SEE ALSO Press release of 13 July 2020

[doc. web no. 9435807]

Injunction against Iliad Italia S.p.A. - July 9, 2020

Register of measures

no. 138 of 9 July

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by Dr. Antonello Soro, president, Dr. Giovanna Bianchi Clerici and Prof. Licia Califano, members, and Dr. Giuseppe Busia, general secretary;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as well as on the free circulation of such data and repealing Directive 95/46 /CE (General Data Protection Regulation, hereinafter "Regulation");

HAVING REGARD TO the Code regarding the protection of personal data (legislative decree 30 June 2003, n. 196), as amended by legislative decree 10 August 2018, n. 101, containing provisions for the adaptation of the national legal system to the aforementioned Regulation (hereinafter the "Code");

HAVING REGARD TO the complaints and reports received by the Guarantor, with regard to various processing of personal data carried out by Iliad Italia S.p.A. (hereinafter also referred to as: "Iliad" or "the Company");

CONSIDERING the results of the inspections carried out on 27, 28 and 29 May 2019 at the registered office of Iliad Italia S.p.A. in Milan;

HAVING REGARD to the documentation in the deeds;

HAVING REGARD TO the observations made by the general secretary pursuant to art. 15 of the Guarantor's regulation n. 1/2000;

SPEAKER Dr. Antonello Soro;

WHEREAS

1. THE INVESTIGATION ACTIVITY CARRIED OUT

Since the end of 2018, the Guarantor has received some complaints and reports referring to various methods of processing personal data implemented by Iliad.

In particular, the issues brought to the attention of the Authority concerned the processing of customer data for the activation of sim cards and the relative method of acquiring payment data, the processing for own and third party promotional purposes and the measures adopted for the storage of data in the customers' personal area.

Given the nature and heterogeneity of the issues represented and in consideration of the fact that the Company, as a new operator of electronic communications, had never been the subject of discussions with the Guarantor, it was deemed appropriate to carry out an overall assessment in the context of a single inspection which was conducted on 27, 28 and 29 May 2019.

2. RESULTS OF THE INVESTIGATION

During this assessment, checks were carried out which, starting from the individual reports and following the practice of the Office for conducting on-site checks, made it possible to evaluate even more generally the methods with which the treatments are carried out and the technical and organizational measures adopted by the Company.

As a result of this activity, violations of the rules on the protection of personal data emerged and some treatments that could probably have violated these rules were also detected. Therefore, on 11 October 2019, the Company was notified of the start of the proceeding pursuant to art. 166, paragraph 5, of the Code for contesting violations of the Code and of the Regulations.

The Company sent its observations in reply with a note dated 8 November 2019 and with a hearing held on the following 10 December.

2.1. Contextual acceptance of the contractual conditions and of the privacy policy.

In order to generally verify the corporate processes most closely connected to the processing of users' personal data, the operations began with the verification of the activities necessary to activate a new user by accessing the website www.iliad.it.

In this context, it was verified that the procedure which led to the order confirmation required, once all the data had been entered, the obligatory check of a box with which the subject declared that he "had read and accepted the general conditions, the service charter, price brochure and Iliad's privacy information on the processing of personal data” (see page 3 of the May 27 report). The documents referred to therein, including the disclosure, were easily accessible via a specific link.

However, it should be noted that the treatments listed in the information published on the website are both optional and mandatory and, in some cases (treatments for marketing and profiling purposes) are subject to the acquisition of a specific consent.

However, the formulation of the declaration mentioned above, simultaneously contemplating the "acknowledgment" and "acceptance" of the information, could lead to the doubt that the collection of consent for marketing purposes - which is also specifically provided for in one of the screens precedents - would take place in this latter location with the tick "for acceptance". Although the presentation of the information at the time of data collection is correct, as required by art. 13 of the Regulation, and taking into account that the data controller must be able to demonstrate, by documenting having read it, that he has provided such information, the simultaneous mention of acceptance of the information also appears superfluous since nothing else can be attributed to this wording. meaning that that of mere confirmation of reading; otherwise, in fact, by ticking the box, the subject would find himself expressing consent to the treatment which would be neither free, because the tick is mandatory and only for acceptance of the contractual clauses as well, nor specific because it concerns all treatments mentioned in the information. In this regard, reference is made to the contents of recitals 42 and 43 of the Regulation regarding the awareness of the subject who expresses a consent in the context of a written declaration that also contemplates other issues.

Therefore, the Office, with a note dated 11 October 2019, challenged the Company that this treatment - taking into account that, in the terms described, the intention of the owner did not appear to be to obtain consent to the treatment, but only to demonstrate to have complied with the disclosure obligations - did not have the character of clarity and intelligibility and, therefore, could have been placed in contrast, in particular, with the principles of correctness and transparency expressed by art. 5, par. 1, lit. a) of the Regulation.

