[doc. web n. 9812423]

Injunction order against Intesa Sanpaolo S.p.a. - July 28, 2022

Record of measures

n. 272 of 28 July 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, 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 presented by Ms XX on 03/03/2021 pursuant to art. 77 of the Regulation, with which Intesa Sanpaolo S.p.a was alleged to have violated the personal data protection regulations;

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

SPEAKER Attorney Guido Scorza;

WHEREAS

1. The complaint and the preliminary investigation.

With the complaint presented to this Authority on 03/03/2021, Ms XX, represented and defended by the Movimento Difesa del citizen Friuli V.G., complained about the unlawfulness of the processing of personal data concerning her put in place by Intesa Sanpaolo S.p.a. (hereinafter, "ISP" or "the bank" or "the institution"); in particular, the complainant, holder of a current account at the Latisana (UD) branch - "formerly the Veneto Banca branch" - represented that an employee of the same branch would have accessed her accounting positions, not justified by operational needs, with subsequent use of the same for the purposes of a judicial proceeding.

Following the invitation formulated by this Office to provide specific observations in relation to what is stated in the complaint,

with a note dated 30/03/2021, Intesa Sanpaolo S.p.a., in providing a copy "of the irrelevant queries made in the period between 18 September 2018 and 29 October 2018 "by the employee in question, illustrated the different types of alerts activated by the bank in compliance with the provisions contained in the provision of the Guarantor no. 192 of 12 May 2011 for the detection of anomalous or risky behaviors relating to inquiries on customer personal data (see paragraph 4.3.1 of the aforementioned provision), specifying at the same time that:

1. in 2018, following the request of the current complainant, "verbally made to the manager of the Latisana branch, to inhibit a specific employee of Intesa Sanpaolo, with whom he reported having had private meetings, access to any information relating to its relations with the Bank, the Internal Control Function proceeded with the appropriate checks on access to the customer's personal data. These checks revealed personal data queries, including of an accounting nature, carried out in the months of September / October 2018 in the absence of professional reasons by the employee mentioned by Ms XX, also in contrast with internal provisions. As a result of the results of these checks, the competent personnel management function imposed a disciplinary sanction pursuant to art. 7 of the law n. 300/1970 ";

2. the progressively implemented alerts, which “are part of the internal regulations made available to the Bank's staff, operate on the basis of frequency criteria in compliance with the provisions of law no. 300 and the Internal Control Function annually carries out the checks provided for in point 4.3.2 of Provision no. 192/2011 "; the same relate to:

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

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);

queries concerning the handling of credit or debit cards;

cancellation of bank transfer transactions;

b) query 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;

c) "access to personal data and information by consulting the document filing tools carried out by traditional or online branch personnel, during the control reference quarter";

d) "queries by users of Central Management functions carried out on all active reports in the month preceding the control reference date and relating to any product linked to the queried report";

3. the bank has been conducting "for years an intense, growing education activity for its employees (especially if they are network employees) to increase their awareness - beyond the verification of alerts in the event of anomalous or risky queries - on the issues of the protection of customers' personal data ".

With a subsequent note dated 05/25/2021, Intesa Sanpaolo, in response to a specific request for clarification formulated by the Office on 05/20/2021, also specified that the employee in question "at the time of the events held the position of "credit officer" at the Credit Unit of the "Regional Directorate of Veneto, Friuli Venezia Giulia and Trentino Alto Adige, assigned to the Credit Management Office. The tasks entrusted to employees with this corporate qualification involve the "Granting and management of loans, mortgages and loans, investigations and credit risk assessments" as highlighted in the attachment extracted from the "Functional chart of the Regional Departments of the Banca dei Territori Division" ".

On 04/10/2021, following the request for additional supplementary elements made by the Office on 17/9/2021, ISP provided a copy of the access logs to the complainant's data "relating to the period between July 2019 and December 2020 ", specifying that in the same" it does not appear that the "User serial number" (...) corresponding to the employee Mr. (...), has made queries on the personal data of Mrs. XX ".

