[doc. web no. 9538748]

Injunction order against the Campania Regional Environmental Protection Agency (ARPAC) - 14 January 2021

Register of measures

no. 5 of 14 January 2021

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 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, containing provisions for the adaptation of the national legal system to regulation (EU) 2016/679 (legislative decree 30 June 2003, n. 196, as amended by legislative decree 10 August 2018, n. 101, hereinafter "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 available on the website www.garanteprivacy.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 Guarantor's regulation n. 1/2000 on the organization and functioning of the Office of the Guarantor for the protection of personal data (web doc. n. 1098801);

Speaker Prof. Pasquale Stanzione;

WHEREAS

1. The personal data breach.

With notes received on XX and XX (respectively, our prot. nn. XX and XX), the Campania Regional Environmental Protection Agency (hereinafter, "ARPAC" or "Agency") notified this Authority of the data breach personal data pursuant to art. 33 of the

Regulation, consisting in the loss of a device containing personal data.

Based on what was declared by ARPAC in the aforementioned notes:

- the violation concerned the theft of an external hard disk, which took place on the XX date, at the premises of the U.O.C. Contaminated sites and Agency remediation;

- this device contained personal data such as copies of identification documents, tax documents (CUD, models F24 and 730), payslips, reimbursement practices and a list containing analytical data referring to legal proceedings;

- it is not excluded "that the data breach was malicious", and it is considered that this violation "resulted in an illicit removal and possible unauthorized disclosure of the data contained in the external hard disk", and therefore that it, "by virtue of the number of interested parties, the nature, number and degree of sensitivity of the personal data infringed could lead to a consequent risk for the freedoms and rights of the interested parties";

- moreover, this violation would have compromised both the confidentiality of the aforementioned data and their availability, since "the backup saving [was] not successful, consequently the data [were] almost all irreparably lost". As specified in the complaint to the Carabinieri Command made on the XX date, "The data in question had been backed up on the XX, therefore those saved after the aforementioned date were lost";

- the stolen hard disk would have been "connected to the server installed in a room to which any employee can access", as well as the employees of ARPAC Multiservices, the Agency's in-house company.

2. The preliminary investigation.

The Office, with deed n. XX of the XX (notified on the same date by certified e-mail), which here must be understood as reproduced in full, initiated, pursuant to art. 166, paragraph 5, of the Code, with reference to the specific situations of illegality referred to therein, a procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation against ARPAC, for the violation of the articles 5, par. 1, lit. f), and 32 of the Regulation.

With note dated XX (our prot. n. XX of XX), ARPAC sent its defense briefs, pursuant to art. 166, paragraph 6, of the Code, where he represented, in particular, that:

- within the more general process of adaptation to the principles and rules of the Regulation, it has equipped itself, among other things, "with an information security management system suitable for identifying any vulnerabilities in the ARPAC data architecture , adhering to the Consip Framework Contract relating to "Digital identity management and application security

services" - Resolution XX of XX" (describing the contractual services), as well as, with reference to the resources present on the Internet, a series of security measures multiple levels (Firewall protection, security measures for individual workstations, security measures for servers);

- with reference to the specific case, the server to which the stolen hard disk was connected "is normally used as a "Shared Area Server for internal use" in which the technical staff of the Analytical Area inserts, in the Test Report files Provisional (Provisional Certificates of Analysis) the data deriving from the processing of the analytical parameters determined in the samples being analysed. [...] From the subsequent investigation carried out [...] it was found that the aforementioned server also stores spreadsheets (in .xls format), methods of analysis, unsigned letters of transmission of documents in word format, proposed resolutions or unsigned determinations (these are mere word drafts, work being studied and processed and not "judicial data" as erroneously identified in the Data Breach Reporting Form) documentation accompanying the same resolutions and/or determinations, such as requests, offers and declarations of suppliers", as well as a copy of the identity documents of the legal representatives of the latter;

- the device also contained "personal data of employees authorized to access the hard disk in question, in any case protected by an access password, as well as those of their family members, [who] have never been requested by ARPAC. In fact, it should be noted that these data have been improperly stored directly by the aforementioned staff and voluntarily on this shared support in their personal folders";