With the defense brief dated 8 November 2019, the Company declared that, although it believes "that the approach followed up to now complies with the principles of lawfulness and transparency [...], with a view to always improving the services to its users , Iliad has removed the reference to the information on the processing of personal data from the contested sentence".

The same has also attached the new screen in which, at the end of the user activation procedure, the user is asked to select acknowledgment and acceptance of the General Conditions, Service Charter and Price Brochure, while the following notice is shown in a separate space: “Your personal data will be processed in accordance with Iliad's Privacy Policy on the processing of personal data”.

2.2. Request for consent for marketing purposes.

During the inspection, the registration procedure present on the website www.iliad.it was examined, aimed at requesting a new user, and it was found that, at the bottom of the page for entering personal data, there was a box to tick to give consent to the

processing of personal data for promotional purposes of the same Iliad. Failure to check the box still allowed to go ahead with the signing of the contract. This in accordance with the privacy policy where, in point 4 lett. i), processing for marketing purposes was contemplated with the express consent of the data subject.

In this regard, with statements made in the minutes (see page 2 of the minutes of 28 May), the Company clarified that "ticking the checkbox relating to the request for consent for promotional purposes, seen in the online activation procedure, does not imply registration of this manifestation of consent in Iliad's information systems, as the Company does not carry out direct marketing activities".

The Office, therefore, with the aforementioned note of 11 October, highlighted that, in the absence of treatment for promotional purposes, both its mention in the information and the request for specific consent were ineffective; on the other hand, if the company had instead intended to carry out this type of treatment, it would not have been able to demonstrate the correct acquisition of the consents of the interested parties, not having registered them. Similarly it was highlighted that in point 4, lett. j) of the disclosure, it was possible to use the data provided by the interested party "for sending marketing communications focused on the interests and needs of the user". Also in this case, the reference to a treatment, profiling aimed at marketing, which in reality is not carried out (and for which, in this case, the request for specific consent is not even envisaged) is irrelevant.

With the defense brief of 8 November 2019, the Company first of all specified that "unlike other operators in the telecommunications market, Iliad does not carry out any marketing, telemarketing or user profiling activity [...] and carries out promotional activities mainly through the television and digital channel that does not involve the processing of users' personal data". Then, with specific regard to the disputed point, he declared that "Iliad intends to process the personal data of its users for promotional purposes and, for this reason, Iliad has included this processing purpose in its information on the processing of personal data and has set up a consent collection system [...]. However, this activity has so far been postponed precisely because - due to a technical problem - the company has not been able to register the consents ". In fact, the same added that the consent collection system, already in place, had resulted affected by a design bug which prevented the identification of the user, the date and time in which the checkbox relating to the consent. The Company has therefore corrected the error and since July 2019 all consents have been recorded in the system; this allows users to express their will to grant or withdraw consent also through the appropriate function in the personal area.

Furthermore, it is acknowledged that the Company has declared that it has not provided for the transfer of customer data to third parties for promotional purposes among its procedures (see minutes of 28 May 2019) and therefore the complaints in some reports in regarding the receipt of promotional calls after activating an Iliad account.

2.3 Suitability of the Simboxes to guarantee the confidentiality of the interested parties.

During the inspection, the Company was asked to describe the methods for assigning SIM cards to customers. Iliad clarified that the new users can be requested via the website or by going to the physical sales channels (Iliad-branded sales points or special spaces, called "corners", set up in places open to the public). In all cases, the company has set up specific procedures to identify the subjects who request the activation of a telephone number, in compliance with the provisions of the current regulations on the fight against terrorism (law 31 July 2005, n. 155).

In the case of activation via the web, the user can choose whether to proceed immediately with identification via the site or to postpone this phase until the SIM is delivered by courier. In the first case, at the end of the procedure, you are asked to attach a copy of your identification document by recording a short video in which you declare your intention to sign the contract; in the second case, on the other hand, the identification of the SIM holder is made directly by the courier, appointed as data processor and specifically trained for this procedure.

If, on the other hand, the activation of a new SIM is carried out through physical channels, the company has set up special machines, called "Simboxes", with which customers can make the purchase independently, entering their data and completing the procedure by scanning the document and recording a video message of consent to the conclusion of the contract. The staff present in the shops only have the function of customer assistance and are not involved in the user activation procedure.

The video recordings made in this way are viewed by back office operators who, after making a comparison with the uploaded document, conclude the procedure allowing the user to be activated.

During the inspection carried out by the Authority, the method of activating a user using a Simbox installed at a point of sale was simulated. During this activity, documented by means of photographs (see attachment 5 to the minutes of 28 May), it was possible to verify that there were several publicly accessible machines inside the shop to carry out the procedure autonomously.

Iliad has been challenged that the camera installed on the Simbox is capable of making a shot with an angle of about 180 degrees; as can also be seen from the documentation in the file, this method could allow for the recording of the image of

people who happen to pass behind or beside the subject who is carrying out the operation; the photographic recordings, referred to in Annex 5 of the May 28 report, in fact show that the shot of the camera does not only capture the face of the person making the recording but also the people behind it. At the same time, the absence of suitable measures to ensure customer confidentiality during operations could allow anyone in the premises to view the data typed on the Simbox screen and listen to the content of the video message (during which the user must pronounce his/her first and last name).

Furthermore, it must be taken into account that these machines are installed, not only in Iliad stores, but also (and mainly) in special spaces set up in railway stations and shopping centers and also in this case there are no particular measures aimed at protecting the confidentiality of customers, considering in particular that these are places characterized, in general, by a notable influx of people (see attachment 2 to the minutes of 27 May where there is a photo of two Simboxes positioned inside a shopping centre).

Moreover, even in the service contract signed with the company that deals with the operational management of the areas located in the shopping centers, there is no reference to particular precautions to be observed in the positioning of the Simboxes for compliance with confidentiality rules (see annex 2 to the minutes of 27 May).

In providing its own observations in reply, Iliad represented that the Simbox camera is activated only for the short period of time (maximum 10 seconds) necessary to carry out the recording and does not allow to clearly frame the subjects passing near the machine. Furthermore, with regard to the possibility, disputed by the Guarantor, of exposing the personal data entered by users to the view of third parties, the Company stated that the size of the screen and its positioning should not allow third parties to read the text entered from the moment that the view would be covered by the person carrying out the operation and taking into account that the input character is gray.

Having said this, while continuing to believe that the measures adopted are already compliant with the rules, the company has nevertheless introduced the following corrective solutions:

- on the screen that appears to the user upon starting the registration procedure, the following warning is shown: "make sure you do not register images of third parties, that you are alone, facing and positioned so that the entire face is visible and identifiable ";

- the records collected, as soon as they are validated by the customer care operators, are made visible only to the managers of the customer care function and, after six months, are accessible only to the JAS (Judicial Authority Services) function for the

duration of the contract.

Furthermore, during the hearing held on December 10, 2019, Iliad added that the video recording is not stored in the Simboxes, but is stored directly in the central database; moreover, the videos containing images of third parties are immediately deleted by the operators in charge of the identification procedure with the simultaneous interruption of the process and the customer's request to make a new registration. The Company has also specified that the identification operator and the assistant present in the points of sale cannot make copies of the documents provided by customers or of the registrations made.

2.4. Compliance with the rules on access and storage of telephone and telematic traffic data.

During the investigation conducted on 28 May 2019, access was made to the company's CRM system, both with an operator profile and with an administrator profile, to verify its content. It was thus found, and reported in the minutes, that the "administrator of the customer care department" profile could view the telephone traffic data of users in unencrypted form by accessing the system by typing in a userid and password. Furthermore, the accessible data related to the traffic carried out since August 2018.

The company was therefore contested that this procedure could not be considered compliant with the rules on the conservation of telephone and telematic traffic data pursuant to art. 123, 132 and 132-ter of the Code and on the basis of the provisions of the Guarantor with a general provision of 17 January 2018 (in www.garanteprivacy.it web doc n. 1482111). This because:

1. the person in charge with an administrator profile - who, being in charge of the customer care function, could only have access to the data stored for billing purposes, could instead view data stored for a period exceeding the six months permitted by art. 123 of the Code (traffic data for August 2018 was present at the date of May 2019);

2. the same has accessed the system containing the traffic data by typing only the username and password, therefore without using strong authentication techniques at the time of the check;

Furthermore, as a result of the above findings, the requirement to keep the different types of data in separate computer systems was not implemented, since the operator, by accessing the CRM system, could also view data generated in a period exceeding six months .

With a note dated November 8, 2019, Iliad deemed the complaints received from the Guarantor unfounded on the basis that

the information contained in the screenshot referred to in Annex 6 to the assessment report of May 28, 2019, "does not allow the reconstruction of the flows of communication of the users to which they refer and cannot therefore be considered traffic data". In this regard, it should be noted that the content referred to by the company (Annex 6), since it refers to access made with an operator profile, has never been contested by the Authority and is therefore improperly cited. The dispute, on the other hand, was based on access made with an administrator profile who, as reported in the report dated May 28, 2019 signed by the party, "can view further information such as outgoing telephone traffic data in the clear from, for the form of the viewed user, since August 2018". On this point, no other observations were received from Iliad either with the aforementioned defense brief, or during the subsequent hearing.

Furthermore, with regard to the disputed access carried out without adopting strong authentication techniques, the Company, in its defense brief, declared that "with reference to the Mobo management system subject to inspection specifically but in general with regard to all company systems, Iliad has adopted a dual authentication technology. In fact, in addition to entering the username and password of the user who accesses the system, there is a form of automatic authentication determined by the connection exclusively of company devices to the Iliad network. In fact, when accessing the Iliad network via the company device, the system carries out a first recognition of the Iliad employee and a second recognition occurs when accessing the Mobo management system ". However, the same did not attach any documentation proving what was declared and it should be noted that this justification was not presented at the time of the investigation.

