[doc. web no. 9815947]

Injunction against Bper Banca S.p.A. - September 15, 2022

Register of measures

no. 305 of 15 September 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 (hereinafter, the "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 complaint presented pursuant to art. 77 of the Regulation on 22 August 2019 by Dr. XX against Bper Banca S.p.A. and regularised, in part, on 8 November 2019 and, finally, on 27 May 2020;

HAVING EXAMINED the documentation in the deeds;

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

SPEAKER Prof. Pasquale Stanzione;

WHEREAS

1. The complaint against the Company and the preliminary investigation.

With a complaint presented on August 22, 2019, then regularized, following invitations to regularize, in part on November 8, 2019 and, finally, on May 27, 2020, Dr. XX complained about alleged violations of the Regulation by Bper Banca S.p.A. (hereinafter, the Company), with reference to the late and unsuitable response to requests for cancellation pursuant to art. 17 of the Regulation presented by the complainant with reference to his/her data processed by the Company.

The Company, in responding to the request of the Office of 10 July 2020, with a note dated 17 August 2020 stated that:

to. "on 12 January 2019, the [complainant] asked, by email to serviziopersonale@pber.it, what was the procedure for deleting

his professional profile and his personal data from the database relating to applications [...]. This email was answered on 15 January 2019 by the institute, asking to send the request accompanied by identity documents, so as to unambiguously recognize the applicant. On 16 January 2019, the institute, at the same email address, received the identity document and the tax code of the [complainant]. However, this last communication was not followed up by the function in charge (HR planning and development service), following an internal mistake" (see note cited, page 1);

b. "on 18 April 2019, the [claimant], through his lawyer, sent this institution a registered letter with return receipt presenting alleged pecuniary and non-pecuniary damages due to the failure to cancel [...] the user generated by them [...]. This communication, even though it contained an explicit request for «the cancellation of the personal data of the [complainant] present in every database managed by Bper Banca Spa», was analyzed as a complaint [...];

c. “the profile referring to the [complainant] and the data entered by him were removed on 6 May 2019 from the front end of the «Work with us» section. Following this intervention, the system no longer allowed the recognition of the account/profile at the time generated by them with the combination of "username and password" chosen. From that date, access to the system through the user offered an error message, no longer finding the data referable to the account created by the candidate and therefore inhibiting access to any other information" (see note 17.8.2020 cit. , p. 1);

d. "on 29 May 2019 the username was definitively canceled by the system administrator" (see note cited, p. 1);

And. "following the definitive cancellation of the user [...] a response was given to the [complainant], through his lawyer, on 17 June 2019" (see cited note, p. 1).

Following the invitation to provide further clarifications sent by this Authority, with notes dated 18 February 2021, the Company represented that "considering the content of the letters [of 18 April 2019 and 21 May 2019] they had initially been classified as a complaint. However, the institute has decided not to proceed in this sense, providing only for the cancellation of the profile and the consequent response. At the same time, the migration activities of the e-mail application were underway, scheduled for the period from 20 to 31 May for the structure responsible for responding. This intervention resulted in a partial misalignment, changing the start of the response times to the letter of May 21, 2019" (see note of February 18, 2021 cited above, p. 1).

On 15 April 2021, the Company also declared that the specific personal data concerning the complainant that it currently processes includes: personal and identification data, contact details (address, telephone number, e-mail), photographic images

present on a copy of the document of the employee's identity, information relating to professional skills and career path (studies, self-assessment of skills, training courses), information relating to employment relationships with the Company (registration number, type of relationship, reason for hiring reason for termination, employment status, salary level, type of contract, positions and organizational roles held, workplaces). With reference to these data, he specified that he processed them for the purpose of "administrative, accounting, operational and organizational management of the employment relationship" and that he kept them for "ten years from the conclusion of the employment relationship". With reference, then, to the personal and identification data, to the contact data and to the data relating to attendance, he specified to treat them for the purpose of "management of the obligations connected with the payment of salaries" for "ten years from the generation of the document relating to the payment , except for the data transposed into the single employment register, kept for the times required by law".

