[doc. web no. 9828965]

Injunction against I.S.P.R.O. - October 20, 2022

Register of measures

no. 344 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 Dr. Claudio Filippi, deputy secretary general;

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 the “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 national legislation 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 the free movement of such data and repealing 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 4/4/2019, 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");

Given 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;

Supervisor Prof. Geneva Cerrina Feroni;

WHEREAS

1. Reporting and preliminary investigation

a) Premise

With a note dated XX, Mr. XX reported an alleged violation of the regulations on the protection of personal data for having received a report, relating to diagnostic tests concerning a third party, from the Careggi University Hospital of Florence (hereinafter the "Company").

In particular, the whistleblower represented that he had received, at his PEC address, on 30 April 2021 "the certified email with the subject "Pathological Anatomy Report XX" (...) (which) as an attachment contained the examination report histology of certain XX".

b) The preliminary investigation

Following the report, the Office, with a note of the XX (prot. n. XX), asked the Company, pursuant to art. 157 of the Code, to provide useful elements for the evaluation of the relevant profiles on the subject of personal data protection.

With a note of the XX (prot. n. XX), the Company provided a response representing, among other things:

- "(...) with respect to the data processing in question, it does not perform the role of data controller but rather of data controller with respect to the controller ISPRO (Institute for the Study, Prevention and Oncological Network), body of the Regional Health Service ";
- "A framework agreement (renewed on 1 March 2021) is active between the Company and ISPRO to regulate various services, each regulated by a specific executive sheet. Among the activities that the Company, through the Department of Services (at which the SOD Histology Pathology and Molecular Diagnostics is established, which carries out laboratory activities of Pathological Anatomy), performs in favor of ISPRO, there is that relating to histological examinations on breast, colorectal, cervical biopsies, on polyps of the rectum and on skin lesions, to which the examination reported to Ms XX is attributable. The executive form of this activity precisely qualifies the Company, with respect to ISPRO, as Data Processor pursuant to art. 28 of the General Regulations";
- "(...) as a result of the difficulty in travel related to the SARS-COV2 epidemic, the SOD Histology, Pathology and Molecular Diagnostics regularly sends reports via PEC (at least those for which particular advice is not required) to users who request it in writing at the time of acceptance, an average of 100 per month";
- "Those in charge of the secretariat of the SOD Pathological Histology and Molecular Diagnostics download the report from the Pathological Anatomy software by optical reading of the barcode present on the acceptance form, and save it in pdf on a spool folder; positioning themselves in the PEC box, they therefore type in the PEC address of the recipient present on the

authorization form signed by the patient, and attach the corresponding report from the spool folder; before sending, they check by means of a preview that the report is the correct one; they therefore note on the paper documentation relating to the file that the transmission of the report via PEC was carried out";

- "The training of secretarial staff takes place by coaching the staff who have been established for the longest time";

- “Regarding the specific alleged violation, the following has been reconstructed: on Friday 30 April, the operator who dealt with the transmission of the reports via PEC that day uploaded all the reports to be sent in the spool folder. The report of Mr. XX and Mrs. XX were one after the other. For mere clerical error, the wrong report was attached”;

- “On the XX date, Mr. XX sent an email to the ordinary email address segreteriaap@aou-careggi.toscana.it in which he stated that he had received another person's medical report (which he attached together with the documentation relating to the acceptance that concerned him). Within 24 hours, the secretariat sent an apology email from the PEC mailbox of the Department of Services to the PEC mailbox of Mr. XX and the correct report”;

- "Ms. XX had duly received her medical report";

- "as an improvement action (and while aware that whenever human intervention is necessary, errors are possible), operators have been given instructions to load only one report at a time into the spool folder, carrying out a further check once the report has been attached related file".

In relation to what was represented by the Company, this Authority, with a note of the XX (prot. n. XX), requested I.S.P.R.O, with headquarters in Florence, Via Cosimo Il Vecchio 2 - 50139 C.F. 94158910482 - VAT number 05872050488 (hereinafter "Institute"), pursuant to art. 157 of the Code, useful information for the assessment of the case, with particular reference to the deed that governs the treatments entrusted to the Company, as Data Processor, with the related obligations and instructions, also inviting the Institute to prove what has been declared with suitable documentation, in compliance with the principle of accountability pursuant to art. 5, par. 2, of the Regulation.

