apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 47/2019, referring to the Catalan Health Institute

Background

1. On 19/02/2019, the Catalan Data Protection Authority received a letter from a person who filed a complaint against the Catalan Institute of Health (ICS), on the grounds of an alleged non-compliance with the regulations on the protection of personal data.

Specifically, the complainant, who provides services as administrative staff in an ICS centre, stated the following:

a. That in May 2017 he had filed a complaint with the Ombudsman stating that the staff in charge of scheduling patients' visits through the SAP-Argos software - software that would be unique and shared for all the centers of the ICS in Girona and the Institut d'Assistència Sanitària (IAS) - could access the data relating to the diagnosis. The person making the complaint indicated that the people in charge of scheduling the visits are people who, like her, may not have a health profile, that is to say, they are people with an administrative profile and even a janitor, which is why he considered it completely disproportionate for these staff to access this type of information.
b. That the Grievance Ombudsman had initiated proceedings (...) in relation to his complaint. That on 11/10/2018, this institution made it aware that, as a result of its actions, the Department of Health had provided it with *"a copy of the functional design to be applied to anonymize the diagnoses within the system of different points, at episode level such as that of the clinical order, so that they will not be visualized in the description for users who are not doctors or nursing staff",* so he trusted that with this measure *"the diagnostic field is not accessible to non-care staff".*
c. That in February 2019, when a visit was scheduled, it still continued to be visible diagnostic field by non-care staff.

The complainant, together with his letter, provided, among other things, the following documentation:

- Copy of complaint filed with the Ombudsman in May 2017.
- Copy of the Office of the Ombudsman of 11/10/2018, addressed to the person making the complaint, mentioned in section b) above.
- Copy of an email of 05/11/2018 sent by the Head of Admissions of the ICS to several people, in which it is reported that *"this week the diagnoses will no longer be seen in the clinical orders".*
- Several screenshots of the SAP-Argos software - which the complainant had accessed as staff with an administrative profile of the ICS - in which the diagnostic field of a person who had been scheduled for a visit is displayed .

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

2. The Authority opened a preliminary information phase (no. IP 53/2019), 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 03/27/2019 the ICS was required to report on the following issues:

- Confirm whether the SAP-Argos software used by the ICS in Girona is shared with the IAS, so that both the staff with an administrative profile or caretaker assigned to the ICS, as well as those assigned to the IAS , can access the diagnostic field of the patients of either entity.

- Indicate the reasons why, on the date of the request, no measure has been implemented to prevent non-care staff (administrative or caretaker) from having access, through the SAP-Argos software, to the diagnosis of the patients

4. On 11/04/2019, the ICS responded to the aforementioned request in writing in which it set out the following:

- That, indeed, the SAP-Argos software used by the ICS in Girona is shared with the IAS, so that both the staff with an administrative profile or caretaker assigned to the ICS, and those assigned to the 'IAS, can access the diagnostic field of the patients of any of the two entities

- That *"administrative staff do not have access to diagnostic information is developed at SAP-ARGOS level and entails a structural change. The next step is its implementation, in which the healthcare impact that this entails must be assessed. At the moment, the ICS is collecting all the roles of the professionals who would not see and who would see the information. Once this screening has been carried out, the structural change will be implemented on these professionals. That the planned calendar for these actions is planned between April and May 2019".*

5. On 11/06/2019, the ICS was again required to report the following:

- Indicate whether, on the date of the request, personnel with an administrative or caretaker profile attached to the ICS and the IAS can access the diagnostic field of the patients of either entity through the SAP-ARGOS software .
- If you answered negatively to the previous question, document it.

Since the ICS did not respond to this request, the same will be repeated on 03/07/2019.

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

6. On 11/07/2019 the ICS responded to this second request, and reported the following.

- That *"staff with an administrative or caretaker profile assigned to the ICS can access the diagnostic field of patients of either entity using the SAP ARGOS software".*

- That *"the computer system is being modified in order to comply with what is being asked of them. At the moment, the evolution of SAP Argos that will allow to hide diagnostic information from non-health personnel is already done. To implement it and put it into operation it must be accompanied by the definition of a new administrative role. At SAP Argos they are working on it and plan to launch it this month, so that it meets the requirements of the ICS".*

7. On 07/19/2019, the ICS informed this Authority that they had *"defined and are in production the creation of a new user role and the necessary modifications to the SAP Argos program so that non-health personnel who , because of his work he does not have to see diagnoses, he is assigned (and they have already started doing) this new role that prevents the visualization of the diagnosis".*
The ICS provided various documentation in order to prove this point.

