SEE ALSO NEWSLETTER OF OCTOBER 24, 2022

[doc. web no. 9817058]

Injunction against Servizio Idrico Integrato S.c.p.a. - October 6, 2022

Register of measures

no. 328 of 6 October 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, prof.ssa Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer. Guido Scorza, components, and the cons. Fabio Mattei, general secretary;

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

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national legal system to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons with regard to the processing of personal data, as well as to the free movement of such data and which repeals Directive 95/46/EC (hereinafter the "Code");

CONSIDERING the Regulation n. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved with resolution no. 98 of 4 April 2019, published in the Official Gazette no. 106 of 8 May 2019 and in www.gpdp.it, doc. web no. 9107633 (hereinafter "Regulation of the Guarantor n. 1/2019");

HAVING REGARD to the documentation in the deeds;

HAVING REGARD TO the observations made by the general secretary pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the Guarantor's office for the protection of personal data, doc. web no. 1098801;

SPEAKER the lawyer Guido Scorza;

WHEREAS

1. Introduction.

With complaint of the XX, presented pursuant to art. 77 of the Regulation, a user of the Servizio Idrico Integrato S.c.p.a. (hereinafter, the "Company") complained that on the Company's website there would be "a user area [...] where contacts and invoices are managed [in the absence of a] encryption system (certified SSL) [, which,] as is known, is necessary as there is an authentication and personal data transit ". The complainant, who also reported this circumstance to the Company "twice via PEC on XX and previously on XX", without having received an answer, believes that "article 32 of the [Regulation] has therefore been violated (Security of processing) in particular paragraph 2".

The use of an insecure network protocol (such as the "http" protocol) on the website in question was ascertained by the Guarantor's Office with a service report from the XX.

2. The preliminary investigation.

With a note of the XX (prot. n. XX), the Office, on the basis of the elements acquired, the checks carried out and the facts that emerged following the preliminary investigation, notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation, concerning the alleged violations of articles 5, par. 1, lit. f), 25, para. 1, and 32 of the Regulation, inviting the aforesaid owner to produce defense writings or documents to the Guarantor or to ask to be heard by the Authority (art. 166, paragraphs 6 and 7, of the Code, as well as art. 18, paragraph 1, of the law November 24, 1981, n. 689).

With note of the XX, the Company, through its lawyer, presented a defense brief, declaring, in particular, that:

"within the site there is [...] a reserved area dedicated only to users who have a service supply contract with the company who have previously registered with the ark itself. Once the user has provided the necessary personal data and the data of the user concerned, access credentials consisting of a username and a password are provided. With these codes the user can directly, confidentially and exclusively verify and monitor the information concerning the supply connected to the user contract and can view and print the bills issued, the service provided, the tariffs applied, the type of user assigned, as well as communicate the self-reading";

"no remarks have been made regarding any violations of personal data which occurred following the disputed situation such as to lead to actual damage to the integrity, confidentiality and availability of personal data processed through the site";

"the security profile of the site itself is perfectly adequate to the current recognized standard, the migration under the "https" (Ayper text transfer protocol over secure socket layer) protocol having now [been] completed [on XX (see annex A to

memory)]";

“SII immediately adjusted the security level of the site. Among other things, it is noted that the certificates used for the transition to the "https" protocol were purchased long before the communication from the Guarantor, this as an indication of the alignment action that the company intended to implement";

"the writings to the reserved area are around 13,000 in all, including over 2,000 businesses with a catchment area represented by the inhabitants of the 32 municipalities where the service is provided, which can be quantified at over 220,000";

"the dispute relates to culpable conduct since the factual circumstances exclude any awareness and intentionality of the violation";

"an analysis of the accesses was carried out which returned, with reference to the period under review, a trend free of anomalies and such as to suggest that there were no attempts or completed events of personal data breach [...; moreover] registration passwords are encrypted”;

"following analyzes carried out on the personal data processing activities carried out in the company, SII has adopted a system of technical and organizational measures suitable for managing the risks for the rights and freedoms of natural persons relating to the processing activities carried out in the company";

"Personal data potentially exposed to violations does not fall within those belonging to particular categories since they consist exclusively of name, surname or company name, tax code or VAT number, e-mail and telephone number, billing schedules, in addition to the SII user ID ”;

“no financial or other benefit derived to SII from the disputed conduct. From it, then, no damage has arisen against the complainant or other interested parties and, with the described adjustment intervention, the risk of damage to natural persons in relation to the data that circulate and are transported by the site www.siiato2 .it was demolished in line with the probability and gravity of the same, with reference to the state of the art and costs".