With the note dated 8 November 2019, the Company also provided its own observations regarding the fact that, at the time of the investigation, the telephone traffic data generated over six months were found to be present in the customer care management system, inconsistent with what is prescribed by the Guarantor regarding the need, after the first six months, to operate a separation of the IT systems responsible for storing data for the various purposes. In this regard, the company declared that it had "created a single database with differentiated security measures and access levels (CRM i.e. Mobo and JAS management) according to the purposes of the processing and the relative conservation term. This system therefore has a logical rather than a physical separation".

3. LEGAL ASSESSMENTS

With reference to the factual profiles highlighted above, also on the basis of the declarations of the Company for which one responds pursuant to art. 168 of the Code, the following assessments are made in relation to the profiles concerning the

regulations on the protection of personal data.

3.1 Contextual acceptance of the contractual conditions and of the privacy information.

The treatment described in point 2.1., the reasons for which are referred to in full, as it was put in place before the changes made by the Company, was not fully compliant with the principles expressed by the Regulation. This is because the wording proposed in the contract conclusion screen was ineffective by requesting the "acceptance" of the information and not just its acknowledgment and this request was, moreover, formulated together with the contractual confirmations. As known, the information drawn up by the owner has the function of making the interested party aware of every aspect of the processing of personal data; this purely explanatory nature means that the holder, although being able to expect the interested party to confirm having read it, cannot however also request to express, through a generic and general acceptance, a will that would in fact be analogous to a consent.

The Office therefore, despite having understood that, in the terms described, the intention of the owner did not appear to be that of obtaining consent to the processing but only that of demonstrating that he had complied with the information obligations, deemed it necessary to contest the lack of the requirements of the clarity and intelligibility with the consequence of a possible treatment in contrast, in particular, with the principles of correctness and transparency expressed by the art. 5, par. 1, lit. a) of the Regulation.

The corrective measures adopted by the Company, following the complaint received, are sufficient to separate the information obligations from the collection of consent, restoring the necessary clarity to this phase of the treatment.

On this aspect, therefore, it is not considered necessary to adopt specific corrective measures, with the exception of what is indicated in point 4.1 of this provision.

3.2. Request for consent for marketing purposes.

With regard to the treatment described in point 2.2., it should be noted that the Company, on the basis of the declarations made, until July 2019 asked the interested parties to give their consent to the treatment for promotional purposes without however keeping track of this will. This would have happened because, as initially stated in the report, the Company did not carry out (and would appear not to still carry out) direct marketing activities but also, as subsequently argued in the defense brief, due to a bug present in the registration system of consents.

On the basis of the declarations made, it must therefore be considered that, as already disputed, the request for consent for

promotional purposes, specifically mentioned in the information, without such processing existing or envisaged, is in contrast with the principle of correctness and transparency pursuant to art. 5, par. 1, lit. a), of the Regulation.

However, acknowledging the intention of the Company, not mentioned during the inspection, but disclosed in the defence, to actually implement a treatment for promotional purposes, taking into account the corrective measures taken, and the fact that the The Company has declared that it considers the consent of subjects registered before July 2019 to be denied, it is believed that, also on this point, the conditions for adopting specific corrective measures do not exist, with the exception of what is indicated in point 4.1 of this provision.

3.3 Suitability of Simboxes to ensure confidentiality.

The checks carried out by simulating the signing of a contract via Simbox, have raised some concerns regarding the confidentiality of the procedure. Therefore, the Company has been challenged that such processing may expose data subjects to the risk of unauthorized access, violating the principle of integrity and confidentiality pursuant to art. 5, par. 1, lit. f) of the Regulation.

The corrective measures introduced by the Company (described in point 2.3) may be considered suitable for containing the risk, but may not be sufficient, especially in the case of totems positioned in places open to the public (not only Iliad points of sale but also corners) which are, in general, characterized by a greater influx of people.

Furthermore, taking into account the overall treatment carried out even before the adoption of the corrective measures, the violation of the art. 5, par. 1, lit. f) of the Regulation with regard to the lack of adequacy of the measures adopted to guarantee the confidentiality of personal data.

That said, pursuant to art. 58, par. 2, lit. a), it is deemed necessary to warn Iliad regarding the detected violations of confidentiality through the use of the Simbox and consequently to order the same, pursuant to art. 58, par. 2, lit. d), to adopt suitable corrective measures to guarantee greater confidentiality to the interested parties at the time of the video recording by adopting specific precautions for the positioning of the machines, placing them in such a way as not to allow undue access to the information (for example near a wall) or by inserting rear panels, or by providing courtesy distances and consequently integrating the instructions to the assistance personnel.

3.4. Compliance with the rules on access and storage of telephone and telematic traffic data.

As reconstructed in point 2.4., during the inspection activity it was ascertained that the person in charge of customer care with

an administrator profile could view unencrypted telephone traffic data, generated for more than six months, by accessing the system, called " Mobo", in charge of customer care management.