8. On 29/11/2019, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the ICS for an alleged infringement provided for in article 83.4.a), in relation to article 25.2; both of 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 12/12/2019.

9. In the initiation agreement, the accused entity was granted a period of 10 working days, counting from the day after the notification, to formulate allegations and propose the practice of evidence that it considered appropriate to defend their interests.

10. On 07/01/2020 the ICS submitted a letter to the Authority in which no objections were made to the initiation agreement, but it was limited to detailing the actions they had carried out in order to avoid in the future events such as those that led to the initiation of this sanctioning procedure. Specifically, the ICS reported having implemented the following measures (which it proved by providing several screenshots of the SAP Argos application):

- That *"on 2/10/2019 a new role was created for non-health personnel, which said profile does not presents the diagnosis on the screens they have access to"*
- That *"with this evolution of SAP Argos, diagnoses for user groups are anonymized who are not doctors or nursing staff".*

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

11. On 09/03/2020, the instructor of this procedure formulated a resolution proposal, by which she proposed that the director of the Catalan Data Protection Authority admonish the ICS as responsible for an infringement provided for in article 83.4.a), in relation to article 25.2; both of the RGPD.

This resolution proposal was notified on 11/03/2020 and a period of 10 days was granted to formulate allegations.

12. This deadline - despite the suspension of administrative deadlines foreseen by Royal Decree 463/2020, of March 14, by which the state of alarm is declared for the management of the health crisis situation caused by COVID-19 ; suspension that was lifted on 01/06/2020 in accordance with article 9 of Royal Decree 537/2020, of 22 May -, has been exceeded by far and no allegations have been presented,

proven facts

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

The Catalan Institute of Health had not implemented a security measure that prevented non-health personnel (administrative staff and caretakers), through the SAP-Argos application (for managing clinical histories), from accessing the "diagnostic" data of the patients, when access to said data would not be necessary to carry out the functions entrusted to them.
This situation, admitted by the ICS itself, remained at least until 02/10/2019, on which date, as reported by said entity, a new role was created for non-health personnel so that the "diagnostic" field on the screens to which they have access.

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 imputed entity has not made any objections to the resolution proposal. Nor did he formulate them before the initiation agreement, since, as stated in the 10th antecedent, in his letter of 07/01/2020 the ICS limited itself to detailing the actions that had been carried out by in order to avoid in the future events such as those that had led to the initiation of this sanctioning procedure.

3. In relation to the facts described in the proven facts section, it is necessary to refer to article 25.2 of the RGPD, which provides for the following:

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

"The person in charge of the treatment will apply the appropriate technical and organizational measures with a view to guaranteeing that, by default, only the personal data that are necessary for each of the specific purposes of the treatment are processed. This obligation will apply to the amount of personal data collected, the extent of its treatment, its retention period and its accessibility. Such measures will guarantee in particular that, by default, the personal data are not accessible, without the intervention of the person, to an indeterminate number of natural persons".

As indicated by the instructing person, during the processing of this procedure the fact described in the proven facts section, which is considered constitutive of the violation provided for in article 83.4.a) of the RGPD, has been duly proven , which typifies as such the violation *"of the obligations of the person in charge and of the manager pursuant to articles (...) 25 to 39 (...)"* of the RGPD.

The conduct addressed here has been included as a serious infringement in article 73.e) of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD), in the following form:

"The lack of adoption of the appropriate technical and organizational measures to ensure that, by default, only the personal data necessary for each of the specific purposes of the treatment are processed, in accordance with what is required by article 25.2 of the Regulation (EU) 2016/679".

4. Article 77.2 of the LOPDGDD provides that, in the case of infractions committed by those in charge or in charge listed in section 1 of said precept, the competent data protection authority:

"(...) must issue a resolution that sanctions them with a warning. The resolution must also establish the measures to be adopted so that the conduct ceases or the effects of the offense committed are corrected.
The resolution must be notified to the person in charge or in charge of the treatment, to the body to which it depends hierarchically, if applicable, and to those affected who have the status of interested party, if applicable."

In terms similar to the LOPDGDD, 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 .(...)".

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

In the case that concerns us here, in accordance with what was stated by the instructor in the resolution proposal, this Authority believes that it is not necessary to require the ICS to adopt any corrective measures since, as has been advanced, this entity has reported having carried out several actions in order to prevent certain categories of personnel from accessing health data of users that are not necessary to carry out the functions assigned to them.

resolution

For all this, I resolve:

1. Admonish the Catalan Institute of Health as responsible for an infringement provided for in article 83.4.a), in relation to article 25.2; both 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 Catalan Health Institute.

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.

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

The director,