During the hearing, requested pursuant to art. 166, paragraph 6, of the Code and held on the XX date (minutes prot. n. XX of the XX), the Company declared, in particular, that:

"in the reserved area there are no data relating to economic transactions, as it is not possible, for example, to pay bills online or activate bank direct debit";

"the company also acts under a monopoly regime and, therefore, the website has no commercial or advertising purpose, being

only aimed at providing useful information to users";

"The company therefore promptly took note of what was found by the Guarantor's Office during the investigation, taking particular steps to encrypt all user connections to the institutional site and the reserved area. Even following the adoption of these measures, no security incidents have been detected in relation to the personal data in question".

3. Outcome of the preliminary investigation.

Pursuant to art. 5, par. 1, lit. f), of the Regulation, the processing of personal data must be carried out in compliance with the principle of "integrity and confidentiality", on the basis of which personal data must be processed in such a way as to guarantee adequate security, including protection, through measures technical and organizational aspects, from unauthorized or unlawful processing and from accidental loss, destruction or damage.

Based on this principle, the art. 32 of the Regulation provides that the data controller, taking into account the state of the art and implementation costs, as well as the nature, object, context and purposes of the processing, as well as the risk of varying probability and severity for the rights and freedoms of natural persons, must implement adequate technical and organizational measures to guarantee a level of security appropriate to the risk, which include, among other things, where appropriate, "the encryption of personal data".

Furthermore, based on the principle of "data protection since design", formalized by the art. 25, par. 1, of the Regulation, the data controller, taking into account the state of the art and implementation costs, as well as the nature, scope, context and purposes of the processing, as well as the risks having different probabilities and seriousness for the rights and freedoms of natural persons constituted by the processing, must implement, both when determining the means of processing and at the time of the processing itself, adequate technical and organizational measures, aimed at effectively implementing the principles of data protection and to integrate the necessary guarantees in the processing in order to meet the requirements of the Regulation and protect the rights of the interested parties. The council 78 of the Regulation highlights a precise responsibility of the owner, i.e. that of constantly assessing whether he is using, at any time, the appropriate means of treatment and whether the measures chosen actually counteract the existing vulnerabilities. Furthermore, the owner should carry out periodic reviews of the security measures put in place to monitor and protect personal data.

The obligation to maintain, verify and update, where necessary, the processing also applies to pre-existing systems. This implies that the systems designed before the entry into force of the Regulation must be subjected to checks and maintenance

to ensure the application of measures and guarantees that implement the principles and rights of data subjects effectively (see the "Guidelines 4/2019 on article 25 - Data protection from design and by default" adopted by the European Data Protection Committee on 20 October 2020, spec. points 38 and 84).

With particular reference to the principle of "integrity and confidentiality", the controller must (see the aforementioned Guidelines 4/2019 on article 25, specifically point 85):

assess the risks to the security of personal data, considering the impact on the rights and freedoms of data subjects, and effectively counter those identified;

protect personal data from unauthorized and accidental changes and accesses during their transfer.

That said, on the basis of the elements acquired and the facts that emerged following the preliminary investigation, it was ascertained that access to the Company's website dedicated to "online services" (accessible at the address http://...) took place via the "http" (hypertext transfer protocol) network protocol. It was also ascertained that the main page of the aforementioned website contained the forms for entering the users' authentication credentials (username and password).

Furthermore, as emerges from the documentation in the file, the user's personal data can be consulted in the "Personal Data" section of the personal area on the website in question, such as the customer code, name and surname, telephone number, tax code, any VAT number, e-mail address, residential address and the type of service provided. In the "Invoices" section it is also possible to view and download the invoices issued by the Company for the services provided to the user.

