SEE ALSO NEWSLETTER OF 3 OCTOBER 2022

[doc. web n. 9809998]

Injunction order against Senseonics Inc. - July 7, 2022

Record of measures

n. 242 of 7 July 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stazione, 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, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46 / EC, "General Data Protection Regulation" (hereinafter the "Regulation");

GIVEN the Code regarding the protection of personal data (Legislative Decree 30 June 2003, n.196), as amended by Legislative Decree 10 August 2018, n. 101, containing provisions for the adaptation of national law to the aforementioned Regulation (hereinafter the "Code");

GIVEN the Regulation n. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved by resolution no. 98 of 4/4/2019, published in the Official Gazette n. 106 of 8/5/2019 and in www.gpdp.it, doc. web n. 9107633 (hereinafter "Regulation of the Guarantor no. 1/2019");

Having seen the documentation in the deeds;

Given the observations made by the secretary general pursuant to art. 15 of the Guarantor Regulation n. 1/2000 on the organization and operation of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web n. 1098801;

Speaker Dr. Agostino Ghiglia;

WHEREAS

1. The violation of personal data

On XX, the US company Senseonics Inc (hereinafter "Senseonics" or the "Company) notified a personal data breach, pursuant

to art. 33 of the Regulation.

The violation consisted in sending "In the context of an information campaign regarding the distribution in Italy of Eversense XL - a continuous glucose monitoring system for people with diabetes - an institutional email" to specific groups of Eversense XL customers by entering the email addresses of the recipients in the "cc" field instead of in the "bcc" field. Consequently, each recipient had the opportunity to view the e-mail addresses of the other recipients of the institutional e-mail ". The violation affected approximately 2000 Italian parties and was caused by an involuntary error on the part of an employee of the Company.

More specifically, it was represented that “The notified incident entails the possibility for unauthorized third parties to access the email addresses of people potentially interested in diabetes products, or the email addresses of their caretakers. These email addresses are in some cases made up of a combination of name and surname which thus makes it possible to identify the person in question, indirectly disclosing data relating to his health, i.e. a particular category of personal data pursuant to Art. 9 of the RGPD ".

It was also reported that the Company “adopts industry standard technical and organizational measures to guarantee data security and protection. In particular, the following measures are adopted: awareness and training, firewall, encryption, privacy policy, logical access control, network authentication, regular software updates, access logs and anti-malware systems ".

The violation was communicated to the interested parties involved by sending an apology email that contained: "[the] description of the violation; [i] contact details in case of questions or problems; [the] description of the possible consequences of the violation and the measures to remedy the violation [and] (…) to mitigate possible negative effects for the interested parties ". Through this communication, the recipients were also asked to cancel the email received with "clear" addresses.

Furthermore, to prevent similar future violations, the Company stated that "it is currently evaluating a complete review of the communication processes with users and will, where it deems necessary, reinforce the technical and organizational security measures useful to ensure that such violations do not happen in the future. Senseonics is also evaluating the possibility of implementing additional control and monitoring processes for communications with users, as well as setting up specialized systems and / or services capable of automating communication processes with users, after setting adequate parameters, in order to prevent human error as much as possible ".

2. The preliminary activity

With specific reference to the facts of the aforementioned violation, the Company with a note of the XX, provided a response to the request for information of the Office, of the XX (prot. No. XX) and, in addition to what has already been communicated, represented that:

- “We felt it was important that patients who were currently using Eversense (…) were informed of Ascenia's support role in order to (…) receive technical support and know who to contact to continue their Eversense therapy. (...) the email was clearly drafted without promotional purposes, but to indicate how to meet customer service needs ";

- "to have recently appointed the representative pursuant to art. 26 of the Regulations: EDPO based in Avenue Huart Hamoir, 71, 1030 Brussels, Belgium and that the privacy policy is being updated ";

- to have regularly provided its employees with guidelines and instructions on the protection of personal data, in particular to those who “manage and process patient data and who communicate directly with patients” (…). The training and guidelines were actually followed by the employee, but a simple human error caused the accident. We will continue to provide guidelines and instructions on a regular basis and with the additional measures and precautions we have taken for patient communications, we are confident this incident will be avoided in the future. "

With specific reference to the measures actually adopted in order to avoid the recurrence of the event that occurred, the Company has represented that:

- “Senseonics normally makes few, if any, direct communications to users (…).

For such occasional communications as a further precaution we will request (as we did with the corrective email) an email confirming that the practice of including addresses in the bcc field is carried out correctly ".

Furthermore, the Company, in response to the aforementioned request for information, also aimed at verifying the conditions of lawfulness of the treatments carried out and compliance with the principles of correctness and transparency and data integrity and confidentiality, has provided further elements on the functioning of the proprietary system. glucose monitoring through the Eversense XL mobile app. In this regard, the download process of the App has been described, which is "downloaded (on iPhone and Android smartphone), installed and used, but only after accepting the relevant legal conditions of Senseonics (the License Agreement with the User Finale (EULA) and the Privacy Policy and Terms of Use ("Privacy Policy"). ”The installation of the App takes place through the following steps:

"Step 1: Before downloading the App in the app store, the user is able to review the privacy policy within the app store (see

Annex 1). The Privacy Policy can also be viewed online on our Eversense website (see https://global.eversensediabetes.com/privacy-policy).

Step 2: Once downloaded, the user is prompted to turn on bluetooth (to connect with the Eversense Smart Transmitter), and to agree to receive alerts (allowing the user, for example, to be notified about their levels glucose).

Step 3: Before being able to create an account and use the App, the user is prompted to accept the EULA. The EULA again refers to the Privacy Policy and also summarizes the main elements of the Privacy Policy (Article 1.5 of the EULA).

Step 4: Once the user clicks on the accept button, a pop-up window appears covering the screen of the mobile device (see Annex 2), asking the user to explicitly authorize the storage, transfer and use of your personal data, including data retention in the United Kingdom and transfer to the United States for limited purposes (such as technical support for customers and to meet certain regulatory requirements), in accordance with the EULA and the privacy, and, therefore, to confirm again that you have adhered to the EULA and the Privacy Policy.

