SEE ALSO Newsletter of 26 June 2020

[doc. web no. 9429195]

Injunction against UniCredit S.p.A. - June 10, 2020

Register of measures

no. 99 of 10 June 2020

GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by Dr. Antonello Soro, president, Dr. Augusta Iannini, vice-president, Dr. Giovanna Bianchi Clerici and Prof. Licia Califano, members and Dr. Giuseppe Busia, general secretary;

HAVING REGARD to the law of 24 November 1981, n. 689, and subsequent amendments and additions, with particular reference to art. 1, paragraph 2;

NOTING that the Office of the Guarantor, with deed no. 15976/119444 of 14 May 2019 which must be understood as fully referred to here, challenged UniCredit S.p.A. (hereinafter "the Company"), in the person of its pro-tempore legal representative, with registered office in Milan, Piazza Gae Aulenti no. 3, P.I. 00348170101, the administrative violations envisaged by the articles 162, paragraph 2-bis, 162, paragraph 2-ter, and 164-bis, paragraph 2, of the Personal Data Protection Code (Legislative Decree 196/2003, hereinafter referred to as the "Code", in the previous wording to the changes that occurred following the entry into force of Legislative Decree 101/2018), in relation to articles 33 and 154, paragraph 1, lett. c), of the same Code;

NOTING that, from the examination of the documents of the sanctioning procedure, initiated with the aforementioned notice of contestation, it emerged that:

- on 25 July 2017, the Company notified this Authority that it had suffered an IT intrusion, which occurred in two distinct moments in a period of time between April 2016 and July 2017, which resulted in unauthorized access to personal data referring to approximately 762,000 interested parties; these unauthorized accesses were made with the users of some employees of an external commercial partner (the company Penta Finanziamenti Italia S.r.l., hereinafter "Penta") through an application called Speedy Arena. In particular, it was found that the data, object of the violation, consisted of: personal data and contact details, profession, level of study, identification details of an identification document and information relating to the employer, salary, loan amount, status of the payment, "approximation of the customer's credit classification" and Iban code;

- the Office launched a complex preliminary investigation against the Company, culminating in an inspection which took place on 22, 23 and 24 October 2018;

- following the investigation carried out by the Office, the Guarantor adopted, on 28 March 2019, provision no. 87 (available at www.gpdp.it, web doc. n. 9104006, hereinafter "provision"), to which reference is made in full, with which it declared the processing of personal data put in place by Unicredit to be unlawful, as as data controller, because it was carried out in violation of the minimum security measures provided for by articles 33 et seq. of the Code and the technical specification referred to in Annex B) to the Code itself and the measures prescribed by provision no. 192 of 12 May 2011, containing "Requirements regarding the circulation of information in the banking sector and the tracing of banking transactions" (web doc. n. 1813953);

- the violation of the minimum security measures pursuant to art. 33 of the Code was ascertained with reference to the non-compliance with rules nos. 12 and 13 of the technical specification referred to in Att. B) to the Code, in relation to the use of an unsuitable authorization system of the Speedy Arena application and the absence of the "access limit" of the authorization profiles to only the data necessary to carry out the processing operations;

- the violation of the measures prescribed by provision no. 192 of 12 May 2011 was ascertained in relation to the inadequacy and incorrect storage of the tracking logs of operations performed on the Speedy Arena application, the failure to implement alerts for operations performed through the aforementioned application and the failure to perform internal control audits;

NOTING that, with the aforementioned deed of 14 May 2019, the Company, in its capacity as data controller pursuant to articles 4, paragraph 1, lett. f), and 28 of the Code:

- the administrative violation envisaged by art. 162, paragraph 2-bis, of the Code, in relation to art. 33, with reference to the failure to adopt the minimum security measures;

- the administrative violation envisaged by art. 162, paragraph 2-ter, of the Code, in relation to art. 154, paragraph 1, lett. c), with reference to the non-compliance with the instructions given by the Guarantor with provision no. 192 of 12 May 2011;

