[doc. web no. 9574117]

Injunction order against General Command of the Port Authorities Corps - Coast Guard - 11 February 2021

Register of measures

no. 55 of 11 February 2021

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 “GDPR”);

CONSIDERING the d. lgs. 30 June 2003, no. 196 containing the "Code regarding the protection of personal data (hereinafter the "Code");

CONSIDERING the general provision n. 243 of 15/5/2014 containing the «Guidelines on the processing of personal data, also contained in administrative deeds and documents, carried out for the purpose of publicity and transparency on the web by public subjects and other obliged bodies», published in the Official Gazette no. 134 of 12/6/2014 and in www.gpdp.it, doc. web no. 3134436 (hereinafter "Guidelines on transparency");

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 4/4/2019, published in the Official Gazette no. 106 of 8/5/2019 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;

GIVEN the observations made by the Secretary General pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web no. 1098801;

Speaker the lawyer Guido Scorza;

WHEREAS

1. Introduction

This Authority has received a report alleging a violation of the legislation on the protection of personal data.

Specifically, it was represented that "on the site of the General Command of the Coast Guard, [it was] possible to view the personal data relating to civic accesses", in which "with a PDF viewer embedded in a browser, for example Firefox, [it was ] possible to obtain a momentary view of the fields obscured with red bordered rectangles» and «once the PDF file was downloaded locally», one could «unlock the security locks also via online procedures, for example via the site [identified in the documents]. [Moreover, the] file obtained could [eva] be easily modified, by removing the masks (rectangles bordered in red), with an application [equipped with] a PDF editing function [...]».

2. Applicable law.

Pursuant to the legislation on the matter, "personal data" is "any information relating to an identified or identifiable natural person ("interested party")" and "an identifiable natural person is one who can be identified, directly or indirectly, with particular reference to a identifier such as a name, an identification number, location data, an online identifier or one or more characteristic elements of its physical, physiological, genetic, psychic, economic, cultural or social identity" (Article 4, paragraph 1 , n. 1, of the GDPR).

The processing of personal data must take place in compliance with the principles indicated in the art. 5 of the GDPR, including those of "purpose limitation" as well as "data minimization", according to which personal data must be - respectively - "collected for specific, explicit and legitimate purposes, and subsequently processed in such a way that incompatible with these purposes", as well as "adequate, pertinent and limited to what is necessary with respect to the purposes for which they are processed" (par. 1, letters b and c).

In this framework, the data controller is required to implement "from the planning stage", i.e. both at the time of determining the means of processing and at the time of processing itself, "adequate technical and organizational measures, [...] aimed at effectively implement the principles of data protection, such as minimization, and to integrate the necessary guarantees in the processing in order to meet the requirements of this regulation and protect the rights of data subjects" (privacy by design), ensuring "that they are processed, by default» (privacy by default) «only the personal data necessary for each specific purpose of the processing» (art. 25, par. 1 and 2, GDPR).

3. Preliminary evaluations of the Office on the processing of personal data carried out.

With the note prot. no. XX of the XX the General Command of the Corps of the Port Authorities - Coast Guard responded to the request for information from the Office (note prot. n. XX of the XX).

Following the checks carried out on the basis of the elements acquired and the facts that emerged following the preliminary investigation, as well as the subsequent assessments, the Office with note prot. no. XX of the XX ascertained that the aforesaid administration - not having adopted «adequate technical and organizational measures», to guarantee the effective obscuring of the personal data contained in the documents relating to civic accesses submitted for online publication - carried out a processing of personal data does not comply with the relevant regulation on the protection of personal data contained in the RGPD. Therefore, with the same note the violations carried out (pursuant to article 166, paragraph 5, of the Code) were notified to the General Command of the Port Authorities - Coast Guard, communicating the start of the procedure for the adoption of the provisions referred to in article 58, par. 2, of the RGPD and inviting the aforementioned entity to send the Guarantor defense writings or documents and, possibly, to ask to be heard by this Authority, within 30 days (Article 166, paragraphs 6 and 7, of the Code; as well as Article 18, paragraph 1, of Law No. 689 of 11/24/1981).

4. Defensive memories and hearing.

With the note prot. no. XX of the XX the General Command of the Corps of the Port Authorities - Coast Guard sent the Guarantor its defensive writings in relation to the notified violations.

In this regard, it should be remembered that, unless the fact constitutes a more serious offence, anyone who, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces false deeds or documents is liable pursuant to art. 168 of the Code, entitled «False statements to the Guarantor and interruption of the performance of the duties or exercise of the powers of the Guarantor».

Specifically, it was highlighted, among other things, that:

- "the activity in question - as will be better explained below - did not consist, in and of itself, in the deliberate "publication of personal data", but in the publication of documents in which personal data were contained, after obscuring the themselves";
- in any case, «some of the personal data, whose publication is contested, belong to the category of the so-called "contact details" of legal persons and, as such, do not fall within the scope of EU Regulation 679/2016, according to the provisions of recital 14 of the same regulation. As represented in the note below, these were data concerning the name and signature of the applicant, the offices, telephone numbers, e-mail addresses, mostly relating to legal persons (companies, organizations or

similar bodies, operating for account of them, such as law firms. In the remaining cases, these were requests presented by journalists-publicists or on behalf of professional orders, media companies, blog managers). Furthermore, these same data were already public, probably by the data subjects themselves, as they could be easily found through a mere consultation activity, on open/free sites (Social, institutional or work-related sites) [...]";

- "the obscuring of personal data contained in documents intended for publication highlights a specific and targeted activity of minimization of the same implemented by this General Command in compliance with the principle referred to in article 5, paragraph 1, letter c) of the EU Regulation 679/2016. In fact, the published file, which can be viewed in ".pdf", reported the complete obscuration of the aforementioned personal data, so that a user with common IT knowledge could not have read them";

- the data «were disclosed as a result of a targeted "alteration" activity of the document thus published, carried out by a third party. In other words, it was not the document published (with the fields darkened) by this Administration that disclosed the aforementioned personal data, but the preordained action of a third party who, on the basis of above-average IT knowledge, through a special computer program knowingly and maliciously removed the "covers" placed by this General Command on the personal data in question. In this sense, [...] it is evident that the alleged violation - i.e. the disclosure of personal data [...], which occurred due to the act of others - could not be attributed to the undersigned, not even as a fault";

- «The level of protection adopted for personal data was consistent with the actual level of threat known up to that moment; in fact, before the disputed episode, the Writer had not received any complaint or report nor was he aware of risk elements that could lead to the need to raise the level of protection adopted to guarantee the security of the processing. Taking into account the minimum known level of threat (assessment of probability and severity), as highlighted above, and the lack of regulations that provide in detail the technical measures to be used for the activity of obscuring personal data, this General Command has placed in be those standard procedures [...] for this purpose suggested by the appropriate diligence and by the deemed reasonableness of the chosen solution, evaluated in terms of costs/benefits and necessary IT skills";

- «In particular, neither - on the one hand - the art. 5, par. 1. lit. c) of the GDPR, nor – on the other hand – the art. 52 of the personal data protection code, after having established, respectively, the "principle of minimization" and the "principle of anonymisation" of personal data (relative to the publication of judgments), give any indication on how this activity should physically be carried out by the obligated party";

- "the presence of the same personal data in question on open/free sites (Social, institutional or work-related sites), can [may] be considered as a specific circumstance to be assessed in order to deem any damage to be minimal invoked by the interested parties, if not completely null, since their personal data were already knowable through - as already mentioned above - a mere activity of consulting websites, or through common search engines that use indexing tools";
- «The reaction of this General Headquarters to the report received was timely and all the necessary corrective actions were immediately put in place, with the result of having further reduced the potential damage caused to the interested parties. Indeed, in relation to the provisions of art. 83, par. 2, lit. c), within 24 hours of receiving the above report, the documents were removed and republished with a stronger technical protection measure (adoption of an image file), suitable for not re-proposing the illicit disclosure. The writer, in the light of the unexpected fact discussed, has responsibly dictated targeted recommendations to his own elements of central and territorial organization so that, should the need to publish documents arise due to a binding legal obligation, more conservative on the unmodifiability of measures suitable for blackout. Finally, with regard to a broader organizational and technical implementation, reconnected to the progressive digitization programs of the Corps' lines of activity, the Writer, at the time of the disputed facts - and since last year to be exact - had already initiated a proceeding tender aimed at identifying a specific provider with which, more recently, it has already entered into a specific contract for the supply of services (expiring on 21 July 2021), for the conduct of dedicated assessments, gap-risk analyses, training and advanced technical assistance. The above activities provide for the launch of specific and necessary IT security initiatives to ensure this General Command the necessary support for the improvement of the security of its cyberspace, both in reference to the security of new services from the early stages planning (by design) and the correction of problems present in the services already active».

5. Outcome of the investigation relating to the report presented

The subject of the specific case brought to the attention of the Guarantor is the adoption of techniques for obscuring the personal data contained in documents published online which have not been effective and can be easily circumvented. Specifically, the preliminary investigation revealed that the complete copies of the documents relating to civic access presented to the administration (application and outcome) had been published on the institutional website of the General Command of the Corps of the Port Authorities, after obscuring the personal data therein contents, as the relative dissemination would have been non-compliant with the regulations on the protection of personal data.

