantor;

NOTING that with the aforementioned deeds of 25 July 2016 and 25 January 2017 Autosat S.p.A. violations of the provisions of the Code regarding the adoption of minimum security measures (dispute no. 86/2016), acquisition of written consent for the processing of sensitive data (dispute no. 87/2016) and failure to submit notification to the Guarantor (dispute no. 8/2017);

READ the administrative reports, drawn up by the Guardia di Finanza, with which it was represented that Autosat S.p.A. did not proceed with the reduced payment with reference to disputes nos. 87/2016 and 8/2017; having also acknowledged that for dispute no. 86/2017 there is no reduced payment;

READ the defense briefs presented on 7 September 2016 and the minutes of the hearing of the company on 3 May 2018, during which further defense briefs were presented, in which the following are represented:

- dispute no. 86/2016 - "Access to the seller's PC [...] took place through authentication to the operating system, with credentials and a password, however that may be. The seller's PC desktop [...], designated in charge of personal data processing, did not report sensitive customer data. Access to the "Link-e-entry" portal for the preparation and management of estimates by the seller [...] was carried out by authentication with username and password consisting of ten characters (see, daily report 05.24.2016 , page 3). Access to the images, recorded by the video surveillance system, is protected by the key lock of the special room where the video surveillance system (monitor and recorder) is kept (see, daily report 05/26/2016, page 2). The keys to this premises are kept in a locker (also locked) of the office of the Legal Representative [...] who is appointed internal manager of data processing through the video surveillance system (as well as within the post sale. See, documentation sent on 06.24.2016). No other internal manager/person in charge of data processing through the video surveillance system has been appointed. The subject in possession of the credentials to (not remotely) extract the recorded images and, possibly, make changes to the system settings is the installing company [...], which has been appointed external manager of data processing through the system of video surveillance (cf., documentation sent on 24.06.2016)";

- dispute no. 87/2016 - “All customers, even in cases of disability, are immediately provided with the preparation of the sales estimate, the information pursuant to art. 13 Privacy Code (see, daily report 05.24.2016, page 3, Annex 2). This disclosure expressly provides that: "the personal data freely provided by you will be processed in order to: a) provide the commercial and/or assistance service freely chosen by you"; "your personal data, collected with this registration, may be processed by data processors, including external ones, in charge of managing the requested service"; "your data may be disclosed to third parties to fulfill legal obligations". The final section of the estimate dedicated to the "Composition of the offer" and, therefore, to the determination of the price of the vehicle shows the "VAT" option and, in the relative window, the category of disabled people entitled to the 4% rate (see ., daily report 24.05.2016, page 3, Annex 2). Simultaneously with the preparation of the estimate with the 4% VAT option and with the acquisition by the seller of the medical documentation required for the tax relief, the customer with disabilities, who has already signed the consent pursuant to art. 23 Privacy Code at the bottom of the disclosure, the specific consent to the processing of sensitive data is further signed. The specific consent to the processing of sensitive data is signed on a separate sheet, then used as the "Fax cover of the consultancy service for car subsidies for people with disabilities provided by Mobilità Informatica Srl" (see, daily report 05.24.2016 , page 4, Annex 4). [...] The sales contract (see, daily report of 05.24.2016, page 5, Annex 6) also contains the disclosure pursuant to art. 13 Privacy Code, which expressly provides that "the personal data provided by the Customer, even verbally, to the Seller, during commercial contacts, pre-contractual negotiations and/or in the execution of this Order, will be treated ... for the following purposes: ... b) purposes related to the fulfillment by the Seller of legal obligations (eg in accounting, fiscal and taxation matters)”;
- dispute no. 8/2017 - “Autosat would have been subject to the obligation to make the notification required by art. 37 of the Privacy Code due to the indication of the profiling activity among the purposes contemplated in the information provided to the interested parties, noting the fact (undisputed and not disputed) that Autosat has never carried out nor, as will be said, have ever been in a position to carry out this kind of treatment. In fact, it should be noted that the Complaint does not indicate at any point that Autosat has carried out profiling activities on the interested parties, and in hindsight it could not have been otherwise, given that from what emerged during the investigations carried out by the Authority, both at Autosat and at FCA , it is clear that the activity in question has never been carried out. In this sense, it should be noted that the basic principle that can be inferred from the Dispute, according to which the mere indication of the purpose of profiling in the context of the information provided to the interested parties automatically gives rise to the obligation to proceed with the notification, even if this treatment is not put