2. The assessments of the Office and the initiation of the procedure.

The Office, therefore, on the basis of the documentation in the deeds and the elements acquired during the investigation, with communication dated 26/01/2022, notified Intesa Sanpaolo the act of initiation of the procedure, pursuant to art. 166, paragraph 5, of the Code, in relation to the violation of the "principles of integrity and confidentiality" and "security of treatment" pursuant to art. 5, par. 1, lett. f) and 32, par. 1, lett. b) and par. 2 of the Regulation, as well as the principle of "data protection from design" referred to in art. 25, par. 1 of the Regulations; as part of these principles, as they are compatible with the new regulatory framework (see Article 22, paragraph 4 of Legislative Decree No. 101/2018), the specific provisions referred to in point 4.3.1 of the provision of the Guarantor n. 192 of 12 May 2011 "on the circulation of information in the banking sector and tracking of banking transactions" (web doc. No. 1813953) concerning the activation, by banking institutions, of specific alerts aimed at detecting intrusions or anomalous accesses and abusive to information systems; the activation of these alerts, already prescribed as a necessary measure pursuant to art. 154, paragraph 1, lett. c), of the previous Code regarding the protection of personal data, must in fact be considered - at present - a measure that a data controller is required to adopt in implementation of the aforementioned principles of "integrity and confidentiality" and "security of treatment "As well as" data

protection from design "referred to in Articles. 5, par. 1, lett. f), 32, par. 1, lett. b) and 25, par. 1 of the Regulation. The alleged violation of Articles 33 and 34 of the Regulation.

On 25/02/2022 ISP sent its defense writings, pursuant to art. 18 of the law n. 689/1981, with which, in formulating a request for a hearing, he requested the dismissal of the proceedings or, in the alternative, the issuance of a warning (with relative obscuration of the name Intesa Sanpaolo S.p.a. "in order to avoid reputational prejudices") based on the considerations below:

a) "ISP has always been committed to promoting the greatest possible awareness of all its collaborators with reference to the general issue of the processing and protection of customers' personal data". In particular, "(...), in addition to the vast" mandatory "training catalog provided to employees, periodically, on the intranet pages with the highest viewing frequency and on three different communication channels, specific messages are published which recall the provisions of the provision of the Privacy Guarantor n. 192 of 12 May 2011 ("Requirements regarding the circulation of information in the banking sector and the tracking of banking transactions"), reiterating the absolute need to query personal data, including those of an accounting nature, only and solely for purposes related to 'work (attached to this, for prompt evidence, the example of the two most recent messages dating back to 03.02.2022 and 17.12.2021) ";

b) "the extent and gravity of the alleged violation is extremely limited", considering that:

"The queries made by the employee identified concerned the relationships attributable to Ms XX (in addition to two other subjects connected to the same) and were carried out in 5 days (18, 21, 25, 26 September 2018 and 29 October 2018)" ;

from what "reported by the same employee during the interviews with the competent Human Resources structures, at the time of the disputed questions the employee had been authorized to do so by Mrs. XX, his partner, given that they had decided to undertake a real estate project which involved the purchase of land and the subsequent construction of a housing unit. According to the employee concerned, he had already invested significant sums in that real estate project. Only later did the relationship deteriorate and a mutual dispute was opened ";

“At the time of the events, there were already specific alerts subject to further refinement. Even in the face, in any case, of the extension of the perimeter of personnel included in the survey, as implemented in the most recent releases, in light of the specific operations characteristic of professional figures ("credit officer") such as that covered by the identified employee, it would not be it was possible to intercept the queries carried out, as they are not representative of a potential anomalous behavior in particular for that specific professional figure ";

in the present case, moreover, "it was data acquired by the employee of ISP who," at the time of the facts was the complainant's partner, authorized by the same to consult his bank details ";

“The competent Audit and Human Resources structures promptly took action also and only on the basis of an initial verbal report by the interested party. The checks and management interventions put in place made it possible to terminate the conduct of the employee identified, who was also sanctioned from a disciplinary point of view ";

c) the questions put in place by the employee “represent access to applications that are completely usual for the professional figure such as that covered by the employee involved […]. The function performed by the employee in question was in fact that of assessing creditworthiness, and to perform this function it is necessary to have much more information than is necessary for a banking function of another type. It therefore made it impossible for a banking institution that manages millions of accesses to identify an anomaly in the accesses in question, or in any case to intervene before reporting the person concerned. These considerations allow us to believe that the conduct of Intesa Sanpaolo S.p.A. is exempt from the fault, and even more so from the willful misconduct, which constitute the subjective conditions of the sanctions envisaged in this matter, having to ascribe all responsibility exclusively to the conduct of the employee, already sanctioned disciplinarily ";

d) with reference to the alleged violation of articles 33 and 34 of the Regulations, the institute underlined that "in the case in question, at the time when it became aware of Ms. XX's grievances, no risk emerged [for the rights and freedoms of the interested parties], both because the accesses had taken place when the employee was authorized by Ms XX, and because the alleged violation had now ceased from the immediate adoption of the measures described here (see following points 5) and 6)) by the owner of the treatment ". Therefore, Intesa Sanpaolo S.p.A., based on the assessments set out below, carried out immediately, did not deem it necessary to notify the Guarantor Authority pursuant to Article 33 of the Regulation, despite having carried out, internally, and in oral form, the assessment presupposed by the aforementioned article 33 ". This is because:

- "with the intervention of the relevant Audit functions, the Bank promptly took action in order to verify the effective basis of the requests of Ms. XX, linked, by her own admission, by a sentimental relationship with the employee, by the itself authorized to access its banking information;

- the information in the possession of the Bank and provided by the employee concerned with an express signed declaration, attested that Ms XX - at the time of the facts - was aware of the operations of the then partner and had authorized it;

- the subsequent and consequent verification and investigation carried out, also carried out with the direct involvement of the employee concerned and the adoption of an adequate disciplinary measure pursuant to art. 7 of Law no. 300/1970, as can be seen from further log checks relating to periods subsequent to the one identified (from 18.09.2018 to 29.10.2018), have demonstrated the effectiveness of the corrective measures implemented, given that no further queries have been detected on the reports of Ms XX by the employee in question, sanctioning the definitive interruption of the reported anomalous behavior ";

e) as regards the technical and organizational measures implemented pursuant to articles 25 and 32 of the Regulation and, in particular, "the implementation of suitable alerts aimed at identifying anomalous or risky behaviors relating to the inquiry operations carried out by the Personnel" , the bank stated that, "in addition to what was already indicated in our communication of 30 March 2021, starting from the survey of January 2022, a further enhancement of these detection systems was released (called" alert ALL ") able to intercept, on a monthly basis, consultations with high quantities and concentrated on a Customer, capturing all the queries made on each application (which traces access to bank data) available to those authorized to process the Bank's data (therefore, with involvement of the personnel of the commercial network, of the Online Branch, of the Remote Branch, of the financial consultants and of the Central Management exception of personnel referring to control structures, eg. Audit).

The logic of the checks carried out by the new alert system makes it possible to highlight all the Queries carried out by the Bank's Personnel, on the basis of the Employee ID key / Customer Identification Code which simultaneously respond to all the following conditions:

are carried out on any report of the Customer Identification Code queried (active, closed or expired);

are related to any application that contains personal banking data and therefore subject to log;

are carried out in large quantities within a calendar month and concentrated on the Customer Identification Code prevailing with respect to all the Customer Identification Codes queried, during the month, by the Employee ".

Therefore, "taking into account the set of queries made by the Bank's staff, certainly relevant but necessary for the performance of normal operating activities, the controls described above consequently aim at identifying as" anomalous behavior "that carried out by the employee who , in the reference period (calendar month), not only carries out an apparently large number of queries but also puts in place other anomalous behavioral evidence, or concentrates these queries (with respect to all those carried out in the reference period) on a specific Customer. This implementation, it seems to us to be able

to affirm, covers the weaknesses that this esteemed Authority has detected with reference to the alerts described in our previous communication (which did not concern, in fact, all the subjects authorized to process by the Bank) ";

f) at the time of the facts, the employee in question performed the duties of "credit clerk"; in this regard, ISP underlined that the same observance of the "Supervisory provisions for banks" (referred to in Bank of Italy Circular No. 285/2013 and subsequent updates and additions) entails, "for the professionals more directly involved (such as that of "credit officer"), a large number of queries, even concentrated on the same customer, resulting in greater difficulty (or impossibility) of intercepting, despite the constant updating of alert systems, potentially anomalous behaviors that are not aligned with precise internal provisions given to the Bank's staff ". On the other hand, "in line with the provisions of the Supervisory Authority" indeed cited, "the specific company legislation also provides, for the professional figures most involved in the loan disbursement process, a set of activities that cannot be carried out without necessarily carrying out, through the use of various applications, a significant number of accesses to data and / or information referring to the counterpart under analysis. […]. In relation to the above considerations, it should be further noted that the regulatory provisions on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, consecrated in Legislative Decree 231 of 21 November 2007, obliges the 'financial intermediary to set up adequate verification and monitoring systems for suspicious transactions, such as to inevitably require control of the operations of its customers […]. In light of the above, by way of example only, considering: - the survey of the data base used for the log collection only for the month of December 2021 […]; - referring to customers (excluding legal entities) of the Friuli Venezia-Giulia and Veneto regions, representing, therefore, a socio-economic fabric compatible with the customers managed by our employee at the time, the following is highlighted:

- 82 employees "credit officers", as technical support in the analysis / management of credit lines relating to customers of the regions specified above, have carried out, through the use of any application that contains personal bank data subject to log, at least one querying of data / information referring to a single customer;

- the 82 credit workers identified carried out, in the reference period, an average of 3,045 queries per worker;

- in the reference period, the 82 credit workers identified above interrogated personal bank data of an average - by default - of 130 customers;

- with respect to the perimeter of 82 credit workers identified, in December 2021, more than 60% of these had a "behavior" similar to that carried out by the employee identified with reference to the relationships of Ms. XX. In fact, these employees

carried out queries on a single customer in a week in a number equal to or greater than the case currently analyzed ".

From this, according to the Bank, it follows that, "despite the implementation described above, it allows, therefore, to further refine the control systems capable of detecting potentially anomalous behavior, demonstrating the continuous effort made by Intesa Sanpaolo S.p.A. on the subject, it is important to highlight in total transparency that, in consideration of the intrinsic characteristics, as better represented above, of the "normal" daily operations of some professional figures

- such as that of "credit officer", the specific queries made in the case under analysis, could not, in any case, have been intercepted and detected, given that a significant percentage of operators belonging to this professional category usually carry out a higher number of queries with the use of multiple applications "; it is also reiterated that - as shown by the numerical examples above - "in the absence of additional criteria with respect to the mere absolute value of the inquiries made by an employee against a customer, there would be a risk of highlighting as potentially" anomalous "a volume of queries so large enough not to be concretely analyzed and above all, relating to the collection of data / information that is absolutely justified, necessary and legitimate for the correct performance of the duties of the Bank's Employees, with particular and specific reference to some professional figures, also taking into account the forecasts regulations and supervision relating to these activities ".

Finally, in the same memorandum, the credit institute underlined how, "confirming the commitment made by Intesa Sanpaolo S.p.A., also on the IT front, aimed at increasing the signals of attention in the presence of behavior by its collaborators, potentially not in line with the provisions of the Guarantor and / or with the applicable internal regulations, also in light of the findings and penalties imposed with the provision adopted on May 27, 2021, reg. n. 270 (referring, however, to each other that took place in a time period subsequent to that of interest for the matter in question), we note the launch of a further alert (called "NC999") referring to the operations carried out by the Personnel of traditional branches, online branch and remote branch in order to identify potential anomalous behaviors relating to accesses made, through a specific application, to data and information present on current accounts and savings deposits. Controls on this type of access to personal data make it possible to identify potential suspicious behaviors in the case of consultations, justified in themselves in the context of normal company activities but quantitatively relevant, repeated over time and concentrated on some customers ".

On 22/03/2022 the hearing requested by Intesa Sanpaolo S.p.a. was held pursuant to art. 166, paragraph 6, of the Code.

During the same, the credit institution, in reporting in full to what has already been stated in the defense writings, illustrated the

functions performed by the credit officers also with the aid of an explanatory document attached to the hearing report.

In particular, it was further highlighted that "credit officers, due to their specific skills, are required to view a very wide range of information that is difficult to predetermine" and that "the number of queries carried out in the case examined here is only "Apparently disproportionate" as the system is constructed in such a way that a single query implies the registration of dozens of accesses (for example, the simple scrolling of a page results as an access) ".

This is a “role characterized by a high degree of transversality, which necessarily involves consultation of customer information repeated over time and which takes the form of queries made on over thirty procedures (Central risks, Eurisk, chamber of commerce, mople, etc.). ) [...] so much so that, taking as a reference the month of December 2021, the 82 credit officers currently operating in the Veneto and Friuli Venezia Giulia regions each carried out about 3000 consultations and 60% of the same behaved similar to the case object of the complaints of the complainant ".

The Bank therefore reiterated that it had in any case carried out, over time, various implementations of the alert systems referred to in the provision of the Guarantor no. 192/2011 and that recently, following the provision with which the Authority decided a case similar to the one analyzed here and referring to events subsequent to those now under examination, a new efficient mechanism called "Catch all" was introduced which however, he would not have been able to intercept the present case precisely because of the duty and ordinariness of the inquiries made.

Finally, during the hearing, the Bank specified that the assessment pursuant to art. 33, par. 1 of the Regulation, or the one relating to the probability that the violation and personal data present a risk for the rights and freedoms of individuals, was carried out only informally and that no documentation of the violation of personal data was provided as required by 'art. 33, par. 5.

In this regard, it was reported that an electronic tool for assessing the severity of data breaches was recently implemented, which also involves tracking the assessments made.

3. The outcome of the investigation.

Upon examination of the declarations made by the data controller during the procedure (whose veracity the author is responsible for pursuant to and for the purposes of art.168 of the Code), as well as the documentation acquired in the proceedings, this Authority formulates the following considerations.

It is established that, in the case in question, Intesa Sanpaolo S.p.a. - prior to the submission of the complaint to this Authority

and following the request made by the interested party to prevent a specific employee from accessing any information relating to their banking relationships - following the outcome of checks carried out by the Internal Control Function, he had ascertained the incorrect processing of the complainant's personal data by the employee in question; in fact, in the period between 18 September 2018 and 29 October 2018, using the IT qualifications necessary for the performance of his duties, he had accessed the complainant's bank details in the absence of professional reasons; for this reason, the employee himself was subjected to disciplinary proceedings and "during 2019" and a penalty was applied to him, pursuant to art. 7 of the law n. 300/1970.

From the technical analysis of the documentation acquired in the proceedings (alerts activated and log of accesses performed by the employee), it also emerged that:

a) at the time of the facts covered by the complaint, the alerts activated by the credit institution operated exclusively on some specific types of operations, or on the query operations carried out by a particular category of persons authorized to process. In particular, the alerts described above (see par. 1, point 2), b)) were aimed at detecting only the anomalous or risky behaviors assumed by the operators of the online branch, while those referred to in par. 1, point 2), lett. c) exclusively concern the anomalous or risky behaviors assumed by the operators of the online or traditional branch;

b) in the week of 18 September 2018, the employee made numerous accesses to the complainant's bank data (34 accesses), some of which related to transactions dating back in time (2004 and 2017) and, presumably, not available online and therefore accessible through tools document archiving; there are also two accesses to the risk center that should not have generated an alert, only in the presence of the conditions indicated by the Institute;

c) the aforementioned accesses, although numerous, compared to a short time span and also relating to existing transactions, did not generate any alerts; this happened for the reasons represented in lett. to); in particular, the Bank had prepared the detection of anomalous behaviors exclusively towards the staff working at the online branch or, in the case of consultation of the document archiving tools, only the staff working at the online and traditional branch, although, obviously , numerous corporate functions can access, for the performance of their work, the personal and banking data of customers.

From the foregoing it is therefore clear that, at the time of the facts covered by this complaint, ISP had not adequately implemented alerts suitable for detecting, in a complete manner, anomalous or risky behaviors relating to the inquiry operations carried out by personnel who, for various reasons, can access the personal data of customers.

Failure to adopt these alerts, prescribed by the aforementioned provision no. 192 of 12 May 2011 (see point 4.3.1 and point 1), lett. d), point i) of the device) configures, as stated above (see par. 2), a violation of the "principle of integrity and confidentiality" and of the "security of processing" pursuant to art. 5, par. 1, lett. f) and 32, par. 1 and 2 of the Regulation, as well as the principle of "data protection from design" pursuant to art. 25, par. 1 of the Regulation.

In this regard, it is noted that the aforementioned violations have already been assessed, also from a sanctioning point of view, by this Authority which, with reference to a similar case concerning events that occurred at a later time than those examined here, during the year of the powers referred to in art. 58, par. 2 of the Regulation, has in fact adopted a corrective and sanctioning measure against Intesa Sanpaolo S.p.a. (see provision no. 270 of 05/27/2021 web doc 9718112).

From this point of view, therefore, while reconfirming the negative assessment of the Authority with respect to the measures adopted by the Bank at the time, it is not considered necessary to exercise the corrective powers provided for by art. 58, given that ISP has acknowledged, with a note dated 11/12/2021 - and subsequent integration - as well as in the context of the defensive writings sent in relation to this proceeding, that it has adequately implemented the alert system.

With reference instead to the alleged violation of articles 33 and 34 of the Regulation, it is ascertained that the Bank, when it learned that the employee in question had made unlawful access to the complainant's accounting positions (upon notification by the latter), initiated the checks and implemented management interventions such as to determine the interruption of the unlawful conduct of the employee who, moreover, was sanctioned from a disciplinary point of view. In this context, it did not consider making a communication to the interested party of the ascertained violation pursuant to art. 34 of the Regulations, as the same was already aware of the violation so much so that it requested the credit institution to inhibit the employee from accessing his accounting positions.

In this regard, it should be noted that art. 33, par. 1 of the Regulation leaves to the data controller the assessment of the probability that the violation of personal data presents a risk for the rights and freedoms of individuals. In this regard, we agree with the assessment made by the Bank.

Even when, in relation to the specific case, the data controller deems not to proceed to notify the violation to the competent supervisory authority, the same is nevertheless required to document any violation of personal data, including the circumstances relating to it, his consequences and the measures adopted and to keep this documentation at the disposal of the competent authority in order to allow verification of compliance with the procedures, in compliance with the accountability

principle envisaged by art. 5, par. 2 and art. 24 of the Regulation.

In the present case, the investigations revealed instead that the Bank did not, as it is required, to document the violation of the personal data relating to the complainant in accordance with the provisions of art. 35, par. 5 of the Regulation.

4. Conclusions: illegality of the treatments carried out.

In the light of the foregoing assessments, it is noted that the statements made by the data controller in the defensive writings - for whose veracity one may be called to answer pursuant to the aforementioned art. 168 of the Code - do not allow the findings notified by the Office to be overcome with the act of initiating the procedure and are insufficient to allow archiving, however, none of the cases provided for by art. 11 of the regulation of the Guarantor n. 1/2019, concerning the internal procedures of the Authority having external relevance.