In this regard, the Authority, also in compliance with the previous regulatory framework on the protection of personal data, stated that the interaction of a user with a website for the purpose of transmitting personal data must be protected with SSL cryptographic protocols (Secure Socket Layer), ensuring better security against the risk of identity theft always present in web interaction with normal unencrypted http protocols (see, among others, provisions of 10 June 2021, n. 235, doc. web no. 9685922; 2 December 2021, no. 422, web doc. no. 9734884; 2 December 2021, no. 423, web doc. no. 9734934; 27 January 2022, no. 34, web doc. no. 9746448; March 24, 2022, no. 107, web doc. no. 9767635; May 26, 2022, no. 201, web doc. no. 9790365).

The use of state-of-the-art cryptographic techniques is, in fact, one of the measures commonly adopted to protect, in particular, the authentication credentials of users of an online service during their transmission on the Internet; this taking into account the high risks presented by the processing of such data, which may derive from unauthorized access to them or from their

disclosure, also due to the habit of many users to reuse the same password, or in any case a very similar password, for access to various online services.

Access to the website in question, on the other hand, took place in an insecure manner, via the "http" (hypertext transfer protocol) network protocol. In fact, this protocol did not guarantee the confidentiality and integrity of the data exchanged between the user's browser and the server hosting the Company's website, and did not allow users to verify the authenticity of the website viewed. Taking into account the nature, object and purpose of the processing, as well as the risks inherent in the data, including the risk of identity theft, possible cloning of the website for phishing purposes and acquisition of authentication credentials for offenses, the solution adopted by the Company could not, therefore, be considered a suitable technical measure to guarantee a level of security adequate to the risks presented by the treatment.

Failure to use cryptographic techniques for data transport constitutes a violation of art. 5, par. 1, lit. f), and of the art. 32 of the Regulation, whose par. 1, lit. a), moreover, expressly identifies data encryption as one of the possible security measures suitable for guaranteeing a level of security appropriate to the risk (on this point, see also recital no. 83 of the Regulation in the part in which it provides that " the controller […] should assess the risks inherent in the processing and implement measures to limit those risks, such as encryption").

The Company should have implemented, right from the design of its website, adequate technical and organizational measures, aimed at effectively implementing the principles of data protection, including the principle of "integrity and confidentiality", by adopting a secure network protocol, such as the "https" (hypertext transfer protocol over secure socket layer) protocol, within the website that is the subject of the complaint. Therefore, the treatment in question also took place in violation of the art. 25, par. 1, of the Regulation.

4. Conclusions.

In the light of the assessments referred to above, it should be noted that the statements made by the data controller during the preliminary investigation □ the truthfulness of which may be called upon to answer pursuant to art. 168 of the Code □, although worthy of consideration, do not allow overcoming the findings notified by the Office with the act of initiation of the procedure and are insufficient to allow the closure of the present procedure, since none of the cases provided for by the 'art. 11 of the Regulation of the Guarantor n. 1/2019.

It is also represented that for the determination of the applicable rule, in terms of time, the principle of legality pursuant to art.

1, paragraph 2, of the law no. 689/1981 which establishes that «the laws that provide for administrative sanctions are applied only in the cases and in the times considered in them». This determines the obligation to take into consideration the provisions in force at the time of the committed violation, which in the case in question - given the permanent nature of the disputed offense - must be identified at the time of cessation of the unlawful conduct, which occurred after the date of the 25 May 2018 in which the Regulation became applicable and Legislative Decree 10 August 2018, n. 101 came into effect. Indeed, the preliminary investigation documents revealed that the Company adopted the "https" protocol on the 20th date.

Therefore, the preliminary assessments of the Office are confirmed and the illegality of the processing of personal data carried out by the Company is noted for not having implemented suitable technical and organizational measures to guarantee a level of security adequate to the risk, in violation of the articles 5, par. 1, lit. f), and 32 of the Regulation, as well as for having failed to implement, right from the design of the website, adequate technical and organizational measures, aimed at effectively implementing the principles of data protection and integrating the necessary guarantees in the processing in order to meet the requirements of the Regulation and protect the rights of the interested parties, in violation of the art. 25, par. 1, of the Regulation.