The Company also declared that it "apply[ed] a rule of retention of relevant data in line with the ordinary statutory limitation period of rights, as well as with the terms for public investigations (for example tax, criminal, etc.). [...] in the event of litigation and/or administrative/judicial proceedings, the bank could keep the data for a further period than the one indicated above to exercise its right of defense and/or comply with the requests of the authorities. It is understood that, once the dispute and/or proceeding have ceased, the ordinary conservation terms will once again apply".

2. The initiation of the procedure for the adoption of corrective measures and the deductions of the Company.

On 16 August 2021, the Office carried out, pursuant to art. 166, paragraph 5, of the Code, the notification to the Company of the alleged violations of the Regulation found, with reference to articles 12 and 17 of the Regulation.

With defensive writings, sent on September 13, 2021, the Company declared that:

to. "By e-mail dated 12 January 2019, the [complainant] requested Bper Banca S.p.A. [...] what was the procedure for deleting your personal profile and personal data at the time contained in the "Work with us" section of the Company's website [...]. Having received the elements necessary to identify the interested party (identity documents and tax code), due to a technical problem, no effective response was provided" (note 13.9.2021 cit., p. 1);

b. "on 18 April 2019 the [claimant], through his lawyer, sent a registered letter highlighting unspecified «pecuniary and non-pecuniary damages" caused by the failure to respond to the first request [...]. Considering the presence within the second request of elements of dispute and claim not pertaining to privacy issues, the Privacy and Data Protection Office has launched,

in line with the operating practices for the management of the so-called "non-technical/mixed" requests/complaints, the involvement of the Legal Department and the Human Resources Department, as well as the offices responsible for managing personal data and the branch in which the bank relationships held in the name of the [complainant] were hinged; these initiatives with the aim of evaluating any possible impact and protective action, as well as preventing a coordinated response concerning i) the request for data deletion; ii) any legal aspects related to the blackmailing tone of the request; iii) the procedures for acquiring the personal data of candidates for employment; iv) the more comprehensive management of the data referring to the bank relationships of the interested party as a customer and to the employment relationships of the same (taking into account that the interested party had also been employed by the Institute for specific periods of time)" (see cited note, p. 2);

c. “with particular reference to the request for deletion of personal data, the Company has proceeded with progressive actions functional to the protection of the right exercised; in particular, on 6 May 2019 (i.e. 18 days after the second request) the Human Resources Department physically deleted the data of the interested party from the tables of the database underlying the "Work with us" section of the site and subsequently, on May 29, 2019, he deleted the user and password of the account, stored in a different table of the said database. Due to the cancellation of the interested party's data, the system no longer allowed the association of the account/profile created by the interested party with the data uploaded by the same, thus generating the error message" (see cited note, p. 2, 3);

d. "on 17 June 2019 the Bank proceeded to formally acknowledge the second request of the interested party acknowledging [...] that the right to cancellation had in substance already been accepted - within the limits of the provisions of art. 17 of the [Regulation] - through [the] interventions of 6 May and 29 May 2019" (see cited note, p. 3);

And. on the culpable nature of the violations, it is premised that "the story that involved the [complainant] constitutes an isolated and unfortunate episode in a general context of operations characterized by systematic and timely responses in relation to the responses to requests to exercise the rights of the interested parties. In support of this statement, it is reported that the Company receives an average of about 20 requests from interested parties per month whose management is not followed up, in almost all cases, by further requests or complaints. In terms of timing, it should also be noted that over 80% of requests receive a reply within 20 days of receipt and the remainder in any case within the regulatory deadline of one month" (see cited note, p. 4);

f. "with specific reference to the first request, it is necessary to point out that despite the presence of consolidated operating practices relating to the responses to the exercise requests of the interested parties, the function in charge did not, at the time, act and operate as requested due to the failure to take charge of fulfillment. With reference to the second request, the deletion of the data subject's data, despite having been correctly taken over and satisfied under the substantial aspect on 6 May 2019 (deletion of personal data from the database) and 29 May 2019 (deletion of user and password), was formally verified late on 17 June due to contextual and prominent requests from the interested party. These elements of contestation and claim have in fact created the need to involve various functions for the management of the second request, with a consequent increase in operating times in order to arrive at an assessment that includes all the most appropriate initiatives (including possibly legal protection) for a complete and coordinated feedback. [...] the Company tries to find individual "non-technical/mixed" letters/complaints through a single reply, collecting contributions from the various functions which are called upon to provide their opinion for various reasons (e.g. Legal Function, Human Resources Function, etc. .); this coordination of functions was, in the specific case, complex due to the presence of multiple elements of claim and the different roles that the interested party had within the company (job candidate, employee, customer). In this context, as a further element of difficulty, the migration of the Company's e-mail system [...] occurred in the second half of May 2019, generating some problems in the communication flows between the various corporate functions. This concatenation of situations has led both to the non-activation, pursuant to the legislation, of the right to postpone the terms, and ultimately to a belated reply to the interested party" (see cited note, p. 5);