Nonetheless - as also noted by the data controller, following the checks carried out after the intervention of the Guarantor - through the use of programs that allow the modification of pdf files (pdf editor) it was possible to eliminate the "obscuring labels" and report the files to their original form, displaying the fields containing the data and information (including personal ones) obscured. Furthermore, the obscuring technique adopted did not prevent the indexing, and consequent search, of the information contained in the files by web search engines (e.g.: Google).

In this regard - while agreeing with what was represented by the General Command where it was highlighted that, in the case in question, the conduct implemented by the data controller was intended to avoid the dissemination of personal data, which had all been previously obscured - it is necessary to reiterate that the owner of the processing of personal data is in any case required to implement, right from the planning stage (by design), the «adequate technical and organizational measures, [...] aimed at effectively implementing the principles of of data, such as minimisation", integrating "in the processing the necessary guarantees in order to meet the requirements of the [RGPD] and protect the rights of the interested parties" taking into account, among other things, the risks, the context and the scope of application of the treatment, guaranteeing «that, by default» (privacy by default) «only the personal data necessary for each specific purpose of the treatment» (art. 25, p arr. 1 and 2 GDPR).

Furthermore, according to the principle of "accountability" the data controller is not only required to comply with the aforementioned principles and implement the aforementioned technical and organizational measures, but must also be able to demonstrate that he has done so (Articles 5, paragraph 2, and 24 GDPR).

For this reason, while acknowledging the willingness to adopt data minimization techniques through the relative obscuration, it is believed that the data controller has underestimated the risks of the treatment, by not using adequate obscuration techniques - and not having demonstrated that he has done -, since they can be easily overcome with the use of pdf editors by even a not particularly expert user, contrary to what was believed by the General Command.

From this point of view, the fact that the GDPR or the Code - as maintained by the General Command - do not describe data minimization or data obscuring techniques cannot be considered as an exemption or a mitigating element with respect to the conduct held, since the assessment of the adoption of the most appropriate technical and organizational measures to comply with the GDPR is totally left to the choice of the data controller, who must make an adequate assessment taking into account - especially in the Internet environment - the state of the art of existing technologies, of the purposes of the processing, of the

risks of varying probability and severity for the rights and freedoms of natural persons, pursuant to the aforementioned principle of accountability.

As for the nature of the information published, it is clear from the deeds that the processed data referred not only to legal persons (excluded, as correctly highlighted by the General Command, from the application of the legislation on the protection of personal data), but also to persons physical although, according to what has been declared, in many cases linked to working contexts and not belonging to "particular categories of personal data" pursuant to art. 9 of the GDPR. However, for the personal data processed (and not effectively obscured), the exception is unacceptable whereby, in some situations, the data was already public because it was present "on open/free sites (Social, institutional sites or sites relating to workplace)" and therefore "knowable through [...] a mere activity of consulting websites, or through common search engines that use indexing tools". This is because, in any case, this condition would not have authorized the General Command to make public the fact that the aforementioned subjects to whom the data refer (with their contact details) have made requests for civic access to the aforementioned administration (with indication of the requested documents and 'outcome of the request), being able to reveal - in many cases - also the journalistic investigative activity (or of another kind) carried out by the interested parties, who could have every interest in keeping confidential, and out of the knowledge of unauthorized third parties, this type of occupation.

For all of the above, the circumstances highlighted in the written defense considered as a whole, certainly worthy of consideration for the purpose of assessing the conduct, are not sufficient to allow the dismissal of the present proceeding pursuant to art. 11 of the Regulation of the Guarantor n. 1/2019.

In this context, the findings notified by the Office with the note prot. no. XX of the XX and the non-compliance of the processing of personal data object of the report with the relevant regulations on the protection of personal data is noted, as the General Command of the Corps of the Port Authorities - Coast Guard has carried out a processing of personal data:

- not "limited to what is necessary with respect to the purposes for which they are processed" and therefore not respecting the principle of "data minimization", in violation of art. 5, par. 1, lit. b) and c) of the GDPR;
- failing to adopt adequate "technical and organizational measures" "to effectively implement data protection principles" from the design stage and to ensure that only "personal data necessary for each specific processing purpose" are processed by "default setting" , in violation of the art. 25, par. 1 and 2 of the GDPR.

Considering, however, that the conduct has exhausted its effects, as the data controller declared that he had removed the

documents from the institutional website and republished them «with a stronger technical protection measure (adoption of an image file) , suitable for not repeating the unlawful disclosure", without prejudice to what will be said on the application of the administrative fine, the conditions for the adoption of further corrective measures pursuant to art. 58, par. 2 of the GDPR.