- finally, the violation provided for by art. 164-bis, paragraph 2, of the Code, with reference to the circumstance that the violations committed refer to databases of particular relevance or size;

DETECTED from the report prepared by the Office pursuant to art. 17 of the law n. 689/1981 that the reduced payment has not been made in relation to the violations referred to in articles 162, paragraph 2-bis, and 162, paragraph 2-ter, of the Code;

HAVING REGARD to the written defenses, sent on 12 June 2019 pursuant to art. 18 of the law n. 689/1981, which are referred to in full here, with which the Company has illustrated the reasons why the conditions for the application of sanctions do not exist in relation to the violations under dispute and has, in summary, declared that:

- with reference to the violation of the security measures pursuant to art. 33 of the Code, the authorization system adopted, with respect to the Speedy Arena application, was fully compliant with the provisions contained in rule 12 of the Technical Regulations referred to in Annex B) to the Code, in force at the material time, provided that "there was no error in the definition of the authorization profiles which were correctly set up and operational". Instead, "unlawful access to personal data was only possible due to incorrect management of access credentials by Penta which allowed the subsequent exploitation of an application bug". The Speedy Arena application could only be used via the Extranet, i.e. an extension of the corporate network suitable for allowing subjects operating outside the Company to access the information or services of the Company itself, access to which (analytically described in point 3.1 , letters a) and b), of the written defence) was possible through an encrypted channel and subject to passing a double IT authentication procedure by the user;
- unlike what was noted in the Provision and subsequently disputed, "the authorization profiles for each UniCredit appointee or for homogeneous classes of appointees are identified and configured prior to the start of the processing, so as to limit access only to data necessary to carry out the processing operations". The Company therefore claims that it has correctly defined the access levels to the Speedy Arena application, but that, due to an improper use of access credentials by Penta users, which was followed by the exploitation of a computer bug of the back-end systems of the aforementioned application, it was possible to overcome the visibility restrictions and access segregations, which had instead been implemented correctly;
- "the circumstance that it was not possible to access the logs tracing the operations carried out (...) and that these logs did not report the registration of the customer's code involved in the bank data access operation by the person in charge does not imply total inadequacy of the security measures adopted". In fact, the Company had adopted a banking transaction tracking system, to integrate and complement the log collection systems for individual applications, which allowed it to reconstruct the events related to the data breach. In particular, it was possible to identify the start date of the violation and its scope, thanks to the log collection system which collected the firewall logs, which included: the case number, the user code of the operator who carried out the access operation, the IP address from which the operation is carried out, the date and time of execution of the operation and the type of operation carried out in accordance with the measures prescribed in point 1, lett. b), of the provision

of 12 May 2011;

- finally, with regard to the dispute relating to the failure to implement alerts, the company stated that, already at the time of the disputed events, a firewall system was in place which filtered and evaluated the amount of traffic on the company's applications as a whole which, when particularly high traffic thresholds were exceeded, sent an alert "without being able to identify a number of queries such as those in the case in question which, although high for the individual application, were not significant with respect to the IT traffic that a credit institution how Unicredit manages it on a daily basis";

READ the minutes of the hearing, held on 6 November 2019, pursuant to art. 18 of the law n. 689/1981, with which the party reaffirmed what had already been declared in the defense briefs, requesting the dismissal of the sanctioning procedure or, alternatively, the application of sanctions to the extent of the statutory minimum, in consideration of the fact that the interested parties have not suffered any harm and that the Company has further strengthened its security measures;

CONSIDERING that, unless the fact constitutes a more serious offence, whoever, 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 "False statements to the Guarantor and interruption of the performance of the duties or exercise of the powers of the Guarantor";

CONSIDERING also that the significant profiles of illegality of the processing that emerged in the present case, as a consequence of the failure to adopt adequate technical and organizational measures, in any case require the corrective intervention of this Authority in today's terms, in order to safeguard the rights and freedoms of the data subjects regardless of the notification of the personal data breach made by the data controller;