in place, in the humble opinion of the writers it cannot be shared nor is it supported by any regulatory data. [...] You are subject to the notification obligation only where you are faced with electronic tools configured and used for the purpose of carrying out a profiling activity, while you do not have to make any notification where, while proceeding with data collection, the the same are processed for other purposes, including marketing, without carrying out any profiling activity on the interested parties. Where compliance is required, as anticipated, this must be in place before the start of treatment. On the basis of the above, it is clear that, also in the light of the ratio of the provision as explained in the context of Directive no. 95/46/EC (advertising of the treatment aimed at its control), the element that gives rise to the notification obligation is, necessarily, the concrete and effective configuration of one of the treatments contemplated by the law (in this case the start of the profiling activity through the use of specific systems or electronic tools). When in practice we are faced with a system configured to carry out a treatment subject to the obligation of notification, this obligation can be correctly fulfilled, in the light of the literal content of the reference standards and of what has been repeatedly reiterated by the Guarantor himself , up to the start of treatment (it is hard to see how else to interpret the statement "before the start of treatment"). A necessary corollary of this reconstruction is that the violation pursuant to art. 163 of the Privacy Code can be detected only a posteriori, with treatment in progress, i.e. only in the event that the carrying out of a treatment fully falling within the cases referred to in art. 37 with respect to which, before the start, no notification appears to have been made "timely". […]. Regardless of any consideration regarding the formal provision [...] of the roles of manager held by FCA and of controller held by Autosat with reference to the processing of personal data acquired through the website, it is emphasized that, as per the declarations made in the As part of the inspections (see report dated 25.05.16, page 5), the website is not owned by Autosat and is managed by FCA as part of service agreements to which the concessionaires have adhered to "receive the incentive prizes", without (i) having "no decision-making power and no possibility of modification" of this site, (ii) nor being able to receive the information collected through the online forms, except those of the so-called lead (name, surname, tel. no.) necessary for the telephone bill, (iii) nor to be able to carry out the processing of such data for the purposes indicated in the information resulting from the website itself. The disputed information forms (and related consent options) and the related updates were in fact prepared by FCA, as is also evident in the deeds. Therefore, even the indication of the "possible performance of the profiling activity" was provided centrally and independently by the FCA parent company in line - by its own admission - with the standards followed by it for the activities it carries out as data controller of customer data, and certainly not on the basis of contractual "specifications" and/or

any directives and instructions to that effect from Concessionaires, such as Autosat";

CONSIDERING that the arguments put forward, together with the documents acquired during the sanctioning procedure, lead us to believe that Autosat S.p.A. is not responsible for the violation referred to in dispute no. 8/2017, while the same company is responsible for the violations referred to in disputes nos. 86/2016 and 87/2016. In this regard it is represented:

- dispute no. 86/2016 - it is ascertained that, during the inspection activity carried out by the Guardia di Finanza at the company's headquarters, a computer assigned to one of the company's employees, in which documentation on customers and related car purchases was kept, was not equipped with a suitable authentication system, since the confidential part of the authentication credentials assigned to the aforementioned employee consisted of only four alphanumeric characters instead of the prescribed eight (rule no. 5 of the technical specification referred to in Annex B) of the Code) . In the same activity it was also ascertained that access to the system for recording images taken with the video surveillance system in use at Autosat S.p.A. occurred in the absence of an IT authentication procedure and therefore in violation of rules nos. 1 et seq. of the aforementioned technical specification. In this regard, it must be pointed out that the defensive considerations regarding the existence of "physical" protections which limited the availability of the aforesaid recording system appear irrelevant, since the rules on the adoption of minimum security measures do not provide for exceptions to the implementation of a suitable authentication system where physical measures are envisaged to limit access to IT tools. It should also be noted that the provisions on simplification (provision of the Guarantor of 27 November 2008, in www.gpdp.it., web doc n. 1571218), on the basis of which, according to the defence, the minimum security measures adopted by the companies would be in line with the current regulatory framework, do not apply to controllers who process sensitive data (such as Autosat S.p.A.) and, moreover, in any case require the presence in the systems of an IT authentication procedure, contrary to what has been observed by the Guardia di Finanza with reference to the device for recording the images taken by the video surveillance system. The violation of the provisions regarding the adoption of minimum security measures must therefore be confirmed (articles 33 and subsequent of the Code and rules no. 1 and subsequent of the technical specification referred to in Annex B) of the same Code);

- dispute no. 87/2016 - it is amply proven by the results of the sanctioning procedure, and confirmed by the same company, that Autosat S.p.A. proceeded with the collection and processing of data suitable for detecting the state of health of the interested parties for the purpose of reducing the rate relating to the value added tax for the purchase of cars. This treatment

requires the acquisition, by the owner, of the written consent of the interested parties. No trace of the prescribed consent was found among the documentation acquired during the investigation since the documents indicated by the defense also refer to consent acquisition models for treatments with promotional purposes. It must therefore be confirmed that the aforementioned treatment, attributable to the areas governed by the "Authorization for the processing of data suitable for revealing the state of health and sexual life", n. 2/2016, adopted by the Guarantor on 15 December 2016, point 1.2, lett. e) (in www.gpdp.it, web doc n. 5803257), was carried out in the absence of the consent required by art. 26 of the Code;

