[doc. web n. 9718112]

Injunction order against Intesa Sanpaolo s.p.a. - May 27, 2021

Record of measures

n. 270 of May 27, 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, Professor Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, members and the cons. Fabio Mattei general secretary;

GIVEN the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "Regulation");

GIVEN the legislative decree 30 June 2003, n. 196 (Code regarding the protection of personal data, hereinafter the "Code") as amended by Legislative Decree 10 August 2018, n. 101 on "Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679";

GIVEN the complaint submitted to the Guarantor pursuant to Article 77 of the Regulation, with which Mr. XX complained about the alleged unlawful communication of data relating to the banking relationships he had with Intesa Sanpaolo S.p.a. (hereinafter "the credit institution", "the bank" or "IntesaSP") to an unauthorized third party;

EXAMINED the documentation in deeds;

HAVING REGARD to the observations made by the Secretary General pursuant to art. 15 of the regulation of the Guarantor n. 1/2000;

SPEAKER Prof. Ginevra Cerrina Feroni;

WHEREAS

1. The complaint and the preliminary investigation.

1.1 With the complaint presented on 10 March 2020, Mr. XX complained about the unlawfulness of the processing of personal data concerning him put in place by Intesa Sanpaolo S.p.a. - branch of Catanzaro 1, with specific regard to the unlawful communication of data relating to banking relationships maintained by the same with the aforementioned credit institution to an unauthorized third party, an employee of the same institution.

The Office, therefore, with a note dated June 16, 2020 (prot. No. 22092) invited the bank to provide information and

clarifications on the facts of the complaint; the latter, with communication dated 1 July 2020 (prot. n. 24256) represented that, following the report received by Mr. XX on 11 March 2019, "it had been possible to ascertain the actual incorrect processing of personal data of the same contained in periodic accounting reports "and" this circumstance was acknowledged by the interested party with a note dated 12 June 2019 "; subsequently, in response to the requests, formulated by Mr. XX through his lawyer, to know the details of the employees responsible for the illegal access and the extent of any disciplinary sanctions imposed on them, the bank provided negative feedback, considering that the requests were "unrelated to the exercise of the rights of the interested party as indicated in Regulation (EU) 2016/679 and in Legislative Decree no. 196/2003 ".

1.2. With a note dated 1 September 2020 (prot. No. 32139) the Office, on the basis of the elements acquired during the investigation, notified the data controller, pursuant to art. 166, paragraph 5, of the Code, the alleged violations, with reference to arts. 5, par. 1, lett. a) and f) and 6 of the Regulations as well as with the specific provisions referred to in par. 4.3.2 of the provision of the Guarantor of 12 May 2011 “on the circulation of information in the banking sector and tracking of banking transactions” (web doc. No. 1813953) and in par. 3.1 and 3.2 of the "Guidelines on the processing of personal data of customers in the banking sector" of 25 October 2007 (web doc. No. 1457247), as they are compatible with the new regulatory framework pursuant to art. 22, paragraph 4 of the legislative decree n. 101/2018. With the same note, the credit institution was invited to produce defensive writings or documents or to ask to be heard by the Authority (Article 166, paragraphs 6 and 7, of the Code; as well as Article 18, paragraph 1, law no. 689 of November 24, 1981).

1.3 Intesa Sanpaolo S.p.a., on 28 September 2020 (prot. No. 36039) sent its defense writings, which are referred to here in full, with which it has, among other things, represented that:

a) already in response to the complaint presented to the bank by the interested party, the Internal Control Function of the same bank had "found that the employee Ms. (...), former spouse of Mr. XX, had carried out, on Sunday 3 March 2019 - not already as an employee of the bank, but using the codes assigned to the account holder - access to the multi-channel contract no. (...) by the customer, resulting in 16 sending - via the internet banking functions - of quarterly account statements for the years 2016 and 2017 relating to current account no. (…) Linked to the multichannel contract in question "; the aforementioned "accounting reports were sent to the employee's private email address: in 15 cases the email address associated with the contract was deselected (...), while for the sending of the account statement as of 31 December 2017, forwarding was maintained for acquaintance with the e-mail address of Mr. XX, thus generating the complaint proposed by the customer "; the