6. Adoption of the injunction order for the application of the administrative fine (articles 58, paragraph 2, letter i; 83 GDPR)

The General Command of the Body of the Port Authorities - Coast Guard appears to have violated the articles 5, par. 1, lit. b) and c); 25, par. 1 and 2 of the GDPR. For the violation of the aforementioned provisions, the application of the administrative sanctions pursuant to art. 83, para. 4 and 5 of the GDPR.

In this regard, the art. 83, par. 3, of the GDPR, provides that «If, in relation to the same treatment or related treatments, a data controller or a data processor violates, with malice or negligence, various provisions of this regulation, the total amount of the pecuniary administrative sanction will not exceeds the amount specified for the most serious violation".

With regard to the conduct in question, therefore, the violation of the aforementioned provisions is subject to the more serious administrative pecuniary sanction provided for by art. 83, par. 5 of the GDPR, which therefore applies to the present case.

The Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the GDPR, as well as art. 166 of the Code, has the corrective 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, depending on the circumstances of every single case". In this framework, «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).

The aforementioned pecuniary administrative sanction imposed, according to 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 GDPR.

In this sense, the detected conduct held in violation of the regulations on the protection of personal data was caused by the adoption of ineffective personal data obscuring techniques as they can be circumvented with the help of computer programs that allow the modification of files pdf (pdf editor) easily accessible to any user. The personal data processed do not belong to particular categories or to criminal convictions or crimes (articles 9 and 10 of the GDPR). The conduct is negligent in nature.

Further mitigating elements should be considered the circumstance that the data controller, while underestimating, in good faith, the risks of the treatment, has not in any case received any complaint or report from the interested parties. Furthermore,

the General Command, following the report received, promptly intervened and immediately put in place "all the necessary corrective actions, with the result of having further reduced the potential damage caused to the interested parties [by removing] the documents [...] and publish [them] again with a stronger technical protection measure (adoption of an image file), suitable for not re-proposing the illicit disclosure", collaborating with the Authority during the preliminary investigation of the present proceeding in order to remedy the violation by mitigating its possible negative effects. In the response to the Guarantor, various technical and organizational measures implemented pursuant to articles 25-32 of the RGPD and there are no relevant previous violations of the RGPD committed by the aforementioned administration.

Based on the aforementioned elements, evaluated as a whole, it is deemed necessary to determine pursuant to art. 83, para. 2 and 3, of the RGPD, the amount of the pecuniary sanction, provided for by art. 83, par. 5, of the RGPD, in the amount of 5,000.00 (five thousand) euros for the violation of articles 5, par. 1, lit. b) and c); 25, par. 1 and 2, of the GDPR, as a pecuniary administrative sanction deemed effective, proportionate and dissuasive pursuant to art. 83, par. 1, of the same GDPR.

In relation to the specific circumstances of the present case, relating to the adoption of ineffective techniques for obscuring personal data, it is also believed that the ancillary sanction of publication of this provision on the Guarantor's website should be applied, provided for by art. 166, paragraph 7, of the Code and by art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019.

Finally, it is believed that the conditions set forth in art. 17 of the Regulation of the Guarantor n. 1/2019.

ALL THIS CONSIDERING THE GUARANTOR

having detected the unlawfulness of the treatment carried out by the General Command of the Corps of the Port Authorities - Coast Guard in the terms indicated in the justification pursuant to articles 58, par. 2, lit. i) and 83 of the GDPR

ORDER

to the General Command of the Port Authority Corps - Coast Guard, in the person of its legal representative pro-tempore, with registered office in Via dell'Arte, 16 - 00144 Rome, to pay the sum of 5,000.00 (five thousand) euros by way of pecuniary administrative sanction for the violations referred to in the justification;

ENJOYS

to the same General Command to pay the sum of 5,000.00 (five 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 no. 689/1981.

It should be remembered that the offender retains the right to settle the dispute by paying - always according to the methods indicated in the annex - an amount equal to half of the fine imposed, within the term set out in art. 10, paragraph 3, of Legislative Decree lgs. no. 150 of 09/01/2011 envisaged for the lodging of the appeal as indicated below (art. 166, paragraph 8, of the Code).

HAS

- the publication of this provision on the Guarantor's website pursuant to art. 166, paragraph 7, of the Code and by art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019;

- annotation in the Authority's internal register of the violations and measures adopted pursuant to art. 58, par. 2 of the GDPR with this provision, as required by art. 17 of the Regulation of the Guarantor n. 1/2019.

Pursuant to art. 78 of the GDPR, of the articles 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, 11 February 2021

PRESIDENT

station

THE SPEAKER

Zest

THE SECRETARY GENERAL

Matthew