Step 5: Once the user has ticked the accept button, they are guided to the account creation section.

Step 6: The user has to complete a form by filling in his name, surname, e-mail address and he will also have to create a password. Before sending, the user must check a box to confirm that he has accepted the Terms and Conditions and confirm, by checking a specific box, that he is over 18 years old (...) ".

The Company then produced a table in documents which lists the different purposes of the treatments carried out through the use of the Eversense XL glucose monitoring system and the Eversense Mobile App, indicating the different legal bases listed below:

- for "the provision of a service / customer assistance" the legal bases of the processing are found in art. 6, par. 1, lett. b) of the Regulation and in the consent, in the case of data relating to health (Article 9, paragraph 2 letter a) of the Regulation);

- for "product improvement (developing and improving products and services; improving or modifying services", the legal bases have been identified in the legitimate interest of the owner (Article 6, paragraph 1, letter f) of the Regulation; in consent in the case of data relating to health (Article 9, paragraph 2, letter a) of the Regulation);

- for "marketing: data analysis, sending emails and notices to our customers regarding opportunities related to our products and services", the legal bases are represented by the "legitimate interest in direct marketing (Article 21.2. GDPR); opt-out of commercial emails addressed to subjects who are already customers, art. 13 E-privacy Directive) ".

With specific reference to the information provided to interested parties, pursuant to art. 13 of the Regulations, the Company has submitted a document called “Privacy Policy and conditions of use. Effective date: August 2016. Last modification: January 2021 ".

On the basis of the elements acquired, through the communication of the violation of personal data as well as in the context of the preliminary investigation, the Office, with deed of XX (prot.n.XX), notified on the same date by certified e-mail, which here must be understood as fully reproduced, has started, pursuant to art. 166, paragraph 5, of the Code, with reference to the specific situations of illegality referred to therein, a procedure for the adoption of the measures referred to in art. 58, par. 2 of the Regulation, against the Company by inviting it to produce defensive writings or documents to the Guarantor 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, l. No. 689 of the November 24, 1981).

With the aforementioned deed, the Office found that the Company, in relation to the violation of personal data, made a communication of data relating to health in the absence of a suitable legal basis and, therefore, in violation of the principles applicable to the processing of data. personal, as per art. 5, par. 1 letter a) and f) and 9 of the Regulations; with regard to the proprietary glucose monitoring system through the Eversense XL mobile application, the Company has also processed personal data in violation of the principles of lawfulness, correctness and transparency and limitation of the purpose referred to in Articles 5, par. 1 letter a) and b), 6, 7, 9, 12, 13 and 15 of the Regulations and in violation of art. 27 of the Regulation as the appointment of the representative by a holder not established in the Union was made by the Company only following receipt of the Office's request for information, therefore after the start of the processing by the Company itself.

3. Defensive memories

With a note of the twentieth, Senseonics sent its defense briefs, without asking to be audited, also providing the elements referred to in art. 83, paragraph 2, of the Regulation, highlighting, in particular, the following.

3.1. The violation of personal data pursuant to art. 33 of the Regulation

The Company in relation to the violation of personal data, notified to the Guarantor, pursuant to art. 33 of the Regulations, in addition to what was represented during the preliminary investigation, stated that:

"The email in question did not [did] provide recipients with certain information about the health status of the other recipients for three reasons: 1. The email itself did not contain any personal health information, but was simply a communication relating to

at the service; 2. The recipients of the email were not necessarily patient, but could also have been their Assistants; 3. The e-mail addresses did not necessarily contain the full name of the recipients, so as to allow their identification ";

"The email was intended to provide them with information relating to the service (...). Therefore, the recipients of the emails were not only subjects who had downloaded the Eversense App in their own interest (eg. People with blood sugar disorders), but in some cases they could also be Assistants ";

"The content of the email was absolutely generic and identical for all recipients (...). The communication did not include any personalized content or specific and personal information relating to individual recipients ";

"Although the vast majority of e-mail addresses are believed to belong to users with diabetes, it is also reasonably believed that those with glycemic disorders were only a subset of all recipients mistakenly included in the CC field";

"That said, the email itself did not contain personal information relating to the health of the recipients, and, without the collection of further information, it was not possible for the recipients to know with certainty the state of health of anyone in particular of the other recipients" ;

"On the basis of the Deed of Contestation, there are no further elements to be able to argue that such additional information suitable for revealing the state of health of a subset of the recipients, has been acquired by any of the recipients";

"Following the communication pursuant to Article 34 of the GDPR, Senseonics received only a few comments and no claims for damages";

“In light of the above, it is not possible to agree with the conclusion of this respectable Authority that“ the Company has communicated data relating to the health of 2,000 patients to as many patients ”;

"The sending of the email to the recipients in CC was not intentional but a consequence of human error". The violation in fact concerned a limited number of emails sent to Italian customers and did not affect those sent to other European users;

"The incident occurred in February 2021, in the middle of the Covid-19 pandemic emergency (...) The employee who sent the email was working remotely. This circumstance may have contributed to the accidental error ";

“Senseonics has not ignored the principles of the GDPR. On the contrary, in full compliance with the accountability principle - pursuant to Article 5, paragraph 2, of the GDPR - (...) has implemented [specific] actions "such as in particular the communication of the violation to the interested parties pursuant to art . 34 of the Regulation and to the Guarantor pursuant to art. 33 of the Regulation;

"In light of the above, (...) Article 5, paragraph 1, lett. (a) and Article 9 of the GDPR are not [] relevant and [must] therefore not be applied ";

"With regard to the alleged violation of Article 5, paragraph 1, lett. (f), it is believed that the Authority should have referred to the provisions pursuant to Article 32 of the GDPR ("Security of Treatment") and not to the general principle referred to in Article 5, lett. (f). It is indisputable that Senseonics - before sending the e-mail in question - applied organizational measures, in accordance with the principle set out in Article 5, paragraph 1, lett. (f) (...). A possible dispute may at most relate exclusively to the adequacy of the measures implemented by Senseonics, pursuant to Article 32 of the GDPR, which must be considered as lex specialis "which, however, has not been the subject of dispute".