g. the Company "capitalized on the events [that occurred] as part of a process of progressive strengthening of the practices and processes underlying the protection of the rights of the data subjects themselves. In fact, in addition to more effective coordination of the various corporate functions involved from time to time in the management of "atechnical/mixed" requests, the owner of which has been identified in the Privacy and Data Protection Office (located within the Compliance Department) and a more stringent monitoring, based on the register of requests, of the timing of fulfillment has given rise to a progressive strengthening of the workforce of this function which, starting from n. 5 resources in the workforce in 2018, currently consists of n. 6 resources with a target of n. 8" (see cited note, p. 6);

h. on the degree of responsibility of the owner taking into account the technical and organizational measures implemented pursuant to articles 25 and 32 "in the presence of "atechnical/mixed" requests, the functions involved (normally the Privacy and Data Protection Office, Complaints and Disguises Office, Legal Department) promptly discuss the nature of the request and

the competence of the response. […] the analyzes of the contents of the requests are systematically carried out in such a way that they can be completed within the ordinarily foreseen period of one month from their receipt" (see cited note, p. 6, 7);

the. on the nature, seriousness of the violation, the number of interested parties involved, the categories of data processed and the measures to mitigate the damages against the interested parties "the company has merely delayed the fulfillment of its obligations pursuant to articles 12 and 17 of the Regulation towards the interested party, whose legitimate claims then naturally found full satisfaction. For this reason [...] it is believed that the violations committed can only be considered as "minor" violations [...] also taking into account the impact generated on a single data subject and the common nature of the personal data processed" (see note cited ., p. 7);

j. on the degree of cooperation "the company has always complied promptly with requests for information [from the] Authority" (see cited note, p. 8);

k. on losses avoided as a result of the violation "given the delay in replying, it is represented that the company has not achieved any benefit or advantage, nor avoided losses, in committing the alleged violations" (see cited note, p. 8).

3. The outcome of the investigation and of the procedure for the adoption of corrective and sanctioning measures.

As a result of the examination of the declarations made to the Authority during the proceeding as well as of the documentation acquired, it appears that the Company, as owner, has carried out some processing operations, referring to the complainant, which are not compliant with the regulations on the matter of protection of personal data, in particular with reference to the late and inappropriate response to requests for the exercise of rights.

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

The data controller, based on the provisions of art. 12 of the Regulation "facilitates the exercise of the rights of the interested party pursuant to articles from 15 to 22" and "provides the interested party with information relating to the action taken regarding a request pursuant to articles from 15 to 22 without unjustified delay and, in any case, at the latest within one month of receipt of the request. This deadline may be extended by two months, if necessary, taking into account the complexity and number of requests".

The same article 12, par. 4 of the Regulation specifies that in the event that he does not comply with the requests to exercise the rights "the data controller informs the interested party without delay and at the latest within one month of receiving the request, of the reasons for the non-compliance and of the possibility of lodge a complaint with a supervisory authority and to lodge a judicial appeal".

The art. 17 of the Regulation recognizes the interested party "the right to obtain from the data controller the cancellation of personal data concerning him without unjustified delay and the data controller has the obligation to cancel personal data without unjustified delay, if [between the other] the personal data are no longer necessary with respect to the purposes for which they were collected or otherwise processed".

From the elements acquired during the preliminary investigation it emerged that the Company gave a merely formal response to the request for cancellation "from the [...] website [of Bber Banca S.p.A.] [of] the professional profile [and of] personal data from the database relating to [the bank's] applications" submitted on 12 January 2019 by the complainant.