- all the interested parties identified above (legal representatives of suppliers, employees, their families and external collaborators) would have been contacted in order to be informed "of the theft/loss, for their protection", through communications sent via email, "urging activate any possible precaution aimed at protecting potential negative consequences due to the violation suffered";

- furthermore, "in order to mitigate, from an organizational point of view, further and potential similar episodes", as well as "pending the implementation of Resolution no. XX of the XX of adhesion to the previously mentioned Consip Framework Contract", specific physical security measures. "At the same time, all personnel were urged not to use all IT agency tools and not for personal purposes, as per the ICT Regulation";

- lastly, "further investigations carried out did not reveal any negative consequences, which appear completely unlikely, in relation to any improper use of personal data of both employees and outsiders".

In relation to some aspects not yet clarified, in response to the request for information sent by the Office, pursuant to art. 157 of the Code, the XX (prot. n. XX), ARPAC provided the requested reply, with notes of the XX and XX (respectively, our prot. n. XX and XX):

- attaching a copy of the communications of the violation made to the interested parties, pursuant to articles 33 and 34 of the Regulation (dating back to the XX);

- producing the "employee self-declaration regarding the voluntary storage of their personal data on the hard disk" (dated XX), in which they recognize "the improper use of the data as well as the damage that could be caused achieve";

- confirming that the aforementioned physical security measures have been set up;

- describing the "implementation of the security measures that the SINF Service has intended to adopt, with particular reference to the aspects concerning risk analysis and the measures envisaged to eliminate them, or at least mitigate them", currently in progress;

- by sending, by courier, a CD containing "a copy of the Test Reports relating to the year XX in .pdf format and a copy of the respective spreadsheets in Excel format (work journals), contained in the stolen Hard Disk, as clear proof that they do not contain personal data relating to criminal convictions and crimes or related security measures, pursuant to art. 10 of the Regulation";

- finally communicating the request made to the Carabinieri Headquarters, aimed at acquiring information on any developments in the investigations launched into the matter.

3. Outcome of the preliminary investigation.

The art. 5, par. 1, lit. f), of the Regulation establishes the principle of integrity and confidentiality, pursuant to which personal data are "processed in such a way as to guarantee adequate security of personal data, including protection, through appropriate technical and organizational measures, from unauthorized processing or tort and from accidental loss, destruction or damage".

In implementation of this principle, the subsequent art. 32 establishes that "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 individuals natural persons, the data controller and the data processor implement appropriate technical and organizational measures to guarantee a level of security appropriate to the risk, which

include, among others, where appropriate: a) pseudonymisation and encryption of personal data ; b) the ability to ensure the confidentiality, integrity, availability and resilience of the processing systems and services on a permanent basis; c) the ability to promptly restore the availability and access to personal data in the event of a physical or technical incident; d) a procedure for regularly testing, verifying and evaluating the effectiveness of technical and organizational measures in order to guarantee the security of the processing" (par. 1) and that "In assessing the adequate level of security, special account is taken manner of the risks presented by the processing which derive in particular from the accidental or illegal destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed" (par. 2).

The case in question therefore concerns a breach of personal data, meaning a "breach of security which accidentally or unlawfully leads to the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed" (art. 4, n. 12), of the Regulation), having occurred "an illicit removal and possible unauthorized disclosure of the data contained in the external hard disk", as notified by ARPAC to this Authority pursuant to art. 33 of the Regulation.

With respect to the aforementioned legal framework, it emerged that the reported violation of personal data was made possible due to the absence of the necessary measures to guarantee a level of security appropriate to the risk, required by art. 32 of the Regulation. Indeed, from the documentation in the documents it appears that the following had not been adopted:

- measures necessary to allow the continuity, on a permanent basis, and the restoration of the availability of the stolen personal data, having been recognized, by ARPAC, as the backup operations have not been successful and therefore, even if only wishing to consider those recorded up to the twentieth, "the data [are] almost all irreparably lost";
- techniques able to ensure the non-identifiability of the interested parties to whom the personal data contained in the device referred, to limit the risk of their consultation by unauthorized subjects (such as pseudonymisation or data encryption), also taking into account that any employee could access the room where the stolen device was kept;
- suitable procedures for regularly testing, verifying and evaluating the effectiveness of the technical and organizational measures in order to guarantee the security of the processing.