- dispute no. 8/2017 - the defensive observations aimed at highlighting that the inclusion in the information present on the website of the company of the purposes of the treatment relating to the elaboration of the consumer profile of the interested parties appears to be acceptable, occurred by mere error and that therefore the violation of the provisions pursuant to art. 37 and 38 of the Code regarding the presentation of the notification to the Guarantor was carried out in the absence of conscious and voluntary conduct. In fact, it is sufficiently proven that the text of the disclosure had been inserted by the commercial partner FCA Italy S.p.A. and that Autosat S.p.A. she had not noticed this insertion; it is also demonstrated that Autosat has not collected personal data from which the processing of the consumer profile of the data subjects could be attributed and that in any case Autosat did not have the software and other tools suitable for carrying out such processing. Therefore, even in the presence of a collection of data (and therefore of a treatment) which, formally (as stated in the information), also appears aimed at the elaboration of consumer profiles, the provision pursuant to art. . 3 of the law n. 689/1981 since, in the case in question, the unlawful conduct took place despite the fact that the company has demonstrated that it has done everything possible to comply with the provisions of the law (see Civil Cassation, section II, sentence n. 7885 of 06 April 2011);

NOTING, therefore, that Autosat S.p.A., on the basis of the above deeds and considerations, appears to have committed, in its capacity as data controller, pursuant to articles 4, paragraph 1, lett. f), and 28 of the Code, the violations indicated in the disputes nos. 86/2016 and 87/2016 and, in particular, the violation of articles 33 et seq. of the Code and of the rules n. 1 et seq. of the technical specification referred to in Annex B) (dispute no. 86/2016), as well as art. 26 of the Code (dispute no. 87/2016); also noted that the filing of dispute no. 8/2017 against Autosat S.p.A. for the reasons indicated in the justification;

CONSIDERING the art. 1, paragraph 2, of the law of 24 November 1981, n. 689, pursuant to which the laws that provide for administrative sanctions are applied only in the cases and for the times considered in them;

CONSIDERING the art. 162, paragraph 2-bis, of the Code which punishes violations of the rules indicated in art. 167, among

which there are also the articles 26 and 33 of the Code, with the administrative sanction of payment of a sum from 10,000 to 120,000 euros, for each of the two violations contested;

CONSIDERING that, for the purposes of determining the amount of the pecuniary sanction, it is necessary to take into account, pursuant to art. 11 of the law n. 689/1981, of the work carried out by the agent to eliminate or mitigate the consequences of the violation, the seriousness of the violation, the personality and economic conditions of the offender;

WHEREAS, in the present case:

to. with regard to the aspect of gravity with reference to the elements of the extent of the injury or danger and the intensity of the psychological element, the violation relating to the failure to adopt the minimum security measures is particularly serious since it is extended to multiple systems in use in society;

b. for the purpose of evaluating the work performed by the agent, the fact that the company has in any case provided full cooperation to the inspections by the Finance Police must be considered in favorable terms;

c. regarding the personality of the author of the violation, the company is not burdened by previous sanctioning proceedings defined with a reduced payment or order-injunction;

d. with regard to the economic conditions of the agent, the financial statements for the year 2016 were taken into consideration;

CONSIDERED, therefore, of having to determine, pursuant to art. 11 of Law no. 689/1981, the amount of the pecuniary sanction, based on the aforementioned elements assessed as a whole, to the extent of:

- 20,000 (twenty thousand) euros for the violation of the provisions on minimum security measures, in relation to the failure to adopt suitable IT authentication systems;
- 10,000 (ten thousand) euros for the violation of the provisions on the processing of data suitable for detecting the state of health of the data subjects, in relation to the failure to acquire written consent from the data controller;

HAVING REGARD to the documentation in the deeds;

CONSIDERING the law n. 689/1981, and subsequent modifications and additions;

HAVING REGARD TO the observations of the Office formulated by the Secretary General pursuant to art. 15 of the Guarantor's regulation n. 1/2000, adopted with resolution of 28 June 2000;

SPEAKER Dr. Giovanna Bianchi Clerici;

HAS

the filing of the sanctioning procedure referred to in report no. 8 of 25 January 2017 relating to the contestation of the administrative violation pursuant to art. 163 of the Code, in relation to art. 37, in the terms referred to in the justification;

ORDER

to Autosat S.p.A., in the person of its pro-tempore legal representative, with registered office in Surbo (LE), via Unità d'Italia no. 1, tax code 03575990753, to pay the sum of 30,000 (thirty thousand) euros as an administrative fine for the violations indicated in the justification;

ENJOYS

to the aforementioned company to pay the sum of 30,000.00 (thirty thousand) euros, according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the law of 24 November 1981, n. 689.

Pursuant to articles 152 of the Code and 10 of Legislative Decree no. 150/2011, opposition to this provision may be lodged with the ordinary judicial authority, with an appeal lodged with the ordinary court of the place where the data controller has his residence, within the term of thirty days from the date of communication of the provision itself or sixty days if the appellant resides abroad.

Rome, 31 May 2018

PRESIDENT

Soro

The SPEAKER

Cleric Whites

THE SECRETARY GENERAL

Busia