In fact, it has been ascertained that on 15 January 2019 the Company informed the interested party that "in order to proceed with the removal of his account, the [...] technical support needs to scan the identity card and tax code attached to the cancellation request" but, despite the fact that the complainant sent the requested documentation (identity document and tax code) the following day, due to a "technical problem", he then did not provide an effective reply to the request.

This conduct violates art. 12 with reference to the art. 17 of the Regulation, taking into account that, once the (lawful) need of the Company to verify the identity of the interested party requesting the exercise of the right to cancellation has been satisfied, the same has not followed up the request for an undefined "technical problem" caused by the "failure to take charge of the fulfilment", forcing the interested party, through his lawyer, to request the exercise of the right to cancellation with a new request.

In fact, not having received any response to his request, through his lawyer, on 18 April 2019 the complainant asked, among other things, "to proceed with the immediate cancellation of the personal data of the [complainant] present in each database managed by Bper Banca S.p.A." and on 21 May 2019, given the lack of any response from the Company, it presented a reminder to the requests already formulated previously.

Only on 17 June 2019, i.e. a good four months after the expiry of the legal term, did the Company give an effective response to the cancellation requests presented by the complainant.

In this regard, the Company, during the preliminary investigation, specified that it had found the request of 18 April 2019 "formally [...] late" and reiterated on 21 May 2019, in particular on 17 June 2019, "due to contextual and pre-eminent requests of the interested party" which "have in fact created the need for the involvement of various functions", but to have substantially fulfilled in practice what was requested prior to the formal reply, in particular by deleting the personal data relating to the complainant's candidacy from its database in date 6 May 2019 and deleting the user id and password relating to the aforementioned account on 29 May 2019.

The Company also specified that "the migration of the Company's e-mail system [...] which occurred in the second half of May 2019, generating some disruptions in the communication flows between the various corporate Functions" contributed to generating the delay in feedback.

However, the conduct of the Company is in contrast with the obligation to provide feedback "without unjustified delay" to the interested party and in any case within one month of receiving the request pursuant to art. 12 of the Regulation.

Taking into account the complexity and number of requests, the holder can take advantage of the extension of the two-month deadline, but, by express regulatory provision, must in any case inform the interested party of the extension and the reasons for the delay, within one month of receiving the request .

If, in fact, the effective removal of the data provided for the application in the "Work with us" section of the Company's website was partially implemented on 6 May, and then definitively on 29 May 2019, the communication to the interested party of the actions taken to satisfy the exercised right was only carried out on 17 June 2019.

What was previously noted therefore constitutes a violation of art. 12 in relation to the art. 17 of the Regulation.

On the other hand, with reference to the non-cancellation of data relating to the complainant (other than those communicated for the purposes of selection for a job) relating to previous employment relationships between the complainant and the Company itself and to bank relationships in the terms and for the purposes indicated during the preliminary investigation, what was represented by the Company regarding the legitimacy of further conservation of the same was shared.

In this regard, however, it has been ascertained that in relation to the aforementioned need to retain certain data, the Company, in violation of the provisions of art. 12 par. 4 of the Regulation, in declaring its (lawful) impossibility of cancellation, has not indicated to the complainant the possibility of proposing a complaint to the supervisory authority or judicial appeal. This aspect denotes the unsuitability of the response as regards the persistent - albeit, as specified, lawful - need to keep certain

data referring to the complainant.

4. Conclusions: declaration of illegality of the treatment. Corrective measures pursuant to art. 58, par. 2, Regulation.

For the aforementioned reasons, the Authority believes that the declarations, documentation and reconstructions provided by the data controller during the preliminary investigation do not allow the findings notified by the Office to be overcome with the act of initiating the procedure and are therefore unsuitable to allow the filing of this proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

The late and unsuitable response by the Company to the cancellation request presented by the complainant is in fact illegal, in the terms set out above, in relation to art. 12 in relation to the art. 17 of the Regulation.

The violation ascertained in the terms set out in the reasoning cannot be considered "minor", taking into account the nature, gravity and duration of the violation itself, the degree of responsibility, the manner in which the supervisory authority became aware of the violation (cons. 148 of the Regulation).