3.2. The further disputes

3.2.1 The features of the Eversense App

With specific reference to the further violations subject to dispute in the context of the proceedings initiated pursuant to art. 166, paragraph 5 of the Code, the Company, after having made some preliminary considerations with which it represented that Senseonics is an SME that at the end of 2021 had fewer than 90 employees and that provides innovative solutions to patients suffering from diabetes in 14 countries in the world, with less than 3,000 Italian users of the application, declared:

that it has put its best efforts to comply with the GDPR by trying in good faith to meet all the requirements set out in designing a global privacy program;

being compliance with the GDPR a dynamic process, to work to continuously try to improve the compliance program in the European Union over time;

that it was "significantly affected by the Covid-19 Pandemic, facing significant economic and organizational difficulties, which inevitably slowed down the review of global compliance programs";

to have "revised its privacy policy (...)", to have "carried out an engineering work aimed at adding pop-up screens with a clearer text to your product for the request for consent to the processing of health-related data (the which require approval by the BSI prior to implementation) "and have" taken further steps in order to strengthen its program ";

that the Eversense mobile application is a component of a "more complex system, the Eversense GCM System, which provides users with continuous glucose monitoring. This system includes a subcutaneous sensor, which is installed by a doctor, and a removable smart transmitter, which sends data to the Eversense App "(...), to be used in conjunction with a

Senseonics implantable medical device (...) that a customer can only be used under the supervision of a physician ";

that "In Italy, Eversense products can only be sold on medical prescription and can only be purchased from hospitals";

that "The download of the Eversense App is only the final step downstream of a longer process, with the assistance of a doctor and - during this process, which includes the implantation of a subcutaneous sensor - the user is informed the operation of the Eversense CGM System and the processing of health-related data via the mobile app ".

3.2.2 The principles applicable to the processing of personal data

In this regard, the Company stated that:

"The processing of common personal data of users relating to the Eversense App is not based on the consent of the interested parties. In fact - as already mentioned - the processing of the user's personal data is necessary for the provision of the service through the Eversense App and therefore the legal basis - for this category of personal data it is the execution of a contract, pursuant to 'Article 6.1, lett. (b) of the GDPR ";

"With regard to health data, it is clear that the processing of such data, in principle, is necessary for the glucose monitoring functionality via the Eversense App (...). This given that for the processing of particular categories of data the execution of a contract cannot be considered a valid legal basis (...) the Company has identified the consent of the interested parties as the legal basis, pursuant to Article 9.2, lett. (a) of the GDPR;

"The Authority's conclusion that the consent collected by Senseonics is not specific cannot be shared. In fact, the registration process includes a specific phase for the collection of the users' privacy consent ";

"The acceptance of the contractual conditions and, in particular, of the EULA (including the Privacy Policy and the Terms of Use) is provided by users by clicking on the" accept "button in Step 3";

"The authorization to process personal data, including health-related data, is provided by users in Phase 4 (...), which was created specifically to provide information and a clear request for consent for the purpose of collecting it after the 'acceptance referred to in Phase 3. The wording summarizes the contractual documents already accepted by the user, and therefore aims to highlight to the user that personal data will be processed ";

"The consent collected during Phase 4 specifically concerns the processing of users' personal data (and, in particular, health data), for the purpose of providing the glucose monitoring service", also in relation to what is represented in the information that would mention sensitive data in this regard;

Consequently, the user would not be forced to provide consent as "it goes without saying that, without the treatment of the user's glucose levels, the Eversense App, as a component of the Eversense Continuous Glucose Monitoring System, would be completely useless";

Art. 7, par. 4 of the GDPR would not apply "as relevant only where the requested data are not necessary for the execution of the contract (including for the provision of a service) and the execution of the contract is subject to obtaining such data on the basis on the assumption of consent. On the contrary, if the processing is necessary to perform the contract (including for the provision of a service), Article 7, paragraph 4, does not apply "(see par. 32, page 11 of the EDPB Guidelines on Consent);

“In consideration of these elements, the conclusion that the consent provided by users is to be considered invalid and that the consequent processing of data is illegitimate cannot be shared. In this regard, we invite you to note that as part of the ongoing process, aimed at improving the level of maturity by Senseonics in the approach to the GDPR, this formulation is being updated ".

the new formulation of consent in which the following formulation is shown to the interested party "After reading the privacy policy, by clicking on the" Accept "button, I give my consent to the processing of my health data for Senseonics to use them to offer and manage the Senseonics Products and Services ", will be submitted for" BSI approval in February 2022 "and" the approval and subsequent release of this version of the app software in the spring of 2022 "is expected;

Finally, with regard to all the other purposes of the processing, the Privacy Policy clarifies that "During the registration or registration procedure or following it, if you are asked to provide further consent to authorize the use of certain categories data, Senseonics will contact you directly to obtain such consent, if it is deemed necessary under the laws applicable in your country or region regarding data protection "(see the paragraph" Enrollment / registration in Senseonics Products and Services ");

In conclusion, Senseonics' conduct did not violate the following provisions: Article 5, paragraphs 1, lett. (a), 6, 7 and 9 of the GDPR.

3.2.3 The privacy policy for the processing of personal data

In relation to disputes concerning the information provided by Senseonics to its customers pursuant to art. 13 of the Regulations, the latter stated that:

"Provides users with comprehensive information on the essential elements mentioned in Article 13 of the GDPR in order to make users aware of the data processing in question. In particular, the Privacy Policy is totally clear in explaining to users that

the treatment related to the Eversense App includes health data ";

they "must be considered completely aligned with the expectations of the users of a medical device and a mobile application whose purpose is specifically to monitor the glucose level";

the "download of the Eversense App is only the final phase of a long process, which begins with the comparison and consultation of a doctor (...) Therefore, the user is fully aware of the operation of the medical device and the related App .