WHEREAS the arguments put forward are not suitable for excluding the liability of the party in relation to the disputed matter. In fact, in its written defence, the party clarified many aspects related to the setting up of IT authentication systems which, on the basis of the checks carried out by the Office, were actually compliant with the provisions indicated in the Technical Regulations. Otherwise, the aspects related to the setting up of the authorization systems of the persons in charge of processing, referred to in rules no. 12 and no. 13 of the aforementioned Technical Regulations. The documentation acquired during the preliminary investigation phase and, above all, the checks carried out during the inspection, highlighted an incorrect design of the authorization system of the Speedy Arena application which was particularly weak both at the front-end and back-end level -end. On the other hand, the same Company had shown, in the audit report of November 30, 2017, how the

Speedy Arena application had been developed to be used only by internal employees (who have no restriction on the visibility of files) and that it was was subsequently also extended to subjects outside the Company, implementing a segregation of accesses which later proved to be unsafe. In fact, "exploiting some weaknesses in the security of the application in question, unknown subjects, through the credentials assigned to Penta personnel, had access to personal data present in financing practices that did not fall within the scope of Penta's mandate, resulting in this way the data breach object of the communication of July 25, 2017" (minutes of October 22, 2018, p. 3). The ascertained presence of some weaknesses of the Speedy Arena application, even if caused by an IT bug (a circumstance that was never represented by the Company during the preliminary investigation), still remains attributable to the sphere of responsibility of the data controller who, in 'prepare the measures referred to in Att. B) to the Code, aimed at ensuring a minimum level of protection of personal data, must guarantee its effectiveness over time and cannot, therefore, be attributed to Penta. In fact, it turned out that Penta operators, after having passed the computer authentication procedures, could access any financing procedure (both "consumer loans" and "salary-backed loans"), taking advantage of the aforementioned weaknesses of the Speedy Arena application, simply by changing the identification number of the case and, above all, regardless of the authorization profile assigned to them. Where, on the other hand, the authorization profiles had been correctly set up and configured with the access restrictions, each Penta operator could only have consulted the data relating to the practices within their competence, as the authorization system would have blocked all access to managed practices from other subjects. However, it was verified that the access restrictions, associated with the authorization profiles, did not work correctly. It should be noted, differently from what was deduced by the owner, that the possibility of also viewing files not within its competence is a circumstance that is independent of the improper use of the utilities used by the persons in charge. Therefore, violations of the security measures referred to in art. must be confirmed. 33 of the Code.

As regards the violation relating to the non-compliance with provision no. 192 of 12 May 2011, it is noted that, regardless of the circumstance that the Company was able to identify the fundamental aspects related to the data breach and to adopt the necessary measures, there is no doubt that the tracking logs had not been correctly implemented, both with reference the log retention times (which was less than 24 months from the date of registration of the operation) and with reference to the failure to indicate the code of the customer involved in the operation of access to bank data. With reference to the first aspect, the same Company has represented that "as no log files are available prior to April 28, 2016, the exact scope of the data breach

cannot be determined" (audit report of November 30, 2017), due to the impossibility to find useful elements. With reference, however, to the second aspect, it is noted that the Guarantor considered that the registration in the tracking logs of the customer's code (together with the other information identified in point 4.2.1 of provision no. 192) is essential in order to ensure effective control of the activities carried out on customer data by each person in charge of processing. Among other things, this prescriptive measure is functional to the others indicated in the provision, including that relating to the activation of specific alerts aimed at detecting intrusions or anomalous and abusive accesses to information systems, analyzing and correlating the tracking logs relating to all the applications used by the persons in charge of the treatment. The circumstance that the case number was present in the logs, instead of the customer's code, would not have made it possible, except through a complex and articulated operation of cross-referencing the data present in the logs with customer data (also considering that the same file may refer to several customers or that different files may refer to the same customer) correlate the tracking logs generated by different applications of the Company. The Company itself declared, during the preliminary investigation, that at the time the illegitimate accesses occurred, there was no alert mechanism useful for detecting anomalous behavior, in the face of access operations performed by users external to the Company (such as Penta operators). In fact, with respect to the specific data breach episode that is the subject of this proceeding, it emerged that "customer files were consulted with a frequency of up to 10 per second, in consecutive order by a single user", without this anomalous behavior being detected , and that the failure to activate alerts was one of the conditions that "contributed to the exfiltration of data, which lasted for at least 14 months without being identified" (audit report of 30 November 2017). In view of the above, it is believed that the Company is liable for the failure to adopt the measures prescribed by provision no. 192;

NOTING, therefore, that UniCredit S.p.A., as data controller pursuant to articles 4, paragraph 1, lett. f) and 28 of the Code, is found to have committed the violations pursuant to articles 162, paragraph 2-bis, and 162, paragraph 2-ter, of the same Code, as indicated in the notice of dispute no. 15976/119444 of 14 May 2019, as well as the violation pursuant to art. 164-bis, paragraph 2, for having committed the aforementioned violations in relation to databases of particular relevance and size;

CONSIDERING that, for the purposes of the amount of the pecuniary sanctions, it is necessary to take into account, pursuant to art. 11 of the law n. 689/1981, of the work carried out by the agent to eliminate or mitigate the consequences of the violation, the seriousness of the violation, the personality and economic conditions of the offender;

WHEREAS, in the present case:

- with regard to the aspect of seriousness, the elements relating to the intensity of the psychological element and the extent of the danger and damage must be assessed taking into account that the violations are committed in relation to a significant number of interested parties;

- for the purposes of assessing the work performed by the agent, it must be noted that the Company, following the data breach in question, has adopted various measures and launched initiatives aimed at strengthening the security of its IT systems;

- regarding the personality of the author of the violation, the circumstance that there are no previous sanctioning proceedings against UniCredit S.p.A. must be considered;

- with regard to the economic conditions of the agent, the financial statements for the year 2018 were taken into consideration;

CONSIDERED, therefore, of having to determine, pursuant to art. 11 of the law n. 689/1981, the amount of the pecuniary sanctions, based on the aforementioned elements evaluated as a whole, to the extent of:

- 120,000.00 (one hundred and twenty thousand) euros for the violation pursuant to art. 162, paragraph 2-bis, of the Code, in relation to art. 33;

- 180,000.00 (one hundred and eighty thousand) euros for the violation pursuant to art. 162, paragraph 2-ter, of the Code, in relation to art. 154, paragraph 1, lett. c);

- 300,000.00 (three hundred thousand) euros for the violation pursuant to art. 164-bis, paragraph 2, of the Code;

for a total amount of Euro 600,000.00 (six hundred thousand);

HAVING REGARD to the documentation in the deeds;

CONSIDERING the law n. 689/1981 and subsequent amendments and additions;

GIVEN the observations made by the Secretary General pursuant to art. 15 of the guarantor's regulation n. 1/2000, adopted with resolution of 28 June 2000;

SPEAKER Dr. Augusta Iannini;

ORDER

to UniCredit S.p.A., in the person of its pro-tempore legal representative, to pay the sum of Euro 600,000.00 (six hundred thousand), as a pecuniary administrative sanction for the violations indicated in the justification;

ENJOYS

to the aforementioned company to pay the sum of Euro 600,000.00 (six hundred thousand), according to the procedures

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 of 24 November 1981, n. 689.

Pursuant to articles 152 of the Code and 10 of Legislative Decree no. 150/2011, opposition to this provision may be lodged with the ordinary judicial authority, with an appeal lodged with the ordinary court of the place where the data controller has his residence, within the term of thirty days from the date of communication of the provision itself or sixty days if the appellant resides abroad.

Rome, 10 June 2020

PRESIDENT

Soro

THE SPEAKER

Iannini

THE SECRETARY GENERAL

Busia