The violation of the aforementioned provisions makes the administrative sanction envisaged by art. 83, par. 5, of the Regulation, pursuant to articles 58, par. 2, lit. i), and 83, par. 3, of the same Regulation.

In this context, considering, in any case, that the conduct has exhausted its effects, given that the Company has adopted the "https" protocol on the XX date, the conditions for the adoption of further corrective measures pursuant to art. 'art. 58, par. 2, of the Regulation.

5. Adoption of the injunction order for the application of the pecuniary administrative sanction and accessory sanctions (articles 58, paragraph 2, letter i and 83 of the Regulation; article 166, paragraph 7, of the Code).

The Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation as well as art. 166 of the Code, has the power to "impose a pecuniary administrative sanction pursuant to article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, according to the circumstances of each single case" and, in this context, "the Board [of the Guarantor] adopts the injunction order, with which it also orders the application of the ancillary administrative sanction of its publication, in whole or in part, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code" (art. 16, paragraph 1, of the Guarantor's Regulation no. 1/2019).

In this regard, taking into account the art. 83, par. 3 of the Regulation, in the specific case the violation of the aforementioned provisions is subject to the application of the administrative fine provided for by art. 83, par. 5, of the Regulation.

The aforementioned pecuniary administrative sanction imposed, depending on the circumstances of each individual case, must be determined in the amount taking into due account the elements provided for by art. 83, par. 2, of the Regulation.

In relation to the aforementioned elements, account was taken of the high number of interested parties, registered in the reserved area of the Company's website, whose personal data is being processed ("about 13,000 in all, including over 2,000 businesses"). . It was also considered that, although the complainant had informed the Company on two occasions of the insufficiency of the security measures adopted on the aforesaid site, the Company did not promptly take action, before the start of the investigation by of the Guarantor, to put an end to the violation.

On the other hand, it was taken into consideration that the Company, once it learned of the procedure initiated by the Authority, promptly adopted the necessary measures aimed at resolving the security criticality on its website, providing full cooperation during the investigation. Finally, there are no previous relevant violations committed by the data controller or previous provisions pursuant to art. 58 of the Regulation.

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction in the amount of 15,000 (fifteen thousand) euros for the violation of articles 5, par. 1, lit. f), 25, para. 1, and 32 of the Regulation, as a pecuniary administrative sanction, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

Taking into account the high number of interested parties registered in the reserved area of the Company's website, whose data is being processed, it is also believed that the accessory sanction of publication on the website of the Guarantor of this provision should be applied, provided for by art. 166, paragraph 7, of the Code and art. 16 of the Regulation of the Guarantor n. 1/2019.

Finally, it should be noted that the conditions pursuant to art. 17 of Regulation no. 1/2019.

ALL THIS CONSIDERING THE GUARANTOR

declares, pursuant to art. 57, par. 1, lit. f), of the Regulation, the illegality of the processing carried out by the Integrated Water Service S.c.p.a. for violation of the articles 5, par. 1, lit. f), 25, para. 1, and 32 of the Regulation, in the terms referred to in the justification;

ORDER

to Servizio Idrico Integrato S.c.p.a., in the person of its pro-tempore legal representative, with registered office in Via I Maggio, 65 - 05100 Terni (TR), Tax Code 01250250550, to pay the sum of 15,000 (fifteen 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 15,000 (fifteen thousand) according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of adopting the consequent executive acts pursuant to art. 27 of the law no. 689/1981.

HAS

pursuant to art. 166, paragraph 7, of the Code, the publication of this provision on the website of the Guarantor, believing that the conditions set out in art. 17 of the Regulation of the Guarantor n. 1/2019.

Pursuant to articles 78 of the Regulation, 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision it is possible to lodge an appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the appellant resides abroad.

Rome, 6 October 2022

PRESIDENT

Station

THE SPEAKER

Zest

THE SECRETARY GENERAL

Matthew