"The legal bases of the processing, even if not specifically mentioned in relation to each of the purposes of the processing, can be easily deduced from the context: In all countries Senseonics has a legitimate interest in offering and using the Senseonics Products and services because you make advantageous use of it, using your data for this purpose and making relevant updates and notifications available to you. Furthermore (in particular for those countries subject to the provisions of the GDPR of the European Union), Senseonics will ask for your consent or authorization if it is necessary for a specific use of your data "(see the paragraph" Who controls your data ?) ";

"Considering that, as mentioned, the Company supplies its products in different countries globally, the data retention periods, in order to comply with the obligations established by law, may vary from country to country, and it was not possible mention in the Privacy Policy a specific data retention period, but only the applicable criteria, relating to contractual obligations and legal obligations; therefore, in line with Art. 13.2 of the GDPR. Therefore, the Privacy Policy mentions the criteria applied by the Company ";

"In relation to the right of access, such information is provided in two separate paragraphs of the Privacy Policy:" Your rights and responsibilities "where it is written" You can update your information and your account at any time by making the access to your account from our Site or mobile App and making the necessary changes ".; "Access to Information" which specifies that "If you decide to exercise your right to request consultation of a copy of the information collected and stored by Senseonics about you, we will do our best to provide it to you. With regard to European citizens, we will comply with the provisions of the European Union GDPR, which gives you the right to access the information we hold about you depending on the processing in question and in compliance with the specific limits set by the same legislation. If you wish to request access to information we hold about you in accordance with the provisions of the European Union GDPR, this may result in the payment of US $ 10 (USD) to cover the reasonable costs we incur in providing you with such information. To submit the aforementioned request, please contact dataprivacy@senseonics.com ".;

"As mentioned, the processing (...) is necessary for the management of the Eversense account. Consequently, the withdrawal of consent implies the deactivation of the user's account. For this reason, users are correctly informed that they can deactivate their account (and therefore withdraw their consent) and that the data relating to their account will subsequently be removed from the Senseonics Products and Services. (...) The withdrawal of consent without the deactivation of the account would not be possible ";

"The only missing piece of information is a specific reference to the right of data subjects to lodge a complaint with a Data Protection Supervisory Authority. This reference will be added to the Privacy Policy";

With regard to the other rights of the interested parties, such as cancellation, limitation and rectification, the Company has represented that in accordance with the Regulations they can be exercised only in the presence of specific conditions and of this the users would be informed where in the information it is specified that "Please note that we may not be able to fulfill all requests for modification, correction, deletion or limitation and that we may need to withhold certain information for registration purposes, for prudential or legal reasons and / or to complete all transactions initiated before the change request. In cases where Personal Information is deleted, it is possible that some residual information will still be kept in our databases and other records without being deleted ".

The Company has also sent, together with the defense briefs, a document called "Privacy Policy and conditions of use. Effective Date: August 2016; Last updated September 2021 "stating that:

"Following the letter of the XX of the Guarantor, has made a series of changes in its Privacy Policy";

this information "was recently updated on the Company's website (https://global.eversensediabetes.com/privacy-policy) and that it, together with the" new wording of the text of the consent request, should be implemented in the Eversense App with the release of an app update scheduled for February 2022 ".

3.2.4 The appointment of the representative established in the EU

Finally, in relation to the appointment of the representative established in the EU, pursuant to art. 27 of the Regulation, the Company represented that it was not "aware of the fact that the appointment of an" authorized representative "in the European Union pursuant to Article 14 (2) of Council Directive 93/42 / EEC [concerning medical devices] is not suitable to meet the requirements of the GDPR. Only after the request for information by this Authority, Senseonics has understood, after having discussed with its external consultants, that the appointment of this authorized representative cannot be sufficient from a

GDPR perspective and, therefore, has decided to specifically appoint a additional representative in the EU, pursuant to Article 27 of the GDPR ".

The Company therefore asked the Authority to evaluate its conduct as compliant with the Regulations or to "consider all the elements of the case and, in particular, the transparency of Senseonics - as demonstrated by the immediate notification of the personal data breach that occurred in February 2021 - and its efforts to respect the principles of the GDPR, considering the improvements that Senseonics has implemented, described below, and, therefore, to exclude the application of financial penalties or other administrative penalties ".

4. Outcome of the preliminary investigation

4.1 The violation of personal data pursuant to art. 33 of the Regulation

In relation to the violation of personal data, pursuant to art. 33 of the Regulation, as a preliminary point, it should be noted that "personal data" means "any information concerning an identified or identifiable natural person (" interested party "); the natural person who can be identified directly or indirectly is considered identifiable, with particular reference to an identifier such as the name (...) "and for" data relating to health "" personal data relating to the physical or mental health of a natural person, including the provision of health care, which reveal information relating to his state of health "(Article 4, paragraph 1, nos. 1 and 15 of the Regulation).

With particular reference to the question raised, it should be noted that personal data must be "processed lawfully, correctly and transparently" (principle of "lawfulness, correctness and transparency") and "in order to guarantee adequate security (...), including the protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage (principle of "integrity and confidentiality") "(Article 5, paragraph 1, letter a) and f) of the Regulation).

The regulation on the protection of personal data provides - in the health sector - that information on the state of health can only be communicated to the interested party and can be communicated to third parties only on the basis of a suitable legal basis or on the indication of the interested party. subject to written authorization from the latter (Article 9 of the Regulations and Article 83 of Legislative Decree No. 196 of 30 June 2003 (Code regarding the protection of personal data - hereinafter the "Code") in conjunction with 'Article 22, paragraph 11, legislative decree 10 August 2018, n.101; see also general provision of 9 November 2005, available at www.gpdt.it, web doc. n. 1191411, deemed compatible with the the aforementioned Regulation

and with the provisions of decree n.101 / 2018; see art.22, paragraph 4, of the aforementioned legislative decree n.101 / 2018).

Given the above, in light of the definition of personal data referred to above, the email addresses can be traced back to the notion of personal data (see Provisions of the Guarantor of 25 June 2002, web doc. N. 29864 and of 24 June 2003, doc. web no. 1132562). Therefore, even if part of the email addresses were devoid of references to the name of the recipients in full or in any case to other data directly identifying the data subjects, this is information of a personal nature, subject, like the others, to the application of the regulations on the matter. of protection of personal data.

Furthermore, with regard to the present case, the information subject to the notification, contained in the aforementioned email, even if it refers to a service communication, being addressed to users of the Eversense XL glucose monitoring system, constitutes personal data relating to health. In fact, this system is intended for people who want to actively manage their diabetes simply and safely, through an implantable sensor, a removable and rechargeable Smart Transmitter and a smartphone application (see provision 25 June 2002, web doc. 29864; provision of 9 January 2020, web doc. 9261234; provision of 13 May 2021, web doc. No. 9688020). The circumstance that not only patients but also their assistants (caretakers) may be present among the recipients does not determine a different qualification of such information as belonging to particular categories of data given that the content of the email unequivocally referred to the presence of a pathology diabetic and that the addresses of the recipients were those that the patients had provided precisely in relation to the aforementioned pathology. It should also be noted that the same Company in the notification of the violation qualified this information as relating to health.

In relation to the principle of integrity and confidentiality pursuant to art. 5, par. 1, lett. f) of the Regulation, it provides that personal data are processed "in such a way as to guarantee adequate security (...), including protection, by means of adequate technical and organizational measures, from unauthorized or illegal processing and from loss, destruction or from accidental damage ". The circumstance that in the act of contestation, the Office in addition to the reference made to art. 5, par. 1 letter f) of the Regulations should also have referred to the violation of art. 32 of the Regulation this because the Company - before sending the email in question - would have applied organizational measures, in accordance with the aforementioned principle and therefore the dispute should have exclusively concerned the adequacy of the measures implemented, it cannot be accepted. .

In fact, the aforementioned art. 5, par. 1, lett. f) of the Regulation requires data controllers to process data in such a way as to guarantee adequate security, including protection, by means of adequate technical and organizational measures. It therefore introduces a principle from which the obligation to process data arises in order to guarantee its integrity and confidentiality, the violation of which is punishable under art. 83, par. 5 of the Regulation. It is evident that in the present case the technical and organizational measures implemented were not adequate given that the violation of personal data subject to notification by the data controller has occurred (see par. 6.2 of Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021; provision of 13 May 2021, web document 9688020; provision of 16 September 2021, web document 9722297 and provision of 28 April 2022 no. 164, forthcoming). Moreover, the same Company, during the investigation, has provided for the adoption of further organizational measures precisely in order to avoid the repetition of events similar to the one that occurred

Therefore, the sending of communications by means of a single e-mail message addressed to a multiple number of recipients, whose addresses have been entered in the carbon copy field (cc), has, in fact, without justified reason and in the absence of a suitable assumption legal status, mutually revealed to the recipients of the communications, the state of health of the other patients entailing the processing of health data in violation of Articles 5, par. 1 letter a) and f) and 9 of the Regulations.

4.2. Further violations

4.2.1 Principles of lawfulness and limitation of the purpose of the processing of personal data (Article 5, paragraph 1, letter a) and b) of the Regulation)

In the first instance, the Office, in relation to the treatments carried out by the Company through the Eversense XL glucose monitoring system and the mobile application, contested the violation of art. 5, par. 1, lett. a) and b) of the Regulation, which provides for compliance with the principle of lawfulness, according to which any processing of personal data must be based on a specific legal assumption, and purpose limitation, for which data can be collected for specific purposes , explicit and legitimate and subsequently processed in a way that is not incompatible with these purposes.

In the event that the condition of lawfulness is represented by consent, it must be given through a positive act by which the interested party expresses a free, specific, informed and unambiguous will regarding the processing of personal data concerning him. If the processing is aimed at pursuing a plurality of purposes - as in the case in question - consent must be given for each of these purposes (Recitals 32, 42 and 43, articles 5, 6, par.1, letter a) and 7 of the Regulation and Guidelines

5/2020 on consent pursuant to Regulation (EU) 2016/679, adopted by the European Committee for the protection of personal data, on May 4, 2020; sent. C-673/17, of 1 October 2019 and C-61/19, of 11 November 2020).

With specific reference to the particular categories of data, including health data, art. 9 of the Regulation establishes a general prohibition on the processing of such data unless one of the specific exemptions to this prohibition applies, including the consent of the interested party. This consent, taking into account the nature of such data, which are particularly sensitive in terms of fundamental rights and freedoms, must also be explicit (Article 9, paragraph 2 letter a) of the Regulation and par. 4 of the Guidelines 5/2020 on consent pursuant to Regulation (EU) 2016/679, adopted by the European Committee for the protection of personal data on May 4, 2020).

In the present case, the documentation in the documents ascertains the violation of the principle of lawfulness of the processing, since at the time of the facts, on the occasion of the download of the application (see attachment 2 to the note of the Company, of XX), with a single "click" on the "accept" button, users were asked to accept both "the terms of the license agreement with the end user" and "the privacy policy and conditions of use of Senseonics, simultaneously authorizing the conservation, the transmission and use of data, including, without limitation, storage in the UK, transmission in the US for limited purposes (for example engineering and customer support) under the terms of the EULA and the privacy policy ".

Therefore, the fact that a single device has been requested by the interested party determines the failure to comply with the requirement of the specificity of consent for the different purposes pursued by the data controller, all the more so in relation to the processing of health data, with respect to which, consent must also be explicit (Article 9, paragraph 2, letter a) of the Regulation). On this point, the aforementioned Guidelines 5/2020 on consent clarify two relevant aspects in relation to the case in question. On the one hand, that "with" unequivocal positive action "means that the data subject must have taken a deliberate action to consent to the specific treatment" on the other hand, "The data controller must (...) pay attention to the fact that the consent cannot be obtained through the same action with which you accept a contract or the general conditions of service. The global acceptance of the general conditions of contract / service cannot be considered as an unequivocal positive action for the purpose of consenting to the use of personal data "(see points 77 and 83). Furthermore, taking into account that with regard to the processing of health data, the legal basis of the processing can only be found in one of the exceptions to the general prohibition of processing this category of data, listed in art. 9, par. 2 of the Regulation, the reference to art. 7, par. 4 of the Regulation and point 32 of the aforementioned Guidelines on consent which refer instead to the processing of data other than

those on health carried out for the execution of a contract including the provision of a service (Article 6, par. . b) of the Regulation).

With specific reference to the purposes of the processing, they are not clearly determined or explicit to the interested parties (see below). The purposes of the processing of personal data, in fact, in compliance with the principle of transparency, must be explicit and legitimate and specified at the time the personal data is collected. In the case in question, they were clearly represented by the Company only in the acknowledgment note to the aforementioned request for information.

4.2.2 The principle of transparency and the information to be provided to the interested parties (articles 5, paragraph 1, letter a), 12 and 13 of the Regulation)

Personal data must be processed in compliance with the principle of transparency (Article 5, paragraph 1 letter a) of the Regulations) providing the data subjects in advance with the information referred to in art. 13 of the Regulation, in the case of data collected directly from them, or pursuant to art. 14, in the case of data collected from third parties. This principle requires that information and communications relating to the processing of personal data be made in a concise, transparent, intelligible and easily accessible form, with simple and clear language (cons. 39, 58 and art.12 of the Regulation).

The obligation to provide data subjects with information in a "concise and transparent" form implies that the data controller presents the information in an effective and succinct manner in order to avoid information "overwhelming". They should be "clearly differentiated from other information that does not concern privacy, such as contractual clauses or general conditions of use" and should be "concrete and certain, should not be formulated in abstract or ambiguous terms or leave room for multiple interpretations" (see points 8 and 12 of the Guidelines on transparency pursuant to regulation 2016/679, adopted by the Article 29 Group, on 29 November 2017, amended version adopted on 11 April 2018 and paragraph and paragraph 3.7).

In the context of applications that are able to collect large amounts of data from the device (e.g. data stored by the user and data from different sensors, including geolocation), the end user has the right to know what kind of personal data are processed, for what purposes they are intended to be used and on the basis of what legal conditions. The availability of this information is in fact essential to obtain consent to the processing of the user's personal data, which can be considered valid only if the interested party has been previously informed about the key elements of the data processing and therefore aware of the choices on the subject. of data processing that is carrying out through the manifestation of consent. Furthermore, users should be communicated in plain and simple language whether the data can be reused by third parties and if so for what

purposes. Generic indications such as "product innovation" are inadequate to inform users (see paragraph 3.7 of Opinion 02/2013, on applications for smart devices adopted on 27 February 2013).

In compliance with the principle of transparency, both the purpose and the corresponding legal bases of the processing must therefore be clear before the processing begins.

In this regard, it should be noted that the disclosure model acquired in deeds, in response to the Company's request for information, of the XX, made by the latter as data controller, was found to be non-compliant with the aforementioned regulatory framework on the subject of protection. of personal data, as it lacks some of the essential elements provided for by the regulations in force:

the document called "privacy policy and conditions of use" (PPTOU ", Privacy policy & Terms of Use)" contains multiple sections that do not concern the processing of personal data (eg. "Senseonics policy towards minors ";" Copyright, trademarks and use ";" Exclusion of guarantees, limitations of Liability ";

the purposes of the processing are not clearly identified in a concise, intelligible and easily accessible form. In fact, they should be inferred by the interested parties by accessing different sections of the information, among other things not always relevant such as those called "Methods of use of data"; "Mobile App and Sites"; “Senseonics requests”;

the legal bases of the processing are not indicated, which cannot be deduced from the context, as - as highlighted above - they represent essential information among those to be provided to the interested parties and must therefore be clearly identified with respect to the different purposes pursued by the data controller treatment;

the data retention times are not indicated and neither can the related data retention criteria be considered defined, for example referring to the need to retain certain information "for prudential reasons". In this regard, the aforementioned Transparency Guidelines have clarified how the identification of retention times must be strictly connected to the obligation to minimize data and limit storage (Article 5, paragraph 1, letter c) e) of the Regulation). Therefore, it cannot be considered sufficient that “the data controller generally affirms that personal data will be kept as long as it is necessary for the legitimate purposes of the processing. Where relevant, different retention periods should be set for the different categories of personal data and / or processing purposes, including, where applicable, storage periods "(see Annex" Information to be provided to the data subject pursuant to article 13 or 14 "of the Guidelines on transparency, WP260, rev. 1);

the right to withdraw consent is not indicated for processing based on this condition of lawfulness, such as the processing of

health data pursuant to art. 9, par. 2, lett. a) of the Regulations, nor can it be considered implicit in the deactivation of the Senseonics account. In fact, the user could deactivate their account for reasons not related to the data protection profiles. In any case, based on art. 7, par. 3 of the Regulations, the data controller must inform the data subject of the right of revocation before the latter actually gives consent;

the rights of the data subjects pursuant to Articles 15 to 22 of the Regulation, and in particular the right to access data, are not clearly indicated in the general information;

lastly, the right to lodge a complaint with the Supervisory Authority is not indicated.

4.2.3 The exercise of the rights of data subjects (Articles 12, 13 and 15 of the Regulations)

The Regulation establishes the general rules that apply to the provision of information to data subjects (pursuant to articles 13 and 14) and to communication with data subjects regarding the exercise of their rights, pursuant to articles 15-22 (art. of the Regulation). In particular, the obligation of transparency relating to the processing of personal data is a transversal obligation that is expressed in three central elements, including the ways in which the data controller facilitates the exercise of the rights they enjoy. At the same time as the collection of personal data, the data controller is in fact required to provide the data subject, in order to ensure correct and transparent processing, information also in order, as to the existence of the rights recognized to it by Articles from 15 to 22 of the Regulations (Article 13, par. 2, letter b) of the Regulations).