Therefore, given the corrective powers attributed by art. 58, par. 2 of the Regulation, the application of a pecuniary administrative sanction pursuant to art. 83 of the Regulation, commensurate with the circumstances of the specific case (Article 58, paragraph 2, letter i) 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; art. 166, paragraph 7, of the Code).

At the end of the proceeding, it appears that Bper Banca S.p.A. has violated the art. 12 in relation to the art. 17 of the Regulation. For the violation of the aforementioned provisions, the application of the pecuniary administrative sanction envisaged by art. 83, par. 5, letter. a) and b) of the Regulation, through the adoption of an injunction order (art. 18, law 11.24.1981, n. 689).

Considering it necessary to apply paragraph 3 of the art. 83 of the Regulation where it provides that "If, in relation to the same treatment or related treatments, a data controller [...] violates, with willful misconduct or negligence, various provisions of this regulation, the total amount of the pecuniary administrative sanction does not exceed amount specified for the most serious violation", the total amount of the fine is calculated so as not to exceed the maximum prescribed by the same art. 83, par. 5.

With reference to the elements listed by art. 83, par. 2 of the Regulation for the purposes of applying the pecuniary administrative sanction and the relative quantification, taking into account that the sanction must "in any case [be] effective,

proportionate and dissuasive" (Article 83, paragraph 1 of the Regulation), it is represented that In the present case, the following circumstances were considered:

a) in relation to the nature, gravity and duration of the violation, the nature of the violation was considered relevant, which concerned the information, communications and methods for exercising the rights of the interested party;

b) with reference to the intentional or negligent nature of the violation and the degree of responsibility of the owner, the conduct of the Company and the degree of responsibility of the same was taken into consideration which did not comply with the data protection regulations with reference to the 'art. 12 in relation to the art. 17 of the Regulation;

c) in favor of the Company, account was taken of the relevant cooperation with the Supervisory Authority for the purpose of defining the complaint and of the fact that the violation ascertained concerned only the complainant, constituting an isolated case.

Furthermore, it is believed that they assume relevance in the present case, taking into account the aforementioned principles of effectiveness, proportionality and dissuasiveness with which the Authority must comply in determining the amount of the fine (Article 83, paragraph 1, of the Regulation) , firstly the economic conditions of the offender, determined on the basis of the revenues earned by the company with reference to the ordinary financial statements for the year 2021. Lastly, the entity of the sanctions imposed in similar cases is taken into account.

In the light of the elements indicated above and the assessments made, it is believed, in the present case, to apply the administrative sanction of payment of a sum equal to Euro 10,000 (ten thousand) against Bper Banca S.p.A..

In this context, it is also considered, in consideration of the type of violations ascertained that concerned the exercise of the rights of the interested party, that pursuant to art. 166, paragraph 7, of the Code and of the art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019, this provision must be published on the Guarantor's website.

It is also believed that the conditions pursuant to art. 17 of Regulation no. 1/2019.

ALL THAT BEING CONSIDERED, THE GUARANTOR

notes the illegality of the processing carried out by Bper Banca S.p.A., in the person of its legal representative, with registered office in Via San Carlo 8/20, Modena (MO), C.F. 01153230360, pursuant to art. 143 of the Code, for the violation of the art. 12 in relation to art. 17 of the Regulation;

ORDER

pursuant to art. 58, par. 2, lit. i) of the Regulation to Bper Banca S.p.A., to pay the sum of 10,000 (ten thousand) euros as an administrative fine for the violations indicated in this provision;

ENJOYS

then to the same Company to pay the aforementioned sum of 10,000 (ten 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 deeds pursuant to art. 27 of the law n. 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 attachment - 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 of the art. 16, paragraph 1, of the Guarantor Regulation n. 1/20129, and believes that the conditions pursuant to art. 17 of Regulation no. 1/2019.

Pursuant to art. 78 of the Regulation, as well as articles 152 of the Code and 10 of Legislative Decree no. 150/2011, opposition to the ordinary judicial authority may be lodged against this provision, with an appeal lodged with the ordinary court of the place identified in the same art. 10, within the term of thirty days from the date of communication of the measure itself, or sixty days if the appellant resides abroad.

Rome, 15 September 2022

PRESIDENT

station

THE SPEAKER

Station

THE SECRETARY GENERAL

Matthew