aforementioned mailings were "carried out using a smartphone device and with the use of the correct access credentials and the OTP key delivered to Mr. XX in October 2015";

b) on the other hand, "from the related analyzes activated, on the basis of the internal legislation implementing the provision 192/2011 of the Guarantor, on access to the personal data of Mr. XX possibly carried out by Mrs. (...) as an employee" it emerged that "the same, in the period between January 21, 2019 and May 10, 2019 and making use of the IT qualifications assigned to it for the performance of its duties at the Catanzaro 1 branch, made requests for inquiries on the relationships held by Mr. XX, in the absence of operational needs and / or related operations; however, to the best of our knowledge, the communication to other third parties of the information obtained by Ms (…) through these queries has not yet emerged ";

c) consequently, the behavior of the employee "in open conflict with the law and company regulations on the processing of personal data", was the subject of the "letter of dispute of 13 June 2019", with which "IntesaSP initiated a disciplinary procedure against Ms (...), then finalized with the suspension from the service and the salary for ten days (...) or the maximum conservative sanction, together with a further period of unpaid leave ";

d) "on the basis of subsequent monitoring, it appears that the employee has no longer carried out any further unauthorized inquiries on the relationships of the client Mr. XX";

e) "following an application filed pursuant to Articles 335 of the Italian Criminal Code and 110 bis of Legislative Decree 271/1989 it emerged that the bank is indicated as an offended person in the criminal proceedings (...) pending in the trial phase before the Public Prosecutor's Office at the Court of Catanzaro and arisen following a complaint presented by Mr. XX for the facts covered by this; in anticipation of the trial hearing scheduled for September 15, 2021, the bank will consider filing a civil party ".

1.4. The Office, having examined the defense brief of Intesa Sanpaolo S.p.a., with a note dated 9 October 2020 (prot. 10 May 2019 (see paragraph 1.3, letter b)), asked the bank to provide a copy of the access logs relating to the aforementioned period and to specify which types of alerts had been activated in the bank's IT systems for detection anomalous or risky behaviors relating to inquiries on customer personal data (see par. 4.3.1 of provision 192/2011).

In producing the required documentation, Intesa Sanpaolo S.p.a., with a note dated 22 October 2020 (prot. , that “an additional set of controls is in the process of being activated” based on new types of alerts and that “the Internal Control Function carries out the checks provided for in point 4.3.2 of provision no. 192/2011 ".

As regards the alerts already active, the same, in summary, relate to:

a) three specific types of processing operations carried out, in the absence of specific conditions, by any bank operator:

1. queries made through the "CRIF-GATE CUSTOMER RISK SYSTEM" application (used to acquire credit information relating to customers with loans in progress or who have requested a loan);

2. queries concerning the handling of credit or debit cards;

3. cancellation of bank transfer operations;

b) the interrogation operations carried out, in the course of a week or the reference quarter of the control, by an operator of the online branch on the same customer.

On the other hand, with regard to the alerts being activated, they concern specific types of processing operations (access to "personal data and information by consulting document filing tools" or "personal data relating to terminated relationships") or a particular category of subjects authorized to process ("queries by users of Central Management functions carried out on all active relationships").

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

Upon examination of the declarations made by the data controller during the procedure referred to in art. 166, paragraph 5 of the Code, as well as the documentation acquired in the acts, this Authority formulates the following considerations.

2.1 It is clear that, in this case, the employee in question, in the period between 21 January 2019 and 10 May 2019, making use of the IT qualifications that have been assigned to her for the performance of her duties at the Catanzaro 1 branch , has accessed the bank details of the complainant, former spouse of the same, in the absence of the latter's consent or other legitimate prerequisite; the processing carried out is therefore illegal as it is in contrast with the general principles on data protection pursuant to art. 5, par. 1, lett. a) and f) and 6 of the Regulations.