On the 20th date, the Institute provided a response (prot. note no. XX) to the aforementioned request for information, representing, among other things, the following:

- “On 1/3/2021, I.S.P.R.O. has signed with the A.O.U. Careggi an agreement aimed at starting an «inter-company collaboration»”;

- "This agreement then refers to specific «executive files» intended to summarize the «specific services requested, the

reciprocal commitments undertaken, the methods of execution, as well as the related economic aspects and insurance coverage as well as the qualifications assumed by the Companies in terms of treatment and protection of personal data";

- "Among the various specialized services covered by the agreement, there was also the laboratory activity of Pathological Anatomy carried out by the A.O.U. Careggi through its S.O.D. Pathological Histology and Molecular Diagnostics, in which context, in fact, the disputed violation occurred";

- "The subsequent article 11 of the agreement, in paragraph 2, provides that "in the context of the relations between the Parties in relation to the processing of personal data and on the basis of the position respectively assumed - Beneficiary Company or Supplying Company - indicated in the executive forms of referred to in Article 2 above, the Parties qualify respectively and alternatively as Data Controller and Data Processor";

- "In the situation reported by Mr. XX, A.O.U. Careggi acted as manager, while I.S.P.R.O. was the data controller, as can be seen from the attached executive form. As manager, A.O.U. Careggi has undertaken to:

"adopt the necessary and adequate security measures (possibly even additional to those indicated below) in such a way as to minimize the risks of accidental or illegal destruction, loss, modification, unauthorized disclosure or unauthorized access allowed for the personal data transmitted, stored or otherwise processed, or the treatment not compliant with the purposes of the collection" (Article 9 of the contract for the appointment of the manager)";

«implement, within the scope of the contractually assigned tasks, all the fulfilments prescribed by the reference legislation on the protection of personal data in order to minimize the risks of destruction or loss, even accidental, of data, unauthorized access authorized and of treatment not permitted or not compliant with the collection (Article 11 of the contract for the appointment of the person in charge)";

- "Actually, A.O.U. As part of its corporate processes, Careggi has adopted technical measures aimed at avoiding accidents such as those that occurred to Mr. XX, but, based on what emerged in the immediate aftermath of the accident, a mere clerical error, attributable to a person in charge, has resulted in the incorrect sending of the report. No responsibility can be attributed to I.S.P.R.O. for this event, which has appointed A.O.U. Careggi as manager, who therefore, net of the instructions contained in the contract for the appointment of external manager, is required to adopt suitable measures aimed at avoiding unauthorized disclosure of data by virtue of the provisions of the law and regulations in force".

In the light of what was declared in the Institute's documents, the Office, having carried out the relative assessments, with a

note of the XX (prot. n. XX) notified the Institute itself, in relation to the matter in question, pursuant to art. . 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions referred to in article 58, par. 2, of the Regulation. In particular, the Authority communicated the initiation of the sanctioning procedure, noting: the absence of the legal conditions envisaged by art. 9 of the Regulation in the communication of data relating to the health of the patient of the I.S.P.R.O. and, therefore, the violation of this provision, as well as the failure to comply with the principles of "integrity and confidentiality", in violation of art. 5, par. 1, lit. f) of the same Regulation, in the processing of personal data relating to the matter in question; the absence of indication of specific instructions aimed at defining the relationship between the Institute, data controller, and the Company, specifically with regard to the processing entrusted to the latter as data controller (art. 28, par. 3, of the Regulation); the absence of communication of the contact details of the data protection officer to the Authority, in violation of art. 37, par. 7 of the Regulation itself.

With a note of the XX, the Institute sent the Authority a defense brief, in which, in addition to highlighting what has already been declared, it specified that:

- "essential to clarify the non-involvement of this Institute with respect to the disputed violation, is this: the aforementioned agreement does not refer to A.O.U. Careggi the transmission of reports to patients. A.O.U. Careggi, once the tests that are requested through special executive forms have been carried out, send the report to I.S.P.R.O., which, in turn, communicates the results to the patient. Likewise, it is useful to specify that Mr. XX, i.e. the person who made the report from which this proceeding originated, has never entertained relations with I.S.P.R.O. On the contrary, Mrs. XX is included in the uterine cervix screening protocols which, as known, are carried out by I.S.P.R.O.";
- "the communication of reports to patients is not a treatment entrusted to the A.O.U. Careggi, which is required to send the reports to I.S.P.R.O., and not directly to the patient. Which promptly happened, so much so that on 5 May 2021 I.S.P.R.O. proceeded to send the report to Mrs. XX";
- “On the basis of the foregoing, one can better understand what exactly happened: (…) A.O.U. Careggi was to send Mr. XX, under treatment at the same A.O.U. Careggi and which has not with I.S.P.R.O. no report, a report. (…) At the time of sending, evidently due to a mere clerical error by the person in charge, perhaps misled by the partial homonymy, Mrs. XX's report was sent to Mr. XX: in short, A.O.U. Careggi was sending a report to one of its patients for its own purposes, totally unrelated to the scope of the agreement; in this context, he erroneously sent a different report”;