The claims made by the data controller in the defense briefs pertain to the measures taken after the episode that caused the loss of the hard disk, or in any case being prepared at that time. The initiatives described, although worthy of consideration in the terms that will be explained below, do not eliminate the fact that, when the device containing the personal data was lost, adequate technical and organizational measures had not been taken to ensure protection against unauthorized or unlawful

processing or loss, and to ensure a level of security appropriate to the risk.

For these reasons, on the basis of the elements acquired and the facts that emerged during the investigation activity, it has been ascertained that ARPAC, in relation to the facts in question at the time of the loss of the hard disk, was responsible for the violation of the articles 5, par. 1, lit. f), and 32 of the Regulation.

4. Conclusions.

In the light of the assessments referred to above, taking into account 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 - it should be noted that the elements provided by the data controller in the defense briefs, as well as in the elements provided following the subsequent request for information, although worthy of consideration, do not allow to overcome the findings notified by the Office with the deed of initiation of the proceeding and are insufficient to allow the filing of the proceeding, since none of the cases envisaged by art. 11 of the Guarantor's regulation n. 1/2019.

Therefore, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by ARPAC is noted, for not having adopted adequate technical and organizational measures to ensure protection from unauthorized or unlawful processing or from loss, and for guarantee a level of security appropriate to the risk, in violation of articles 5, par. 1, lit. f), and 32 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. 5, of the same 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; art. 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 present case, the violation of the aforementioned

provisions is subject to the application of the same pecuniary administrative sanction 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 aforesaid elements, it was also considered that the violation concerned personal data which, in terms of quality and quantity, are not particularly significant - moreover, according to what has been declared, in part improperly stored by the interested parties themselves - and from which excluding particular categories of personal data and personal data relating to criminal convictions and offences, pursuant to articles 9 and 10 of the Regulation, and emerged only following an allegedly criminal action carried out by persons to be identified (in relation to which the Agency immediately filed a specific complaint with the competent authorities to ascertain any liability of a criminal nature).

Furthermore, the technical and organizational measures that the Agency has declared to have already prepared on a transitional basis and those in the process of preparation were favorably taken into account, as well as the full cooperation shown towards the Authority in providing elements for the reconstruction of the event and for the mitigation of the possible negative effects of the violation (including the communication of the violation to the interested parties pursuant to Article 34 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 8,000.00 (eight thousand) euros for the violation of articles 5, par. 1, lit. f), 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 that the violation emerged in the event of a presumably criminal conduct which could present aspects of a criminal nature, given the complaint presented by the Agency to the competent authorities, it is also believed that the ancillary sanction of publication on the website of the Guarantor of the this provision, provided for by art. 166, paragraph 7, of the Code and art. 16 of the Guarantor's regulation n. 1/2019.

Finally, it should be noted that the conditions pursuant to art. 17 of the Guarantor's regulation n. 1/2019.

ALL THIS CONSIDERING THE GUARANTOR

the unlawfulness of the treatment carried out by the Campania Regional Environmental Protection Agency (ARPAC) was detected for violation of articles 5, par. 1, lit. f), and 32 of the Regulation, in the terms referred to in the justification,

ORDER

to the Campania Regional Environmental Protection Agency (ARPAC), in the person of its pro tempore legal representative, based in Naples, Via Vicinale S. Maria Del Pianto – Multipurpose Center, Torre 1, Tax Code 07407530638, pursuant to articles 58, par. 2, lit. i), and 83, par. 5, of the Regulation, to pay the sum of 8,000.00 (eight 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 Agency, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of 8,000.00 (eight thousand) euros 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 689/1981;

HAS

a) pursuant to art. 166, paragraph 7, of the Code and of the art. 16 of the Guarantor's regulation n. 1/2019, the publication of this provision on the website of the Guarantor, considering that the conditions set forth in art. are met;

b) pursuant to art. 17 of the Guarantor's regulation n. 1/2019, the annotation in the internal register of the Authority of the violations and measures adopted, pursuant to art. 58, par. 2, of the Regulation, with this provision.

Pursuant to articles 78 of the Regulation, 152 of the Code and 10 of Legislative Decree 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, 14 January 2021

PRESIDENT

station

THE SPEAKER

station

THE SECRETARY GENERAL

Mattei