For the above reasons, therefore, the complaint submitted pursuant to art. 77 of the Regulation and, in the exercise of the corrective powers attributed to the Authority pursuant to art. 58, par. 2, of the Regulation, the application of a pecuniary administrative sanction pursuant to art. 83, par. 4 and 5, of the Regulation.

In fact, considering that the data controller, already responsible for a violation relating to the same type of treatment and recipient of the corrective and sanctioning provision of the Authority no. 270/2021 mentioned above, in the course of 2021 it complied with the order contained therein, implementing alert systems aimed at identifying anomalous or risky behaviors relating to the inquiry operations carried out by bank staff and making them aware of compliance with the instructions given to them , even further by strengthening the systems themselves in the first months of 2022, it is believed that the conditions for the adoption, in this regard, of further corrective measures pursuant to art. 58, par. 2, of the Regulation.

5. Order of injunction.

The Guarantor, pursuant to art. 58, par. 2, lett. i) of the Regulations and art. 166 of the Code, has the power to impose a pecuniary administrative sanction provided for by art. 83, par. 4 and 5, of the Regulation, through the adoption of an injunction order (art. 18. L. 24 November 1981 n. 689), in relation to the processing of personal data referring to the complainant, whose unlawfulness has been ascertained, in the terms set out above.

With reference to the elements listed in art. 83, par. 2, of the Regulations for the purposes of applying the pecuniary administrative sanction and its quantification, taking into account that the sanction must be "in each individual case effective, proportionate and dissuasive" (Article 83, par. 1 of the Regulations), 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 relevant, which concerned the general principles of lawfulness in the processing of personal data as well as the fact that the owner became aware of the violation only following the reporting of the interested party;

b) the Bank, as soon as it became aware of the violation, immediately proceeded to inhibit the employee's access to the complainant's accounting data but failed to document the violation in the manner indicated in art. 35, par. 5 of the Regulations;

c) the credit institution was recently the recipient of the corrective measure mentioned above in relation to the assessment, by the Authority and following a complaint presented by an interested party, of a similar violation by an employee (in case in point, as in the case already examined, it concerned subjects linked by a marital relationship or cohabitation with the complainant). The repetition of these violations highlights the need for a supplement for reflection, by the data controller, with respect to the adequacy of the procedures aimed at verifying the correct fulfillment of the instructions by the persons designated to process the data;

d) the fact that the credit institution actively cooperated with the Authority during the procedure, illustrating in detail the effectiveness of the alert systems adopted and, on the other hand, indicating the relative limits in consideration of the intrinsic characteristics of normal daily operations of some professional figures;

e) the circumstance that the personal data affected by the violation are bank data, therefore data of particular sensitivity even if not belonging to the so-called type of data. details 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 circumstance that the ascertained violation concerned a single customer was considered as an attenuating element.

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 were taken into consideration, determined based on the revenues achieved and referred to the financial statements for the year 2021.

On the basis of the aforementioned elements, evaluated as a whole, it is believed to determine the amount of the pecuniary sanction in the amount of € 100,000 (one hundred thousand) for the violation of Articles 5, par. 1, lett. f), 32, par. 1, lett. b), 25,

par. 1 and 33, par. 5 of the Regulation.

In this context, also in consideration of the type of violation ascertained, which concerned the principles of protection of personal data, 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, the unlawfulness of the processing carried out, in the terms set out in the motivation, for the violation of Articles 5, par. 1, lett. f), 32, par. 1, lett. b), 25, par. 1 and 33, par. 5 of the Regulation.

ORDER

to Intesa Sanpaolo S.p.a., with registered office in Turin, Corso England 3, P.I. 01111200505, pursuant to art. 58, par. 2, lett. i), of the Regulations, to pay the sum of 100,000 (one hundred thousand) euros as a pecuniary administrative sanction for the violations indicated in this provision;

INJUNCES

to the same Intesa Sanpaolo S.p.a. to pay the sum of € 100,000 (one 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 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.

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 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, July 28, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei