apdcat
Autoritat Catalana de Protecció de Dades

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

File identification

Resolution of sanctioning procedure no. PS 43/2019, referring to the Maresme and Selva Health Corporation.

Background

1. On 06/22/2018, the Catalan Data Protection Authority received a letter from a person who filed a complaint against the Catalan Health Service (hereinafter, CatSalut), on the grounds of an alleged breach of the regulations on the protection of personal data. In particular, the complainant stated that by accessing his clinical history through the digital space La Meva Salut (hereinafter, LMS), he could access various clinical documentation of another patient who would have the same CIP number ((...)) than her. The complainant provided various documentation.

2. The Authority opened a preliminary information phase (no. IP 167/2018), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure of application to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, on the common administrative procedure of public administrations (henceforth, LPAC), to determine whether the facts they were likely to motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances involved.

3. In this information phase, on 28/06/2018, CatSalut was required to report, among others, on the actions carried out in response to the facts that were the subject of the complaint; if the two affected persons (the reporting person and the person referred to in the clinical documents to which they accessed) shared the same CIP code ((...)) and/or the same medical history number; as well as if in the LMS space corresponding to the other patient other than the reporting person, there were clinical documents referring to the reporting person.

This requirement was reiterated on 07/24/2018.

4. On 02/08/2018, CatSalut responded to the previous request in writing in which it stated, among others, the following:

- That the reporting person contacted CatSalut in relation to these events on 06/25/2018.

- That the incident generated two types of actions. Those that were considered to be of a priority nature and that had as their objective the repair of the situation that had given rise to the incident. In other words, remove the incorrectly published information. And the other actions that were meant to respond to the other consequences that the incident had generated and that would be launched once the priorities had been achieved.
- That the priority actions were as follows: On the same day that the complainant contacted CatSalut (25/06/2018), CatSalut spoke with

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

her requesting him to facilitate her CIP. The following day, the complainant was informed that the matter was being studied and that he would be informed as soon as the answer was available. In turn, on 26/06/2018 the eHealth Office, which is the unit that manages HC3, was requested to depublish the erroneous information. This action was not immediate since the HC3 is a repository of clinical documentation which is incorporated from the centers that are members. For this reason, the depublishing circuit requires the office that manages HC3 to contact the care center that made the publication, which, once informed, must carry out the internal actions it has established to do depublication effective.

- That the other measures that had been taken or were being taken were: reporting the incident to the Data Protection Group of the Department of Health; analyze the situation with the Data Protection Officer; report the security breach to the Catalan Data Protection Authority; report the incident to the person whose data has been exposed.

- That the investigation of the incident concluded that the reason why it occurred was the introduction of an incorrect CIP in the affected documents. Therefore, the two affected people do not share the same CIP, but a human error occurred while typing it.

- That the appropriate checks have been made and it is concluded that there has been no exchange of information between the two affected persons, so that in the historical shared clinic (HC3) corresponding to the other patient other than the reporting person there were no documents of the reporting person.

CatSalut attached various documentation to the letter.

5. On 08/03/2018, CatSalut notified the Catalan Data Protection Authority (NVS 19/2018) of the security breaches that occurred on 06/25/2018, 07/18/2018 and 25 /07/2018. In all of them, the incident suffered was described in the following terms: *"The person accesses LMS, and identifies reports that are not theirs. It is possibly an error in the documents, the documents incorporate an incorrect CIP, this fact causes other documents that are not their own to appear in the query carried out by the person.*

6. On 08/09/2018, CatSalut notified the Authority of another security breach (NVS 20/2018). In this case, CatSalut reported that *"The person accesses LMS, and identifies reports that are not theirs."*

7. On 08/14/2018, also during this preliminary information phase, the Authority's Inspection Area again required CatSalut, among others, to identify the CIP of each of the affected persons in relation to the security incidents that occurred on 06/25/2018, 07/18/2018, 07/25/2018 and 08/09/2018; specify which were the supplier entities that would have erroneously entered the user's CIP in the system; as well as whether the erroneous CIP was also contained in the patient file of each provider entity (and therefore in the original clinical documents); or if, on the contrary, the error only took place at the time of incorporating the documents into the shared medical record.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

This requirement was reiterated on 09/18/2018.

8. On 30/11/2018, CatSalut responded to the request of 14/08/2018 by providing the same letter of 02/08/2018 in response to the first request.

9. On 03/12/2018, the Authority notified CatSalut of the previous circumstance, specifying that it was necessary to respond to the 2nd request formulated.

On 11/03/2019 and 27/05/2019 the second request was reiterated.

10. On 06/20/2019, and still within the framework of this prior information phase, the Authority required the CatSalut data protection delegate, among others, to indicate the actions taken carried out with the data controller (CatSalut) in order to respond to the requirements of this Authority.

11. On 09/08/2019, CatSalut responded to the above-mentioned requirements through a letter in which it set out, among others, the following:

- That the Office of the Data Protection Delegate of the Catalan Health Service has requested on several occasions since the arrival of the various requirements, the information requested by this authority.
- That in relation to the security incidents that occurred on 25/06/2018, 18/07/2018, 25/07/2018 and 09/08/2018, the correct CIP of the reporting person was (...) and that of the other affected person was (...).
- That the provider entity that would have erroneously entered the user's CIP in the system is the Maresme i la Selva Health Corporation (hereinafter, CSMS).
- That in the heading of the clinical documents provided by the complainant, referring to another user, although the latter's data were included (name and surname, address, address and telephone number), the CIP was that of the reporting person ((...)).
- That *"it is established that the user is not in the entity's database and it is estimated that the error occurred when the data was entered into HC3."*

12. On 14/11/2019, the director of the Catalan Data Protection Authority agreed to initiate disciplinary proceedings against the CSMS, for two alleged violations both provided for in article 83.5.a), the first in relation in article 5.1.d); and the second in relation to article 5.1.f); all of them from Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27/4, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 11/22/2019.

13. The initiation agreement explained the reasons why no charge was made with regard to CatSalut, given that the entity responsible for the events reported would be the CSMS.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

14. On 13/12/2019, the CSMS made objections to the initiation agreement.

The accused entity provided various documentation with its letter.

15. On 23/01/2020, the person instructing this procedure formulated a resolution proposal, by which he proposed that the director of the Catalan Data Protection Authority admonish the CSMS as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1.f); all of them from the RGPD.

This resolution proposal was notified on 01/24/2020 and a period of 10 days was granted to formulate allegations.

16. On 05/02/2020, the accused entity presented a statement of objections to the proposed resolution.

proven facts

Of all the actions taken in this procedure, the facts detailed below are considered accredited.

The CSMS published in the HC3 several clinical documents referring to the person with CIP (...). However, the CIP introduced by the CSMS for that purpose was the one corresponding to the person making the complaint here (CIP (...).

This resulted in the reporting person's HC3 containing clinical documents relating to a third person ((...)), which could be accessed through LMS. In turn, these facts would also have meant that the HC3 of the third person did not include those clinical documents that the person making the complaint had viewed.

These events would have taken place in an undetermined period of time, but which would in any case include between 06/22/2018 and 08/09/2018.

Fundamentals of law

1. The provisions of the LPAC, and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of the Catalan Data Protection Authority. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

2. The accused entity has made allegations both in the initiation agreement and in the resolution proposal. The first ones were already analyzed in the proposed resolution, but even so it is considered appropriate to mention them here, given that they are partly reproduced in the second ones. The set of allegations made by the accused entity are then analysed.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

2.1. On the shared clinical history of Catalonia (HC3).

In its statement of objections to the proposed resolution, the CSMS states that on the HC3 *"he does not hold the status of responsible for the treatment and therefore cannot decide on the security measures that are implemented."*

At this point, the first thing to note is that in the present case the CSMS is not charged with the breach of data security.

Having established the above, as indicated in the resolution proposal, article 4.7 of the RGPD defines the data controller as *"the natural or legal person, public authority, service or other body that, alone or together with others , determine the ends and means of the treatment; if the Law of the Union or of the Member States determines the purposes and means of the treatment, the person responsible for the treatment or the specific criteria for his appointment may be established by the Law of the Union or of the Member States".*

And article 4.8 of the RGPD considers that the person in charge of the treatment is *"the natural or legal person, public authority, servicio or other organism that treats personal data on behalf of the person responsible for the treatment".*

For its part, article 33.1 of Organic Law 3/2018, of December 5, on Protection of Personal Data and guarantee of digital rights (hereinafter, LOPDGDD), provides that *"Access by a person in charge of processing personal data that is necessary for the provision of a service to the person in charge is not considered a communication of data as long as the provisions of Regulation (EU) 2016/679, this Organic Law and its rules are complied with of deployment."*

In the present case, as explained by the instructing person in the resolution proposal, it cannot be considered that in the treatments linked to the HC3, the CSMS holds the status of data controller as such, given that it does not process the data for account of a manager in order to provide him with a service.

Indeed, the CSMS is responsible for the information relating to its patients, which it is obliged to communicate to the HC3 in accordance with the additional provision of Law 21/2000, of December 29, on the rights of information concerning the patient's health and autonomy and clinical documentation (hereinafter Law 21/2000). Consequently, the CSMS is also responsible for the information of its patients that can be consulted through LMS, so it must guarantee the accuracy of the data it provides to the HC3, as well as that it is not violated the principle of confidentiality because of this inaccuracy.

Having said that, the additional provision of Law 21/2000, attributes to the Department of Health *"the objective of advancing the configuration of a single clinical history per patient, must promote, through a process that guarantees the participation of all the agents involved, the study of a system that,*

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

taking into account the evolution of technical resources, enable the shared use of clinical histories between care centers in Catalonia, so that patients treated in several centers do not have to undergo repeated examinations and procedures, and care services have access to all available clinical information."

Therefore, the Department of Health (which in turn has delegated certain actions to CatSalut) is responsible for the processing of this system (HC3) and, as an example, must guarantee the security of the data that there are incorporated However, the care centers of Catalonia continue to be responsible for the data they provide.

2.2. On the principle of confidentiality.

The CSMS also states in its letter of objections to the proposed resolution that *"Despite the allegations made at the time by this party, it is true that it has been accepted in those same allegations that produce an involuntary error in the transcription of a patient's CIP and that this error implies a violation of the principle of data accuracy."*

So, as indicated by the instructing person in the resolution proposal, in the framework of the present sanctioning procedure the CSMS has admitted that since 1999 it has been wrongly treating the CIP data linked to the person to whom the disputed reports (patient 2), to which the CSMS assigned the CIP of the person reporting here (patient 1), so that we would be faced with a permanent violation of the principle of accuracy, the effects of which maintain until 26/07/2018 (date on which all erroneous HC3 reports were withdrawn).

And then, he explains that he does not share that he *"violated the principle of confidentiality, since this violation occurs when the person making the complaint accesses through La Meva Salut data that this platform "obtains" from the Clinical History of Catalonia."*

In this respect, as the instructing person argued in the resolution proposal, the violation of the principle of confidentiality certainly took place following the publication in the HC3 of the controversial reports relating to patient 2, which the person here was able to access complainant given that they were erroneously linked to his CIP.

However, the violation of the principle of confidentiality is a consequence of the violation of the principle of accuracy, since if the CSMS had not mistakenly associated the information of patient 2 with the reporting person, the latter would not have been able to access the relevant reports to another person (patient 2).

Another thing is that, as specified by the instructing person in the resolution proposal, in accordance with article 29.5 of Law 40/2015, of October 1, on the legal regime of the public sector (hereafter, LRJSP), s only impose a penalty, given that the violation of the principle

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

of accuracy, it would be subsumed by the violation of the principle of confidentiality, as will be explained later.

2.3. About the performance of the CSMS.

Finally, the CSMS points out in its statement of objections to the proposed resolution that it is *"relevant that the response of the CSMS when the violation of the principle of accuracy was detected was quick and effective, so that, as the instructor acknowledges, a position of pro-active responsibility was made clear in relation to the incident that happened."*

Indeed, as the instructing person highlighted in the resolution proposal, it is worth highlighting the diligence shown by the CSMS both to correct the effects of the imputed infractions (removing from the HC3 the documents associated with an erroneous CIP and publishing them again but with the correct CIP); as well as in the measures that, in the statement of objections before the initiation agreement, it stated that it would implement to avoid the erroneous publication of information in the HC3, which demonstrates the good disposition of the CSMS to implement the necessary measures to guarantee the fundamental right to the protection of personal data and, ultimately, their proactive responsibility.

However, it should be pointed out that the adoption of corrective measures would in no way detract from the imputed infractions or their legal classification.

Ultimately, the allegations made by the CSMS against the proposed resolution must be dismissed

3. The conduct described in the proven facts section violates the principles of accuracy (article 5.1.d RGPD) and data confidentiality (article 5.1.f RGPD).

Firstly, article 5.1.d) of the RGPD regulates the principle of accuracy establishing that personal data will be *"exact and, if necessary, updated; all reasonable measures will be taken to delete or rectify without delay the personal data that are inaccurate with respect to the purposes for which they are processed".*

And, secondly, article 5.1.f) of the RGPD regulates the principle of confidentiality determining that personal data will be *"treated in such a way as to guarantee an adequate security of personal data, including protection against treatment unauthorized or illegal and against accidental loss, destruction or damage, through the application of appropriate technical or organizational measures".*

As indicated by the instructing person, during the processing of this procedure the facts described in the proven facts section, which are considered constitutive of an infraction provided for in article 83.5.a) in relation to articles 5.1.d); and also, of an infringement provided for in the same article 83.5.a) in relation to article 5.1.f); all of them from the RGPD.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Article 83.5.a) of the RGPD, typifies as an infringement, the violation of the *"basic principles of the treatment, including the conditions for consent pursuant to articles 5, 6, 7 and 9",* among which they contemplate both the principle of accuracy (art. 5.1.d RGPD), and the principle of confidentiality (art. 5.1.f RGPD).

As has been advanced, in the present case both infringements are linked in the sense that one of the infringements (the violation of the principle of accuracy) has led to the commission of the other (the violation of the principle of confidentiality).

In this sense, article 29.5 of the LRJSP provides that *"When the commission of one offense necessarily leads to the commission of another or others, only the penalty corresponding to the most serious offense committed must be imposed ."*

In the present case, in which the two offenses committed are provided for in article 83.5.a) of the RGPD (which refers to both the violation of the principle of accuracy and the principle of confidentiality), the conduct described in proven facts, by reason of their connection, should only be sanctioned for the violation of the principle of confidentiality, given that the violation of the principle of accuracy would be subsumed by the first violation.

4. Article 83.7 of the RGPD provides that each Member State may establish rules on whether administrative fines can be imposed on authorities and public bodies, without prejudice to the corrective powers of the control authority under art. 58.2 of the GDPR. And adds article 84.1 of the RGPD that the member states must establish the rules regarding other sanctions applicable to the violations of this Regulation, in particular those that are not sanctioned with administrative fines in accordance with article 83.

In this regard, article 21.2 of Law 32/2010 determines the following:

> *"2. In the case of violations committed in relation to publicly owned files, the director of the Catalan Data Protection Authority must issue a resolution declaring the violation and establishing the measures to be taken to correct its effects . In addition, it can propose, where appropriate, the initiation of disciplinary actions in accordance with what is established by current legislation on the disciplinary regime for personnel in the service of public administrations. This resolution must be notified to the person responsible for the file or the treatment, to the person in charge of the treatment, if applicable, to the body to which they depend and to the affected persons, if any".*

In this same sense, the art. 46 of Organic Law 15/1999, of December 13, on the protection of personal data (LOPD), valid until the entry into force of the LOPDGDD, provided that in the case of infractions committed by public administrations, in the resolution in which the infringement is declared, the measures to be taken must be established so that the effects of the infringement cease or are corrected.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

However, as explained by the instructing person in the resolution proposal, it is not appropriate propose no requirement for corrective measures, given that the CSMS already carried out the relevant actions to correct the inaccuracy of the erroneously published reports in the HC3 and that allowed a third person other than the affected person to access them through LMS .

resolution

For all this, I resolve:

1. Admonish the Maresme and Selva Health Corporation as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1.f), all of them of the RGPD.

It is not necessary to require corrective measures to correct the effects of the infringement, in accordance with what has been set out in the 4th legal basis.

2. Notify this resolution to the CSMS.

3. Communicate the resolution issued to the Ombudsman, in accordance with the provisions of article 77.5 of the LOPDGDD.

4. Order that this resolution be published on the Authority's website (apdcat.gencat.cat), in accordance with article 17 of Law 32/2010, of October 1.

Against this resolution, which puts an end to the administrative process in accordance with articles 26.2 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, and 14.3 of Decree 48/2003 , of February 20, by which the Statute of the Catalan Data Protection Agency is approved, the imputed entity can file, with discretion, an appeal for reinstatement before the director of the Catalan Data Protection Authority Data, within one month from the day after its notification, in accordance with the provisions of article 123 et seq. of the LPAC. You can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

If the imputed entity expresses to the Authority its intention to file an administrative contentious appeal against the final administrative decision, the decision will be provisionally suspended in the terms provided for in article 90.3 of the LPAC.

Likewise, the imputed entity can file any other appeal it deems appropriate to defend its interests.

The director,