- "it cannot be said that there has been a data breach in the context of the convention in which I.S.P.R.O. works as owner. When Ms. XX's report was sent to Mr. XX, A.O.U. Careggi was not carrying out an activity pursuant to the agreement with I.S.P.R.O. And this because the transmission of reports is not the subject of the agreement; A.O.U. Careggi had to send a report to Mr. XX, his patient, and he made a mistake".

Together with the aforementioned brief, the Institute, also in the face of the failure to transmit the documentation cited in the reply provided on the XX date and noted by the Authority in the act of initiation of the sanctioning procedure, has produced, among other things, a copy of the above agreement mentioned ("Framework agreement for reciprocal regulation of health services") and the related annexes, including the "Executive file" of the "Pathological Anatomy laboratory" activity carried out by the A.O.U. Careggi through its S.O.D. Pathological Histology and Molecular Diagnostics", the "Deliberation of the Director General" no. 175 of 25 June 2018 of the appointment of the Data Protection Officer (DPO) of the Institute, a copy of the communication made on the XX to the Guarantor regarding the data of the DPO, as well as the deed containing "Provisions applicable to the Company identified as data controller data pursuant to art. 28 of EU Regulation 2016/679 (art. 2 and art. 11 Framework Agreement)".

2. Outcome of the preliminary investigation

Having taken note of what was represented during the preliminary procedure by the data controller and the data processor, the following is observed.

The processing of personal data must take place in compliance with the applicable legislation on the protection of personal data and, in particular, with the provisions of the Regulation and of the Code.

With particular reference to the question raised, it should be noted that personal data relating to health deserve greater protection since the context of their processing could create significant risks for fundamental rights and freedoms (Cons. No. 51 of the Regulation).

The regulation on the protection of personal data establishes that personal data must be "processed in such a way as to guarantee adequate security (...), including protection, through appropriate technical and organizational measures, against unauthorized or unlawful processing and against loss , from accidental destruction or damage (principle of "integrity and confidentiality")" (Article 5, paragraph 1, letter f) of the Regulation).

This last provision then provides that "the data controller is responsible for compliance with paragraph 1", in relation to the

principles applicable to the processing of personal data, including that referred to in letter f) "and able to prove it" ("accountability")".

In this sense, the Regulation provides for a "general responsibility of the data controller for any processing of personal data that the latter has carried out directly or that others have carried out on his behalf" (Recital n. 74 of the Regulation in relation to art. 5 of the aforementioned regulation).

The "Data Processor" is the natural or legal person, public authority, service or other body that processes personal data on behalf of the data controller (art. 4, paragraph 8, of the Regulation).

As regards, specifically, the health sector, the regulations on the protection of personal data also provide that information on the state of health can only be communicated to the interested party and can be communicated to third parties only on the basis of a suitable legal prerequisite or upon indication of the interested party subject to written authorization from the latter (Article 9 of the Regulation, as well as Article 84 of the Code - in the previous version the reformulation of the same Code by the legislator with Legislative Decree 10 August 2018 , no. 101 - in conjunction with art. 22, paragraph 11, Legislative Decree no. 101 of 10 August 2018).

3. Conclusions

In the light of the assessments referred to above, taking into account 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 "False statements to the Guarantor and interruption of the execution of the duties or the exercise of the powers of the Guarantor" □ it is represented that the elements provided by the owner himself, in the defense briefs, do not allow to fully overcome the findings notified by the Office with the deed of initiation of the proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

The circumstance, in fact, that the transmission to third parties of the report of XX, a patient of I.S.P.R.O. was carried out by the A.O.U. Careggi, as Data Processor, does not exonerate I.S.P.R.O. from liability, which should have carried out supervisory and control activities on the activity carried out, on its own behalf, by the A.O.U. Careggi (articles 24 and 28 of the Regulation). This, due to the fact that the owner is the person responsible for the decisions regarding the purposes and methods of processing the personal data of the interested parties and who has a "general responsibility" for the treatments implemented (articles 4, par. 1, point 7, art. 5, paragraph 2 of the Regulation - so-called principle of "accountability" and art. 24 of the