The Company's conduct was assessed in the light of the provisions of art. 123, 132 and 132-ter of the Code which dictate specific indications regarding the measures to be adopted in the conservation of traffic data. In particular, the art. 132-ter requires providers of electronic communication services to use, pursuant to art. 32 of the Regulation, of technical and organizational measures appropriate to the existing risk. These measures, to be considered, at the state of the art, as a minimum security requirement generally used by operators on the market, are concretely identifiable with the provisions of the Guarantor, regarding the conservation of traffic data, with a general provision of 17 January 2008 (in www.garanteprivacy.it web doc. n. 1482111, as amended by the subsequent provision of 24 July 2008, web doc. n. 1538224), according to which:

- the processing of telephone and telematic traffic data by suppliers must be permitted only to specifically authorized persons in charge and solely on the basis of the prior use of specific IT authentication systems based on strong authentication techniques, consisting in the simultaneous use of at least two different authentication technologies; for traffic data stored for the exclusive purpose of ascertaining and prosecuting crimes (and generated for more than six months), one of these technologies must be based on the processing of biometric characteristics of the person in charge;
- the computer systems used for the processing of traffic data kept for the exclusive purpose of justice must be different from those used also for other company functions (such as billing, marketing, anti-fraud); however, an initial period of 6 months from generation is admissible, during which the data can be processed with IT systems that are not exclusively reserved for justice purposes;
- the supplier must define and assign specific authorization profiles to the persons in charge, differentiating the traffic data processing functions for ordinary management purposes from those for the purpose of ascertaining and prosecuting crimes.

At the end of the preliminary investigation carried out, the Office considered that the elements acquired could constitute violations and therefore initiated the procedure pursuant to art. 166, paragraph 5 of the Code. In the face of the precise objections received, the Company - which also presented a 22-page brief and was heard in a subsequent hearing - responded on the point in a non-exhaustive and sometimes equivocal manner.

In the specific case relating to the retention of traffic data, Iliad replied that the complaints received were to be considered unfounded as, in his opinion, there would have been three issues to consider:

1) the levels of access to personal data;

2) the verification that it was possible to view the traffic data through the Mobo management system;

3) the retention period for personal data.

With regard to the first point, Iliad said it has adopted levels of access to differentiated systems based on the role of employees and, also in the case in question, access to the Mobo system allows different levels of visibility of information depending on the profile (operator/administrator). In this regard, it must be noted that this aspect has never been contested by the Office which, however, contested the fact that the person in charge, as a customer care employee (albeit with the profile of administrator) has been able to view data stored for a period exceeding six months, a period beyond which the personnel responsible for verifying the correctness of the billing (such as the customer care administrator) should no longer be allowed and should, instead, be reserved only for figures authorized to access traffic data stored for justice purposes.

With regard to the second point, as already described in paragraph 2.4, the Company observed that the screenshot included in attachment 6 to the report of May 28, 2019 does not contain traffic data and, for this reason, the dispute is unfounded. As already mentioned, the attachment referred to by the Company is the one relating to access made with an operator profile which has never been contested by the Office. Logged in with the system administrator profile is instead shown in attachment 7, which shows how the person in charge accessed the system by typing userid and password and that the customer care platform keeps track of the operations performed by the administrator; moreover, the overall result of this access, which acknowledges the presence of "unencrypted outgoing telephone traffic data starting from August 2018 for the user profile viewed" was reported in the report that the party signed and never subsequently contested.

Furthermore, the Company, in the aforementioned brief, continuing with regard to the alleged groundlessness of the dispute (third point of the above list), added that "in any case, Iliad confirms that accessibility to traffic data in the Mobo system is currently limited to a period of six months from their registration". It is therefore to be considered undoubted, as confirmed by Iliad itself, the presence of traffic data in the customer care system (Mobo) and, as underlined by the adverb "currently", storage times are now limited to six months, thus being able deduce that this conservation term was different before and that, probably, the Company has put in place a corrective action (which, however, it has not mentioned nor documented).

The dispute addressed to Iliad also concerned the aspect connected to the conformity of the authentication procedure. As reported in the minutes of 28 May 2019, the person in charge with an administrator profile logged into the customer care

system by entering a user-id and password (as reported in attachment 7 to the minutes). It was therefore disputed that, at the time of the investigation, the measure of two-factor authentication was not used which, as prescribed in the provision of the Guarantor, is necessary to guarantee the confidentiality of the traffic data even if kept only for purposes of billing.