In this regard, it should be noted that the document called "Privacy Policy and Conditions of Use" in the section on your rights and responsibilities does not bear any reference to the right of access of the data subjects, this in violation of art. 13, par. 2 lett. b) of the Regulations. The "access to information" section in fact concerns the information on cookies.

Therefore, the behavior of the Company that failed to mention the right of access to data provided for by art. 15 of the Regulation is in contrast not only with the provisions of art. 13 and 15 of the Regulations but also in violation of art. 12, where precise indications are provided regarding the methods by which the owner and interested party should relate with reference, among other things, to the exercise of rights by the latter.

4.2.4 The appointment of a representative established in the EU

Art. 27 of the Regulation provides that, where art. 3, par. 2, the holder is required to designate in writing a representative in the European Union, who must be established in one of the Member States in which the data subjects whose data are processed in the context of the offer of goods and services are located or the whose behavior is monitored and who acts as an

interlocutor, in particular of the supervisory authorities and data subjects, for all matters concerning the processing.

In the present case, there is no doubt that the conditions for the applicability of art. 3, par. 2, lett. a) of the Regulations; Senseonics, in fact, processes personal data of data subjects who are located in the Union and its processing activities are connected to the provision of services to European users.

The Company was therefore required to designate, by written mandate, a representative in the Union territory, instructing him to interact on its behalf with regard to the obligations deriving from the Regulations also with regard to cooperation with the Supervisory Authority. Failure to appoint this representative until 29 June 2021, the date following the start of the preliminary investigation by the Guarantor, therefore integrates the violation of art. 27 of the Regulation.

4.2.5 Additional critical issues relating to the information sent

In relation to the document in the documents, sent by the Company together with the defensive writings, specific profiles of non-compliance persist with respect to the aforementioned regulatory framework regarding the protection of personal data, as:

the document continues to be erroneously referred to as "Privacy Policy and Conditions of Use", containing multiple sections that do not concern the processing of personal data (eg. "Senseonics policy towards minors"; "Copyrights, trademarks and use ";" Exclusion of guarantees limitations of Liability ";

the purposes of the processing are not clearly identified in a concise, intelligible and easily accessible form. In fact, they should be inferred by the interested parties by accessing different sections of the information, inter alia irrelevant such as those called "Methods of use of data"; "Mobile App and Sites"; “Senseonics requests”;

it is not clear whether the "purpose" section of the new table included in the document containing the legal bases of the processing applicable to users in the European Union prevails over the multiple purposes that can be inferred from the entire document;

in relation to marketing purposes, for which the use not only of emails but also of other means of communication is envisaged (the document makes generic reference to "notes" / "notices"), it is necessary that this treatment is based on a specific legal basis. In this regard, art. 130 of the Code which requires the acquisition of specific consent from the interested parties if the use of call communication systems is envisaged without the intervention of an operator for sending advertising or direct sales or commercial communication material;

in the section called "which categories of data is collected by Senseonics" the following sentence is reported "By using the

Senseonics Products and services, you agree that we collect, transfer, store and / or process your information for the purposes described in this PPTOU document" , in fact providing a generic implicit consent to the processing of data for all the purposes indicated therein, in clear contrast not only with the legislation on the protection of personal data (see par. 3.2.1), but also with the listing the legal bases of the processing, referred to in the following table indicated in the document;

the general information does not indicate the rights due to the data subjects pursuant to articles 15 to 22 of the Regulation.

5. Conclusions

In light of the aforementioned assessments, taking into account the statements made by the owner during the investigation □ the truthfulness of which one may be called to answer pursuant to art. 168 of the Code the elements provided by the data controller in the defense brief, although worthy of consideration, do not allow to overcome most of the findings notified by the Office with the act of initiation of the procedure, however, none of the cases provided for from art. 11 of the Guarantor Regulation n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the Company in violation of articles 5, par. 1 letter a), b) and f), 6, 7, 9, 12, 13, and 27 of the Regulation. The violation of the aforementioned provisions also makes the administrative sanction provided for by art. 83, par. 4 and 5, of the Regulation, pursuant to art. 58, par. 2, lett. i), and 83, par. 3, of the same Regulation.

6. Corrective measures

Art. 58, par. 2, provides for the Guarantor a series of corrective powers, of a prescriptive and sanctioning nature, to be exercised in the event that unlawful processing of personal data is ascertained.

Among these powers, art. 58, par. 2, lett. d) of the Regulation, provides for the power to "order the data controller or the data processor to conform the processing to the provisions of this regulation, if necessary, in a certain manner and within a certain term".

In light of the aforementioned assessments, it is deemed necessary to order the Company, pursuant to the aforementioned art. 58, par. 2, lett. d) Regulation, to adopt the following corrective measures within ninety days from the notification of this provision:

1. to re-elaborate the document called "Privacy Policy and Conditions of Use" in a concise, transparent and intelligible form, also eliminating the sections that are not relevant to the personal data protection profiles such as eg. the "Senseonics Policy

towards minors"; "Copyright, trademarks and use"; "Exclusion of guarantees, limitations of Liability" and the reference to the "conditions of use";

2. to clearly indicate in the aforementioned document the specific section relating to the processing of personal data carried out towards data subjects of the European Union, in which it is necessary to expressly refer to the regulatory framework for the protection of personal data applicable to them and in particular to art. 13 of the Regulation.

3. to indicate in the same document, in a concise, transparent and intelligible form all the information required by art. 13 of the Regulations;

4. to identify, with respect to each of the purposes pursued, suitable legal bases, taking into due consideration those provided for by art. 9, par. 2 of the Regulations for the processing of health data;

5. to identify in the general information the rights of the data subjects pursuant to articles 15 to 22 of the Regulation;

6. to confirm that the privacy policy has been supplemented by providing for the right of interested parties to lodge a complaint with the Supervisory Authority, in particular in the Member State in which they usually reside, if they believe that the processing that concerns them violates the Regulation (art.77, par.1 of the Regulation).