Regulation); the same is, in fact, required to "implement adequate and effective measures [and...] demonstrate the compliance of the processing activities with the [...] Regulation, including the effectiveness of the measures" (Cons. n. 74), also with reference to the preparation of technical and organizational measures that meet the requirements of the Regulation in terms of safety (articles 24 and 32 of the Regulation). This obligation also exists when certain processing operations are carried out by a manager who acts on his behalf and when he uses services provided by third parties (see the recent decisions of the Guarantor also relating to the role and related responsibilities of the owner and of the data processor: provision of 2 December 2021, n. 422 and 423, web doc. n. 9734884, 9734934; provision. 17 September 2020, n. 160 and 161, web doc. n. 9461168 and 9461321, provision. 11 February 2021, no. 49, web doc. no. 9562852, as well as provision 17 December 2020, nos. 280, 281 and 282, web doc. nos. 9524175, 9525315 and 9525337; see also already provision 7 March 2019, no. 81, web doc. no. 9121890).

For these reasons, the illegality of the treatment carried out by I.S.P.R.O., in its capacity as data controller, is noted in relation to the ascertained communication of data relating to the health of one of its patients carried out in the absence of a legal basis, in violation of art. 9, as well as the basic principles referred to in art. 5, par. 1, lit. f), of the Regulation.

The violation of the aforementioned provisions makes it applicable, pursuant to art. 58, par. 2, lit. i), the administrative sanction provided for by art. 83, par. 5, letter. a) of the Regulation, as also referred to by art. 166, paragraph 2, of the Code.

In this framework, taking into account that measures have been implemented to minimize the risk of similar events occurring (see note of the XX, prot. n. XX), the conditions for the adoption of measures, of a prescriptive or inhibitory, pursuant to art. 58, par. 2, of the Regulation.

4. 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 violation of the articles 5, par. 1, lit. f) and 9 of the Regulation in relation to the matter covered by this provision, attributable to the Institute on the basis of the aforementioned provisions, is subject to the application of the administrative pecuniary sanction pursuant to art. 83, par. 5, letter. a) of the Regulation and 166, paragraph 2, 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

College [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 account the principles of effectiveness, proportionality and dissuasiveness, indicated in art. 83, par. 1, of the Regulation, in the light of the elements provided for in art. 83, par. 2, of the same Regulation, in relation to which it is observed that:

- the communication of health-related data sent to a third party not authorized to receive them concerned only one patient (Article 83, paragraph 2, letters a) and g) of the Regulation);
- with respect to the affair, no willful behavior emerges (article 83, paragraph 2, letter b) of the Regulation);
- no provision concerning a pertinent violation has been previously adopted against the Institute (article 83, paragraph 2, letter e) of the Regulation);
- it is necessary to take into account the fact that it was an isolated case that took place in the context of the Institute's institutional activity, the particular social relevance of which is noted with respect to the continuity of oncological investigations (art. 83, paragraph 2, lett. k) of the Regulation).

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 5, letter. a) of the Regulations, to the extent of 7,000.00 (seven thousand) euros for the violation of articles 5, par. 1, lit. f) and 9 of the Regulation as a pecuniary administrative sanction deemed, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed that due to the nature of the data, the ancillary sanction of publication, on the website of the Guarantor, of this provision, 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 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

ALL THIS CONSIDERING THE GUARANTOR

declares the unlawfulness of the processing of personal data carried out by the data controller I.S.P.R.O., with registered office in Florence, Via Cosimo Il Vecchio 2 – 50139, C.F. 94158910482 - P. Iva 05872050488, for the violation of the articles 5, par.

1, lit. f) and 9 of the Regulation in the terms referred to in the justification;

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to I.S.P.R.O., to pay the sum of 7,000.00 (seven thousand) euros as an administrative fine for the violations indicated in this provision; 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 data controller, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of 7,000.00 (seven 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 n. 689/1981.

HAS

pursuant to art. 166, paragraph 7, of the Code, the entire publication of this provision on the website of the Guarantor and believes that the conditions set forth 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.

Pursuant to art. 78 of the Regulation, 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, 20 October 2022

PRESIDENT

Station

THE SPEAKER

Cerrina Feroni

THE DEPUTY SECRETARY GENERAL

Philippi