As described in point 2.4, the company, in its defense brief, declared that two-factor authentication is given automatically "by connecting exclusively company devices to the Iliad network. In fact, when accessing the Iliad network via the company device, the system performs a first recognition of the Iliad employee and a second recognition occurs when accessing the Mobo management system ". On this point, reference is made to the aforementioned provision of the Guarantor which admits that "this authentication phase can be carried out with procedures strictly integrated with the IT applications with which the supplier processes the traffic data, or with procedures for the protection of the individual workstations which integrate with the authentication functions of the operating systems used. In the second case, the supplier must ensure that there are no methods of access to the IT applications by its data processors that allow them to circumvent the strong authentication procedures set up for access to the workstation". Therefore, while considering that the justification put forward by the Company could in principle be acceptable with regard only to the data generated within the six months, it nevertheless appears late and therefore no longer verifiable, as it is made present only after receiving the complaint and not during the inspection assessment; the same is also not documented since the Company has limited itself to stating that an initial phase of authentication is passed with access to the company device without however proving, either during the inspection or subsequently, that the tool used by the person in charge possessed the characteristics necessary to identify the user unequivocally. Furthermore, it must be remembered that for access to data generated for more than six months, it is in any case required that one of the authentication technologies is based on the biometric characteristics of the person in charge.

Lastly, the findings raised against the Company concerned more generally the methods of storing traffic data which, based on the preliminary investigation findings, also aroused perplexities regarding separate storage according to the purpose (invoicing or justice). In fact, the presence of traffic data generated for more than six months in the system dedicated to customer management has led to the complaint to the Company of failure to comply with the requirement to keep the different types of data in separate IT systems.

In relation to this specific dispute, the Company replied only that "Iliad has created a single database with differentiated security measures and access levels (CRM i.e. management Mobo and JAS) depending on the purpose of the treatment and

the relative conservation term. This system therefore has a logical rather than a physical separation [...] Iliad has not decided to proceed with a physical duplication of the databases according to the purpose of the processing". From the laconic response of the Company, which also received punctual objections and had ample opportunity to articulate its defense, it can only be deduced that there is a single system, logically separated through differentiated accesses based on the purposes and storage times. However, the Company has not provided any explanation regarding the disputed access to the data generated over six months ago by the person in charge of the customer care area who, due to the function performed, should not have had access to such data taking into account that, according to what was declared, the logical separation according to the purposes should have prevented such access anyway.

Therefore, the answer given above confirms what has already been disputed regarding the failure to separate the systems responsible for storing traffic data.

The aforementioned provision of the Guarantor, in fact, prescribes that the data stored for the exclusive purposes of justice are stored in IT systems physically - and not logically - distinct from all the other company systems and dedicated measures are applied to these systems such as, among others, the access only to authorized personnel with two-factor recognition systems (one of which is biometric) and data encryption. The same provision also admits that, at the choice of the owner, the data generated for up to six months can be stored in a single system in order to be processed also for justice purposes, without the need to resort to any separation; this faculty, however, is applicable, as mentioned, only within six months of generation and therefore, in the presence of data generated more than six months ago, it cannot be considered applicable to the case in question.

Therefore, the statements made by the data controller during the investigation, the truthfulness of which may be called upon to answer pursuant to art. 168 of the Code, do not allow, in any case, to overcome the findings notified by the Office with the act of initiation of the procedure, and are not suitable for excluding the party's liability for the disputed since they have not contributed to demonstrating that the measures adopted by the company can be considered compliant with the security measures - available at the state of the art and generally adopted by electronic communication operators - described in the provision of the Guarantor regarding the conservation of traffic data.

In the light of the new regulatory framework constituted by the Regulation and the Code, it must in fact be considered that the specific provisions of the provision of the Guarantor of 17 January 2008 are to be considered in the same way as the basic

processing security measures applicable to providers of electronic communication services. Failure to comply with these provisions must be considered equivalent to the lack of technical and organizational measures adequate to the existing risk and, consequently, integrates the violation of art. 132-ter of the Code.

Furthermore, for the above, the violation of art. 123 of the Code, with regard to storage exceeding six months in systems used for billing purposes.

Based on the elements set out above, having detected the violations indicated in this paragraph, it is necessary pursuant to art. 58, par. 2, lit. d), of the Regulation, order Iliad to adapt the security measures set up to protect traffic data by conforming them to the provisions of the Guarantor with the provision of January 17, 2008 as amended by the provision of July 24, 2008.

Furthermore, taking into account that the disputes addressed to the Company have not proved sufficient to solicit a corrective action by the latter, it is deemed necessary to adopt an injunction order against the same Company, pursuant to articles 58, par. 2, lit. i), of the Regulation, 166, paragraph 7, of the Code and 18 of the law n. 689/1981, for the application of the pecuniary administrative sanctions provided for by art. 83, para. 4 and 5, of the Regulation.

4. INJUNCTION ORDER FOR THE APPLICATION OF THE PECUNIARY ADMINISTRATIVE SANCTION

4.1. Information and consent.

The conduct ascertained in points 3.1. and 3.2. of this decision respectively integrate the violation of art. 5, par. 1, lit. a), of the Regulation.

