[doc. web n. 9809201]

Injunction order against Intesa Sanpaolo Vita S.p.a. - July 7, 2022

Record of measures

n. 244 of 7 July 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by Prof. Pasquale Stanzione, president, Prof. 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 presented by Mr. XX on 30/03/2021 pursuant to art. 77 of the Regulation, with which Intesa Sanpaolo Vita 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 30/3/2021, Mr. XX, represented and defended by the lawyer Armando XX, complained that Intesa Sanpaolo Vita S.p.a. (hereinafter, "ISP Vita" or "the Company") has put in place an unlawful communication of personal data concerning him, relating to a life policy signed with the aforementioned Company, to unauthorized third parties; in particular, the same represented that in response to the specific request for access made pursuant to art. 15 of the Regulations, ISP Vita, confirming what had already been communicated with a letter dated 19 January 2021, stated that "in the wrong settlement procedure, only the following personal data of his client were communicated to subjects outside the policy: name, surname, policy number and paid amount. The communication of these data, in the

absence of further identification data, such as for example tax code, address, date of birth etc., does not allow to uniquely identify your client, Mr. XX, and therefore we believe that there has been no violation of personal data".

Following the invitation formulated by this Office to provide observations regarding the facts covered by the complaint, with the note dated 7/9/2021, ISP Vita reiterated that it was an "operational error connected to a policy liquidation" (error which was promptly remedied) and that the communication of the personal data of the interested party to third parties, as limited to the data referring to the "name, surname, policy number and amount paid [...] in the absence of further identification elements, such as the tax code, address, date of birth, etc. " that make it possible to trace "the actual identity of the complainant, has been assimilated to an absence of violation"; this considering that "with respect to the name and surname, numerous homonyms have been found" and that "the policy number is a numerical code internal to the Holder, which does not allow the subjects who received the communication to trace the holder of the policy itself ".

With subsequent communications dated 19/10/2021 and 5/4/2021, the Company, in response to the notes with which the Office requested further information - also attaching useful supporting documentation - declared that:

a) the operational error consisted in the incorrect entry of the last digit of the policy number by the operator responsible for the settlement of the file. In particular, on March 3, 2020, the operator received "a claim report from the intermediary under policy no. [...] 78 "proceeded to" instruct the settlement process for the correct beneficiaries, searching in the registry for the policy number corresponding to the deceased insured. On this occasion, in the policy settlement process, the operator of the Company, instead of entering the policy number referring to Mr. [..... 78), entered the different policy number [...] 79 (different for the last digit but coinciding as a product), whose contracting party is the complainant, Mr. XX "; this was followed by "the automated sending of a" communication of payment for claim "to the beneficiaries, in which the name and surname of the insured, policy number and paid amount appear";

b) on 2 December 2020, following the grievances of the complainant who, through a manager of the Intesa Sanpaolo branch (policy placer) "complained about the incorrect liquidation of his policy, the Company became aware of the error and took action immediately to restore the position, which took place in the meantime on 4 December 2020 […]. In parallel, on 9 December the Customer Management office started the checks relating to the actual file to be settled (policy no. [...] 78) [...] ".

At that time, it emerged that, as part of the first erroneous settlement, the communications containing the complainant's personal data had been sent, "the Customer Management Office promptly initiated the process envisaged for the" reporting

and notification of data breaches ", opening a specific ticket on 10 December to track and analyze the event "(a copy of which has been attached). "In this circumstance, the DPO was promptly involved in order to assess a potential violation for the information communicated to third parties". As part of this assessment process, the Company considered that "the event did not constitute a significant violation from the point of view of the rules on the protection of personal data (in particular, Article 33 of EU Regulation 679/2016) taking into consideration the reasonable improbability for the recipients of the communication to uniquely identify, directly or indirectly, the data subject, and the fact that it was highly unlikely that what happened represented a risk (consisting, for example, in identity theft, or other) for the rights and freedoms of Mr. XX, thus excluding the onset of notification obligations to this Authority. In this regard, it was also considered that:

• together with the name and surname (XX, no further elements have been provided (eg: address, profession, etc.) that would allow the data subject to be distinguished from the mass of existing homonyms;

• the recipients are geographically enormously distant from the data subject, thereby also limiting the possibilities of face-to-face knowledge;

• incorrect communications have been sent to a low number of clearly identified subjects (2), who have been appropriately informed through the intermediary about the incorrectness of the sending and the need to eliminate the communications received ".