7. Adoption of the injunction order for the application of the pecuniary administrative sanction and ancillary sanctions (articles 58, par. 2, lett. I and 83 of the Regulation; art. 166, paragraph 7, of the Code).

The violation of articles 5, par. 1 letter a), b) and f), 6, 7, 9, 12, 13, and 27 of the Regulations, caused by the conduct put in place by Senseonics Inc. is subject to the application of a pecuniary administrative sanction pursuant to art. 83, par. 4, lett. a) and 5, lett. a) and b) of the Regulations.

The Guarantor, pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, has the power to "inflict an administrative pecuniary sanction pursuant to Article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, depending on the circumstances of each single case "and, in this context," the College [of the Guarantor] adopts the injunction order, with which it also disposes with regard to the application of the ancillary administrative sanction of its publication, in whole or in excerpt, on the website of the Guarantor pursuant to Article 166, paragraph 7, of the Code "(Article 16, paragraph 1, of the Guarantor Regulation no. 1/2019).

The aforementioned administrative fine imposed, depending on the circumstances of each individual case, must be determined in the amount taking into account the principles of effectiveness, proportionality and dissuasiveness, indicated in art. 83, par. 1,

of the Regulation, in light of the elements provided for in art. 83, par. 2 and, of the Regulation. In relation to the breach of personal data notified by the data controller, pursuant to art. 33 of the Regulation, it is noted that:

1. the processing carried out concerned information suitable for detecting the state of health of about 2000 interested parties, although not of all as "the email addresses of the recipients did not necessarily contain the full name" (art. 4, par. 1, no. . 15 of the Regulations and art.83, par. 2, letters a) and g) of the Regulations);

2. the Authority became aware of the violation, through the notification of the violation, carried out by the Company on the 20th and no reports or complaints were received regarding this conduct (Article 83, paragraph 2, letter h) of the Regulations) ;

3. from the point of view of the subjective element, no intentional attitude emerges on the part of the data controller as the violation occurred as a result of a human error in sending the email (although characterized by gross negligence, taking into account that the employee had received specific instructions on the need to hide the address of all patients when sending communications via email), (Article 83, paragraph 2, letter b) of the Regulation);

4. There are no previous relevant violations committed by the data controller, nor have any provisions previously been made pursuant to art. 58 of the Regulations (Article 83, par. 2, letter e) of the Regulations);

5. the Company cooperated fully with the Authority during the investigation and this proceeding (Article 83, paragraph 2, letter f) of the Regulations);

6. the data controller, as soon as he became aware of the violation, adopted organizational measures aimed at avoiding the repetition of the unlawful conduct, providing for:

an analysis "of all other e-mails sent to make sure that the error was not repeated in other groups of e-mails";

(...) "a confirmation process in order to monitor, review and ensure that the clarification email was properly addressed and sent to the correct recipients, and that the error was not repeated";

for future and occasional direct communications to users, to request "as a further precaution (...) (as we did with the corrective email) an email confirming that the practice of including addresses in the bcc field is carried out correctly" (art. 83, par. 2, letter c) of the Regulation).

In relation to the remaining violations, it is noted that:

7. There are no previous relevant violations committed by the data controller, nor have any measures previously been ordered pursuant to art. 58 of the Regulations (Article 83, par. 2, letter e) of the Regulations);

8. the Company cooperated fully with the Authority during the investigation and this proceeding (Article 83, paragraph 2, letter f) of the Regulations);

9. the Company has put in place some measures aimed at conforming the processing of personal data to the current regulatory framework for the protection of personal data, however the non-compliance profiles highlighted above persist (par. 6)

Due to the aforementioned elements, assessed as a whole, it is believed to determine the amount of the pecuniary sanction provided for by art. 83, par. 5, lett. a) of the Regulations, to the extent of € 45,000.00 (forty-five thousand) for the violation of Articles 5, par. 1 letter a), b) and f), 6, 7, 9, 12, 13 and 27 of the Regulations, as an administrative pecuniary sanction, pursuant to art. 83, par. 1 and 3 of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary sanction of the publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Guarantor Regulation n. 1/2019, also in consideration of the type of personal data subject to unlawful processing.

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 the unlawfulness of the processing of personal data carried out by Senseonics Inc, with registered office in 20451 Seneca Meadows Parkway - Germantown, MD 20876-7005, USA, in the person of the pro-tempore legal representative represented and defended by the XX, just special power of attorney in deeds, for the violation of art. 5, par. 1 letter a), b) and f), 6, 7, 9, 12, 13 and 27 of the Regulations in the terms set out in the motivation.

ORDER

pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, to Senseonics Inc, to pay the sum of € 45,000.00 (forty-five thousand) as a fine for the violations indicated in this provision. It is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the sanction imposed.

INJUNCES

To Senseonics Inc .:

to pay the sum of € 45,000.00 (forty-five thousand) - in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code -, 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;

pursuant to art. 58, par. 2, lett. d) of the Regulations, to conform the processing to the provisions of the Regulations, adopting the corrective measures indicated in paragraph 6 of this provision, no later than 90 days from the notification of this provision. Failure to comply with an order formulated pursuant to art. 58, par. 2, of the Regulations, is punished with the administrative sanction referred to in art. 83, par. 6, of the Regulations;

pursuant to art. 58, par. 1, lett. a), of the Regulations and art. 157 of the Code, to communicate which initiatives have been undertaken in order to implement the provisions of the aforementioned par. 6, and in any case to provide feedback, adequately documented, no later than 20 days from the expiry of the term indicated above. Failure to respond to a request made pursuant to art. 157 of the Code is punished with an administrative sanction, pursuant to the combined provisions of art. 83, par. 5, of the Regulation and 166 of the Code.

HAS

pursuant to art. 166, paragraph 7, of the Code, the full 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 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

Pursuant to art. 78 of the Regulation, of art. 152 of the Code and 10 of Legislative Decree no. 150/2011, 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

Ghiglia

THE SECRETARY GENERAL

Mattei