2.2 In the light of what was represented by the data controller during the sanctioning procedure regarding the alerts active on 22 October 2020, it appears that these operated exclusively on some specific types of operations or on query operations carried out by a particular category of subjects authorized for processing. In particular, the alerts referred to in letter a) (see above, paragraph 1.4) take into consideration only the query operations that concern information on credit relationships, the movements of a payment card or the cancellation of wire transfers, while the alerts referred to in letter b) (see above, paragraph 1.4) are aimed at detecting abnormal or risky behavior assumed exclusively by operators of the online branch.

From the above it emerges that the credit institution, until 22 October 2020, had not implemented alerts suitable for detecting, in a complete way, anomalous behavior in the face of inquiry operations carried out by operators of a traditional branch, limiting itself to activating, in order to this type of person authorized to process, only some alerts relating to specific types of transactions.

On the other hand, it should be noted - for the sake of completeness of the analysis - that the same alerts that IntesaSP has declared to be being activated, do not appear to overcome the criticality described, as they too refer to specific types of processing operations (accesses to "data and personal information by consulting document filing tools" or "personal data relating to terminated relationships") or to a particular category of persons authorized to process the processing ("users of Central Management functions").

2.3 With the note dated 22 October 2020, IntesaSP also provided a copy of the access logs made by the employee - and former spouse of the complainant - in the period between 21 January and 10 May 2019 to the personal data of the complainant.

The technical examination of the aforementioned access logs showed that, aggregating them on a daily basis, the accesses, even if not carried out on holidays or outside working hours, appear to be numerous on the days of 8 and 11 February 2019 (respectively, 336 and 115 accesses); even aggregating them on a weekly and monthly basis, the accesses made in the first two weeks of February 2019 (respectively, 341 and 233 accesses) and those made in February 2019 (708 accesses) are numerous, even compared to the other periods subject to analysis .

In this regard, even though we do not have detailed information that allows us to understand the types of operations carried out in the various accesses and considering that each processing operation may have generated multiple records in the access log (as commonly occurs in the Customer Information Control System), it is believed that the accesses made by the employee in this case (related to various financial relationships) were indeed numerous and that they would probably have been classified as anomalous or at risk if the credit institution had previously activated adequate and specific alerts. The activation of alerts capable of detecting anomalous or risky behaviors relating to inquiry operations carried out, in a specific period (day, week or month), by an operator of a traditional branch on the data of the same customer would - with reasonable probability - allowed the bank to detect improper accesses made by the employee and to adopt adequate and timely corrective measures, mitigating the negative effects on the person concerned.

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

3.1 For the aforementioned reasons, taking into account the nature, object, context and purpose of the processing in question, which concerns particularly sensitive data (such as banking data) and which presents high risks for the rights and freedoms of individuals physical, the Authority believes that the measures adopted by IntesaSP have not proved suitable for detecting the behavioral violation that is the subject of the complaint, allowing - rectius, not preventing - the carrying out of illegal operations of consultation of banking data carried out by subjects acting under the authority of the data controller. In particular, the ascertained violation is considered to be the source of the failure to adopt and implement specific alerts aimed at detecting intrusions or anomalous and abusive accesses to the information systems of a banking institution; measure, moreover, which is mentioned in the aforementioned provision of the Guarantor no. 192 of 12 May 2011 (see point 4.3.1 and point 1), lett. d), point i), of the device), pursuant to art. 154, paragraph 1, lett. c), of the previous Code, and which must currently be considered a measure that a data controller is required to adopt, also in implementation of the principles of "integrity and confidentiality" pursuant to art. 5, par. 1, lett. f) and 32 of the Regulations.

From here:

- the ascertainment of the behavioral violation - denounced with the complaint of Mr. XX - consisting in the execution by a bank employee, in the time period between 21 January 2019 and 10 May 2019, of a series of accesses to the complainant's bank data - making use of the IT authorizations assigned to him / her in the absence the consent of the claimant or other legitimate cause of justification (violation of the general principles on data protection referred to in articles 5, paragraph 1, letters a) and f), and 6 of the regulation);

- the attribution of such illegal behavior to the intermediary, as a direct source of procedural and organizational deficiencies, as well as the omitted supervision of the employee's illegal actions; and, indeed, the measures adopted by IntesaSP - as confirmed by the analysis of the access logs carried out by the employee (see par. art. 5, par. 1, lett. f) and art. 32 of the Regulation which establishes that the data controller must implement measures to "ensure the confidentiality, integrity, availability and resilience of the processing systems and services on a permanent basis" (Article 32, par. 1, letter b)) and that in "assessing the adequate level of security, special account is taken of the risks presented by the processing that derive in particular from the destruction, loss, modification, unauthorized disclosure or access, in accidental or illegal way, to personal data transmitted, stored or otherwise processed "(art. 32, par. 2).

3.2. Therefore:

- a pecuniary administrative sanction is imposed pursuant to art. 83 of the Regulation, commensurate with the circumstances of the specific case ((Article 58, paragraph 2, letter i) of the Regulation), for the behavioral violation consisting in unauthorized accesses carried out by a bank employee, former spouse of the complainant ;

- in the exercise of the corrective powers attributed to the Authority by art. 58, par. 2 of the Regulation, taking into account the nature of the ascertained violation - deriving ex post from the failure to prepare adequate security safeguards ex ante - the credit institution is ordered to conform the processing of personal data to the provisions of the Regulation, providing for the adoption of further and adequate measures (alerts) - according to the indications referred to in par. 3.1 - aimed at implementing checks on the legitimacy and lawfulness of access to customer data by all persons authorized to process and to sensitize them to compliance with the instructions given to them, within 120 days of receipt of this provision.

4. Injunction order.

Pursuant to art. 58, par. 2, lett. i) of the Regulations and art. 166, paragraphs 3 and 7 of the Code, the Guarantor provides for the application of the pecuniary administrative sanction provided for by art. 83, par. 5, lett. a) of the Regulation, through the adoption of an injunction order (Article 18, Law 24 November 1981, no. 689), in relation to the processing of personal data referring to the complainant, whose unlawfulness has been ascertained, within the terms set out above, in relation to articles 5, par. 1, lett. a), and f), 6.

Considering it necessary to apply paragraph 3 of art. 83 of the Regulation where it provides that "If, in relation to the same treatment or related treatments, a data controller [...] violates, with intent or negligence, various provisions of this regulation, the total amount of the pecuniary administrative sanction does not exceed the amount specified for the most serious violation "; considering that the ascertained violations of art. 5 of the Regulation are to be considered more serious, as they relate to the non-compliance with a plurality of general principles applicable to the processing of personal data, the total amount of the sanction is calculated in such a way as not to exceed the maximum permitted by law for the aforementioned violation. .

With reference to the elements listed in art. 83, par. 2, of the Regulation for the purpose of applying the pecuniary administrative sanction and its quantification, taking into account that the sanction must "in any case [be] effective, proportionate and dissuasive" (Article 83, par. 1 of the Regulation), is represents that, in the present case, the following circumstances were taken into consideration:

a) with regard to the nature, gravity and duration of the violation, the nature of the violation was considered, which concerned the general principles of treatment in terms of security; with reference to the seriousness, account was taken of the fact that the owner was aware of the violation only following a report by the interested party;

b) with regard to the willful or negligent nature of the violations and the degree of responsibility of the data controller (Article 83, paragraph 2, letter b) and d) of the Regulation) the negligent conduct of the intermediary was taken into consideration, whose procedural and organizational deficiencies and the omission of supervision, have ultimately made it possible to commit the offense materially committed by the employee, to the detriment of the legal sphere of the complainant;

c) the fact that the credit institution cooperated with the Authority during the procedure;

d) the absence of specific precedents - relating to the same type of treatment - by Intesa Sanpaolo S.p.a .;

e) the circumstance that the personal data affected by the violation are bank data, therefore common data of particular delicacy, but not belonging to the category of particular data referred to in art. 9 of the Regulations;

f) with reference to any other aggravating or mitigating factors applicable to the circumstances of the specific case (Article 83, paragraph 2, letter k)), the following was considered as an attenuating element:

- the activation of the disciplinary procedure against the employee responsible for the illegal access, which resulted in the suspension from the service and from the salary for ten days, together with an additional period of unpaid leave;
- the circumstance that the violation ascertained by the Offices has damaged the legal sphere of a single customer (the complainant).

Furthermore, it is believed that they assume relevance in the case in question, in consideration of the aforementioned principles of effectiveness, proportionality and dissuasiveness (Article 83, paragraph 1, of the Regulation) to which the Authority must comply in determining the amount of the sanction , the economic conditions of the offender, determined on the basis of the revenues achieved and referring to the financial statements for the year 2020.

Based on the aforementioned elements, assessed as a whole, it is believed to apply to Intesa Sanpaolo S.p.a. the administrative sanction for the payment of a sum equal to Euro 200,000.00 (two hundred thousand).

In this framework, in consideration of the type of violations ascertained, which involved the adoption of adequate security measures such as to effectively implement, right from the design, the principles of data protection, it is believed that, pursuant to art. 166, paragraph 7, of the Code and art. 16, paragraph 1, of the regulation of the Guarantor n. 1/2019, this provision

should be published on the Guarantor's website.

Finally, it is noted that the conditions set out in art. 17 of regulation no. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

WHEREAS, THE GUARANTOR

declares, pursuant to art. 57, par. 1, lett. f) and 83 of the Regulations as well as art. 166 of the Code, the unlawfulness of the processing carried out, in the terms set out in the motivation, by Intesa Sanpaolo S.p.a., for the violation of articles 5, par. 1, lett. a) and f), and 6 of the Regulations;

INJUNCES

then to Intesa Sanpaolo s.p.a., based in Turin, Piazza San Carlo, 156, P.I. 11991500015, in the person of the pro-tempore legal representative, to pay the sum of Euro 200,000.00 (two hundred thousand), according to the methods indicated in the annex, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to from art. 27 of the law n. 689/1981. It is represented that pursuant to art. 166, paragraph 8 of the Code, the offender has the right to settle the dispute by paying - again in the manner indicated in the annex - of an amount equal to half of the sanction imposed within the term referred to in art. 10, paragraph 3, of d. lgs. n. 150 of 1 September 2011 envisaged for the submission of the appeal as indicated below;

INJUNCES

pursuant to art. 58, par. 2, lett. d) of the Regulations, to the aforementioned Company, to conform the processing of personal data to the provisions of the Regulations, providing for the adoption of further and adequate measures (alerts) - according to the indications referred to in par. 3.1 - aimed at implementing checks on the legitimacy and lawfulness of access to customer data by all persons authorized to process and to sensitize them to compliance with the instructions given to them, within 120 days of receipt of this provision;

HAS

pursuant to art. 166, paragraph 7, of the Code and art. 16, paragraph 1, of the regulation of the Guarantor n. 1/2019, the publication of this provision on the website of the Guarantor and believes that the conditions set out in art. 17 of regulation no. 1/2019.

Pursuant to art. 78 of the Regulation, of art. 152 of the Code and 10 of the legislative decree 1 September 2011, n. 150,

against this provision, it is possible to 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 applicant resides abroad.

Rome, May 27, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Cerrina Feroni

THE SECRETARY GENERAL

Mattei