However, taking into account:

- the intentions of the owner which, on the basis of what has been acquired in the documents, do not appear aimed at consciously realizing the effects of the disputed conduct and are rather attributable to a negligent application of the rules;
- the presumable lack of consequences for the interested parties since the promotional purpose of the treatment has not yet been achieved;
- the measures adopted and aimed at resolving the critical issues indicated above,

it is believed that they can be qualified as "minor degree" violations in the light of art. 83, par. 2 and recital 148 of the Regulation and that, therefore, it may be sufficient in this regard to warn Iliad, pursuant to art. 58, par. 2 lett. b) of the Regulation for failure to comply with art. 5, par. 1, lit. a) of the Regulation, as well as the principles referred to in art. 25 of the Regulation, also meaning that failing that, the sanction pursuant to art. 83, par. 5 lett. a) of the Regulation.

4.2. Simbox and security measures.

The conduct ascertained in point 3.3 of this decision are suitable for exposing the interested parties to the risk of unauthorized access to personal data and are therefore likely to integrate the violation of the principle of integrity and confidentiality pursuant to art. 5, par. 1, lit. f) of the Regulation.

However, taking into account the corrective measures introduced by the Company suitable for containing this risk, as well as the precautions adopted with reference to any videos containing images of third parties, it is believed that this violation can also be classified as "minor" in the light of art. 83, par. 2 and recital 148 of the Regulation. Therefore it is considered sufficient in this regard to admonish Iliad, pursuant to art. 58, par. 2, lit. a), of the Regulation regarding the detected violations of confidentiality through the use of the Simbox and, at the same time, order the same, pursuant to art. 58, par. 2, lit. d) of the same Regulation, to adopt suitable corrective measures to guarantee greater confidentiality to the interested parties at the time of carrying out the video recording by adopting the specific precautions indicated in point 3.3 of this decision.

4.3. Security measures applied to the retention of traffic data.

The conduct ascertained in point 3.4 of this decision integrates the violations of articles 132-ter and 123, paragraph 2 of the Code, respectively subject to the sanction pursuant to art. 83, par. 4 and par. 5 of the Regulation.

4.4. Quantification of the pecuniary administrative sanction.

In view of the above, the art. 83, par. 3, of the Regulation, on the basis of which, if, in relation to the same treatment or related treatments, a data controller violates, with willful misconduct or negligence, various provisions of the Regulation, the total amount of the pecuniary administrative sanction does not exceed the amount specified for the most serious violation with consequent application of the sole sanction provided for by art. 83, par. 5 of the Regulation.

In particular, for the purposes of quantifying the administrative sanction, for the violations referred to in point 4.3 above, the aforementioned art. 83, par. 5, in setting the statutory maximum in the sum of 20 million euros or, for companies, in 4% of the annual worldwide turnover of the previous year where higher, specifies the methods for quantifying the aforementioned fine, which must "in any case [be] effective, proportionate and dissuasive" (art. 83, paragraph 1 of Regulation (EU) 2016/679), identifying, for this purpose, a series of elements, listed in par. 2, to be evaluated when quantifying the relative amount.

In fulfillment of this provision, in the present case, the following circumstances must be considered:

1. the wide range of treatments concerning the retention of traffic data) which, on the basis of the elements provided and in the

absence of other specifications in this regard, can be considered of a systemic nature and therefore extended to the generality of mobile telephone service customers of Iliad relating to approximately 3 million users at the date of the inspection, as declared by the same (Article 83, paragraph 2, letter a) of the Regulation);

2. the seriousness of the violations detected, due to the fact that, due to the inadequacy of the security measures, a type of personal data (telephone traffic data) was exposed to violation for which the legislator, in consideration of the serious prejudice deriving from the treatment, has prepared special rules to protect conservation (Article 83, paragraph 2, letter a) of the Regulation);

3. the degree of responsibility of the data controller, taking into account that the technical and organizational measures described have not been found to be adequate to the state of the art, despite the fact that the provisions of the Guarantor are to be considered by now widely known among operators of electronic communication services, as imparted with a general provision of 2008, repeatedly subject to specific implementing provisions;

4. the general approach taken by Iliad in the processing of personal data (Article 83, paragraph 2, letter d) of the Regulation), considering that, in addition to what is highlighted in the previous point, the violations described in points 3.1, 3.2. and 3.3, although considered of a minor nature, have nonetheless shown an overall negligent picture in the application, right from the planning stage, of measures to protect the data subjects which, given the constant and numerous pronouncements of the Guarantor, are now to be considered commonly known to the data controllers of the treatment (see, also here, the numerous provisions regarding the correctness of the information and the collection of consent and, with regard to compliance with suitable measures to avoid unauthorized access, through, for example, the establishment of distances " courtesy", the numerous clarifying interventions of the Guarantor, among which, for example, the note of 30.3.1998, web doc. n. 39464);

5. the degree of cooperation with the Supervisory Authority, since the Company limited itself to deeming the disputed violations unfounded, supporting its reasons with arguments often not pertinent to what was ascertained in the report, and taking into account that, against of the complaints received regarding the retention of traffic data, the same, unlike what was done with the other findings received, did not deem it necessary to intervene in any way to adapt its security measures, limiting itself only to confirming the current presence in the Mobo system of traffic data generated no more than six months ago (Article 83, paragraph 2, letter f) of the Regulation);

6. the manner in which the Supervisory Authority became aware of the violation, which emerged during an inspection (Article

83, paragraph 2, letter h) of the Regulation).

As mitigating elements, it is considered necessary to take into account:

1. the measures adopted by Iliad which, although not sufficient, nevertheless appear useful to mitigate part of the prejudicial consequences of the violations found;

2. of the significant loss recorded in 2018, higher than the value of production (Article 83, paragraph 2, letter k) of the Regulation).

In an overall perspective of the necessary balance between the rights of the interested parties and the freedom to do business, taking into account that the Company, also due to its recent presence on the Italian market, has not had any previous sanction proceedings, and in the initial application of the pecuniary administrative sanctions envisaged by the Regulation, it is necessary to prudently evaluate the aforementioned criteria, also in order to limit the economic impact of the sanction on the organisational, functional and employment needs of the Company.

Therefore, it is believed that - based on all the elements indicated above, the administrative sanction of payment of a sum equal to 4% of the maximum statutory sanction of 20 million euros, corresponding to 800,000.00 (eight hundred thousand) euros, should be applied to Iliad. The maximum statutory sanction is identified with reference to the provisions of art. 83, paragraph 5, taking into account that 4% of the turnover of Iliad Italia S.p.A. is less than 20 million euros.

It should be noted that the conditions set out in art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

In this context, it is also believed - in consideration of the delicacy of the treatments whose illegality has been ascertained in the light of the fundamental rights of the interested parties and the high number of the same - that, pursuant to art. 166, paragraph 7, of the Code, and of the art. 16, paragraph 1, of the Guarantor's Regulation n. 1/2019, it is necessary to proceed with the publication of this provision on the website of the Guarantor, by way of ancillary sanction.

Please note that in the event of non-compliance with this provision, the sanction referred to in art. 83, par. 5, letter. e), of the Regulation.

ALL THIS CONSIDERING THE GUARANTOR

against Iliad Italia S.p.A., with registered office in viale Francesco Restelli, 1/A, Milan, Tax Code 13970161009,

a) with regard to the violations found in relation to the correct methods of administration of the information and the consent of

the interested parties (points 3.1. and 3.2 in the introduction), warns Iliad, pursuant to art. 58, par. 2 lett. b) of the Regulation for failure to comply with art. 5, par. 1, lit. a), of the Regulation, as well as the principles referred to in the following art. 25 of the Regulation;

b) with regard to violations found in relation to video recordings made using Simbox (point 3.3. in the introduction): pursuant to art. 58, par. 2, lit. a), of the Regulation warns Iliad regarding the detected violations of confidentiality and, pursuant to art. 58, par. 2, lit. d), of the Regulation, enjoins the same to adopt, within 120 days of receipt of this provision, the corrective measures indicated in the introduction, suitable for guaranteeing greater confidentiality to the interested parties during the use of such equipment;

c) with regard to the violations found in relation to the retention of telephone traffic data (point 3.4. in the introduction), pursuant to art. 58, par. 2, lit. d), enjoins the adoption, within 120 days of receipt of this provision, of all the necessary measures to make the treatment compliant with the provision of the Guarantor of 17 January 2008 as amended by the provision of 24 July 2008;

d) believes that the conditions pursuant to art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor;

e) pursuant to art. 157 of the Code, requires to communicate, within the following 30 days, what initiatives have been undertaken in order to implement the provisions, with an adequately documented response; any failure to reply may result in the application of the pecuniary administrative sanction provided for by art. 83, par. 5, letter. e) of the Regulation;

ORDER

pursuant to art. 58, par. 2, lit. i), of the Regulation, to the aforementioned Iliad Italia S.p.A., in the person of its legal representative, to pay the sum of 800,000.00 (eight hundred thousand) euros as an administrative fine for the violations indicated in the justification; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the fine imposed;

ENJOYS

to the aforementioned Company, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of 800,000.00 (eight hundred 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 deeds pursuant to art. . 27 of the law n. 689/1981;

HAS

pursuant to art. 166, paragraph 7, of the Code, the full publication of this provision on the Guarantor's website.

Pursuant to art. 78 of Regulation (EU) 2016/679, as well as articles 152 of the Code and 10 of Legislative Decree 1 September 2011, n. 150, 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 owner of the processing of personal data has his residence, or, alternatively, with the court of the place of residence of the interested party. , within the term of thirty days from the date of communication of the provision itself, or sixty days if the appellant resides abroad.

Rome, 9 July 2020

PRESIDENT

Soro

THE SPEAKER

Soro

THE SECRETARY GENERAL

Busia