Finally, in the opinion of the Company, "while wanting to consider the event as a violation of personal data pursuant to the GDPR, it did not present elements of such gravity as to lead to the onset of an obligation to report to the Guarantor Authority for the protection of Personal Data and / or to the interested parties (even if on closer inspection Mr. XX had been made aware of the matter) […]. The above reconstruction also seems to find comfort in the recent "Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, adopted on 14 December 2021" of the EDPB, and in particular in examples nos. 13 and 15 of the Guidelines for which the EDPB itself, in the face of communications of personal data to unauthorized but in any case identified third parties, deriving from isolated and unsystematic human errors, suggests an assessment of "low risk" for rights and the freedoms of the interested parties, for which notification to the supervisory authority is not necessary ";

c) "at the time of the facts, together with the" Technical and organizational measures adopted for the IT tools "used for the settlement of the file [document attached], the Company has adopted organizational safeguards, or line controls and second level, as described in the internal regulations governing the settlement process ("Settlement management") ", a copy of which

is also attached; "These measures have ensured that the case in question falls within a case of 0.001% incidence against approximately 73,000 annual payments", where the operator "failed to verify the personal data summarized in the settlement screen" (or to verify "the consistency between the name of the insured, the policy number and the beneficiaries").

Together with the measures already mentioned, “the Company launched a further project during the first quarter of 2021 aimed at revisiting the settlement process and further strengthening the control measures for the correct management of policies. In particular, it is planned to automate part of the compilation of the settlement steps with the acquisition of supporting data and documents, directly from the intermediary himself, if any. This project, which also involves the parent company Intesa Sanpaolo, will be completed within the first half of 2022 ”.

The Office, therefore, on the basis of the documentation in the deeds and the elements acquired during the investigation, with communication dated 5/5/2022, notified ISP Vita of the act of initiation of the sanctioning procedure, pursuant to art. 166, paragraph 5, of the Code, in relation to the violation of the general principles of "lawfulness, correctness and transparency" and "integrity and confidentiality", pursuant to art. 5, par. 1, lett. a) and f) of the Regulations.

On May 31, 2022, ISP Vita sent its defense writings pursuant to art. 18 of the law n. 689/1981, with which, in reiterating in full what has already been highlighted in the previous communications "with regard to the genesis and the concrete development of the event under consideration, as well as to what is put in place by the Company in relations with the interested party and for the to remedy the effects of the event itself ", further highlighted that:

a) "the event occurred following a fortuitous error committed by an employee authorized to process personal data and adequately trained in relation to the same, whose work culpably deviated from the internal protocols governing the process defined by the Company, as reported in the documents attached to the feedback provided previously. In particular, reference is made here to the specific operating guide which also governs the organizational measures aimed at overseeing the claims settlement process "(see Annex 3 to the feedback of 19 October 2021) . "In addition, in terms of training, all staff undergo a compulsory specialist training course (see Annex no. 1," summary of compulsory training courses "), on the basis of the activity carried out, which involves passing various online training modules, which are followed by a test to verify the skills acquired. Finally, coaching, training on the jo b and support, even remotely, between employees and direct coordinators and / or managers. In addition, the Data Controller formalizes the task of processing personal data, including special data, to all employees. In fact, during the hiring phase of each employee, a document kit is provided which includes, among other things,

the appointment of a person in charge of data processing (subject authorized pursuant to art. 29 of the GDPR), as well as a copy of the "Internal Code of conduct of Group ", which also refers to the main provisions on privacy (see attachments no. 2" Appointment of data processor "and attachment no. 3" extract of the Group's internal code of conduct "). This documentation can be consulted at any time by the employee within a specific section of the company intranet ";

b) the event in question "took place as part of the settlement process of life policies with respect to which the beneficiaries of the insurance benefit, as required by the relevant legislation, can also be designated in generic form as" testamentary heirs or failing legitimate heirs of the insured party ", without indicating their names. In these cases (in which the event that concerns us and the policies involved - the one referring to Mr. XX and the one that had to be effectively liquidated) falls, the specific identification of the beneficiaries themselves takes place during the claim phase (i.e. death of the insured party), following the communication that the Company receives in relation to the identity of the heirs of the deceased. This peculiarity of the policies in question does not allow the definition of an entirely automated process on the basis of which, starting from a specific policy number, the settlement in favor of the beneficiaries of the same can be automatically linked.

For these reasons, in all cases in which the beneficiaries are generically identified as "testamentary heirs or in the absence of legitimate heirs of the insured", the association with the policy of the beneficiaries themselves, necessarily takes place through an organizational process that involves intervention of the operator following the opening of the claim. And it is precisely in this phase of liquidation of the policy that, as mentioned, the clerk, departing from company practices and the instructions received, entered a last wrong figure and subsequently did not precisely check the summary of the case being liquidated. This entailed, as far as is of interest here, the automatic sending of a communication confirming the settlement with some data of the interested party (name, surname, policy number and amount of the amount to be settled) to the two beneficiaries. of another similar policy (which had reported the claim). Specifically, as already mentioned, it was an isolated and occasional case (the first case involving over 73,000 liquidations per year) ";

c) the Company, "once made aware of the inconvenience that occurred following the reporting of the interested party, proceeded to promptly restore the insurance position of the interested party (2 days after his notification) and to inform the latter of the erroneous communication of some of your personal data to the aforementioned beneficiaries. In addition, the intermediary (the branch of Intesa Sanpaolo S.p.A. which had handled the distribution activity), proceeded to contact the beneficiaries themselves, with an invitation not to take into account and delete the communications received by mistake.

Furthermore, as already highlighted in the previous findings, with respect to the framework of procedures and measures already in place (referred to in the documents in force), specific activities were launched for the adoption of further technical security measures. - additional organization to those planned at the time of the event, with particular regard to the increase in training activities in favor of personnel ". In particular, "it was envisaged, where compatible with the insurance products managed, to automate part of the compilation of the settlement steps with the acquisition of data and supporting documentation directly from the intermediary. This innovation actually translates into a process subject to "doublecheck", in which the preliminary investigation carried out manually by the intermediary is automated, leaving the final verification and settlement phase to a third party, appointed by the Company " .

d) for the reasons described above "it is believed that, in the present case, the configuration of a potential non-compliance with the principles of lawfulness / correctness or integrity / confidentiality by the Company, as data controller, can be traced back to a so-called "Minor violation" pursuant to Recital 148 of the GDPR. This in consideration of the fact that it is a circumscribed and entirely occasional episode due to a human error that is difficult to predict (which occurred, among other things, in the particular and stressful emergency period due to the Covid-19 epidemic that affected the situation organizational and working conditions of employees), and which did not entail any consequences of an economic nature for the interested party (since his position was promptly and fully restored), nor in terms of any dangers of identity theft or other financial or social damage significant. All this also in the light of what has been demonstrated by tabulas in order to respect the Company's compliance with the aforementioned principles, since it is an isolated case compared to the high volume of liquidations managed. They also note the organizational, technical and security measures already adopted by the Company and the additional ones recently introduced also following the incident, in order to further reduce the risk (unfortunately unavoidable) of the occurrence of accidental human errors such as the one mentioned above. to the present case ";

e) finally "in the unlikely event that the Authority intended to proceed with the adoption of a sanctioning measure against the Company, in the present case, in consideration of the particular intrinsic characteristics of the event, as well as the fact that it is a isolated case, not significant and rather dating back over time, it is believed that the conditions for the application of the accessory administrative sanction of the publication of the order-injunction on the Authority's website provided for by art. 166, paragraph 7, of the Privacy Code ".

2. The outcome of the investigation.

Upon examination of the documentation produced and the declarations made by the party during the proceedings, provided that, unless the fact constitutes a more serious crime, anyone, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces false deeds or documents and is liable pursuant to art. 168 of the Code, it emerged that the Company, on the occasion of the liquidation of an insurance policy other than the one referring to the complainant, communicated to two third parties (beneficiaries of the policy being liquidated) personal data referring to the interested party, holder of another policy ; this occurred due to a material error put in place by the operator responsible for the settlement of the file, of which the Company became aware months after the incident and only following the report made by the interested party (whose policy was been liquidated in the absence of conditions).

The processing of personal data carried out by the Company is therefore illegal since - taking into account the methods and circumstances in which the event took place - it was carried out in a manner that does not comply with the principles of "lawfulness, correctness and transparency" and "Integrity and confidentiality", in violation of art. 5, par. 1, lett. a) and f) of the Regulations.

3. Conclusions: illegality of the treatments carried out.

In light of the foregoing assessments, it is noted that the statements made by the data controller in the defense briefs, although worthy of consideration and whose truthfulness may be called upon to respond 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. 5, of the Regulation.

4. 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. 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, within the terms shown 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 culpable nature of the event, due to the error of an employee who operated by deviating from the instructions given by the data controller regarding the completeness and consistency checks that must be carried out before proceeding with the settlement of the policies;

c) the Company immediately proceeded, as soon as it became aware of the event, to restore the insurance position of the interested party and to contact third parties, inviting them to delete the communications received;

d) even before the event, the Company had adopted internal regulations concerning specific controls on the policy settlement processes. It should also be positively acknowledged that, after the same, the Company proceeded to further implement the technical-organizational measures and to increase the training activity of the staff, significantly decreasing the possibility of the repetition of similar episodes;

e) actively cooperated with the Authority during the procedure;

f) there are no previous violations committed by Intesa Sanpaolo Vita S.p.a. or previous provisions pursuant to art. 58 of the Regulation;

g) the personal data affected by the violation are common data.

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.

Due to the aforementioned elements, assessed as a whole, it is believed to determine the amount of the financial penalty in the amount of 20,000 (twenty thousand) euros for the violation of Articles 5, par. 1, lett. a) and f) of the Regulations.

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 Regulation, the unlawfulness of the processing carried out, in the terms set out in the motivation, for the violation of Articles 5, par. 1, lett. a) and f) of the Regulations;

ORDER

to Intesa Sanpaolo Vita 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 € 20,000 (twenty thousand) as a pecuniary administrative sanction for the violations indicated in this provision;

INJUNCES

to the same Intesa Sanpaolo Vita S.p.a. to pay the sum of € 20,000 (twenty 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 filing 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 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, July 7, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei