apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Sanctioning procedure resolution no. PS 39/2021, referring to the Catalan Health Service.

Background

1. On 07/14/2020, the Catalan Data Protection Authority received a letter by which a Data Protection Officer (DPD) of a hospital participating in a study promoted and financed by the Catalan Service of Health (hereinafter, CatSalut), brought to the attention of this Authority some facts that could contravene the Data Protection regulations. Specifically, the DPD explained that the hospital in which he performed his functions had initially agreed to participate in the study called *"Evaluation of the immune status of healthcare personnel in Catalonia against the SARS-COV2 virus: information for strategies and decision-making of the Catalan health system";* and, he explained that in the framework of this study a security breach had been detected in the platform that CatSalut used for this study, in particular he indicated that *"it has been observed that on the platform if you put the NIF in the search engine to which you have access as a user of the survey of the study, you can see absolutely all the data that the RCA* [Central Register of Insured Persons] has *(address, affiliation number, CAP, type of coverage....). If we keep inventing NIFs we can access anyone's data".*

Along with this letter, various documents were provided, among others, the document entitled *"ASSESSMENT OF THE IMMUNE STATUS OF HEALTHCARE PERSONNEL IN CATALONIA AGAINST THE SARS-CoV2 VIRUS Communication of data from professionals",* dated 06/29/2020 , which detailed the design of the study and the protocols to be followed in the collection of information. Among others, and with regard to the relationship with the people who could participate with the study, the following is indicated:

"(...) an email will be sent to each professional, indicating the possibility of joining this study. In the text of this email, you will be informed of the address to which professionals can access in order to be able to fill in a short survey and give their explicit consent to participate in this study (...)".

2. Although the DPD had brought these facts to the attention of the Authority using the security breach notification form, it was considered that, given the nature of the events described, this notification should be considered as a complaint, of which was reported to the hospital DPD.

3. In line with the above, the Authority opened a preliminary information phase (no. IP 216/2020), in accordance with the provisions of article 7 of Decree 278/1993, of November 9 , on the sanctioning procedure applied to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of 1 October, on the common administrative procedure of public administrations (henceforth, LPAC), to determine if the facts were likely to motivate the initiation of a sanctioning procedure.

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

4. In this information phase, on 07/24/2020 the complainant DPD was required to inform in which specific circumstances - through the application accessed by the health personnel who had decided to participate in the aforementioned study - could be visualized
data contained in the RCA of any person whose NIF was entered in the search engine of the aforementioned application.

5. On 07/26/2020 the DPD of the hospital responded to this request in the following terms:

"We can transcribe what our information services detected: "The security problem, yes, it is true. I have put my wife's NIF in the search engine that can be accessed as a user of this survey and I can see absolutely all the data that the RCA has (address, affiliation number, ZIP code, type of coverage...). If we keep inventing NIFs we can access anyone's data".

Like other health center workers at first:
"Personal data has been transferred to third parties without my explicit consent: such as number and surname, VAT number, CIP, I know that because it identifies you with the VAT number and automatically loads the CIP, (...)
The program has a security bug and I have been able to see the variables of the same, I have not tampered with it anymore, but it is not properly protected, I am sending a photo.

6. On 07/31/2020, CatSalut - as responsible for the treatment of CKD, and as promoter of the cited study - was required to report on the circumstances under which hospital workers had decided participate in the research study, they could access data from third parties contained in the RCA; and specifically, if this access allowed viewing: a) the data of any person registered in this register; or, b) the data of the employees of the centers that participated in the study.

7. By means of a letter dated 08/03/2020, CatSalut requested an extension of the deadline to respond to the request, which was granted on 08/05/2020.

8. By means of a letter dated 31/08/2020, CatSalut requested a new extension of the deadline to respond to the request, which was denied on 16/09/2020. On the same day, the entity was warned that if it did not respond to the request, it could be in breach of data protection regulations.

9. On 09/23/2020, CatSalut responded to the request, setting out the following:

- *"The system is planned so that to access the survey you need a personalized Link that sends the application through a unique Token, with this Link that only the interested person* [the person participating in the study] receives], *a page is accessed where*

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

it asks for the DNI and it is checked that the TOKEN-DNI relationship is fulfilled, otherwise it cannot continue.

During the first few days in the survey there was a bug that allowed you to change your ID and put that of another person. As soon as the problem became known, it was solved immediately and nothing can be changed about the person participating in the study, this was specifically solved on 07/21/2020, which was the day it became known of the incidence".

- *"It cannot be specified with exactness whether access to the data of the RCA allowed viewing the data of any register, the data of all the people who participated in the study, given that from the moment it was knowledge of the 'incident was resolved and at the moment it is not reproducible, which cannot be checked at this time'.*

10. On 06/21/2021, the director of the Catalan Data Protection Authority agreed to initiate disciplinary proceedings against CatSalut for an alleged violation provided for in article 83.4.a), in relation to article 32; both of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 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 06/23/2021.

11. 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.

This deadline has been exceeded and no objections have been made.

proven facts

The workers of certain health centers received an email through which the professionals were offered the possibility to join the research study called *"Evaluation of the immune status of the health personnel in Catalonia against the virus SARS-COV2: information for the strategies and decision-making of the Catalan health system";* promoted by CatSalut. In this email, the worker was provided with a personalized link through a unique Token - associated with the DNI - which they had to connect to in order to fill out the survey and give their explicit consent to participate in the study.

From at least 14/07/2020 until 21/07/2020, the system allowed the user of the survey to change the DNI in the search engine of the application and put that of another person, from so that, in the event of doing so, the data of this third person contained in the Central Register of Insured Persons (such as address, CIP number, etc.), for which CatSalut is responsible for processing, could be viewed.

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

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. In accordance with article 64.2.f) of the LPAC and in accordance with what is indicated in the agreement initiating this procedure, this resolution should be issued without a previous resolution proposal, given that the accused entity has not made allegations in the initiation agreement.
This agreement contained a precise statement of the imputed liability.

3. In relation to the facts described in the proven facts section, it is necessary to go to article 5.1.f) of the RGPD), which regulates the principle of integrity and confidentiality, according to which personal data will be *" treated in such a way as to guarantee an adequate security of personal data, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, through the application of appropriate technical and organizational measures".*

For its part, article 32 of the RGPD, regarding data security, establishes the following:

> *"1. Taking into account the state of the art, the costs of application, and the nature, scope, context and purposes of the treatment, as well as risks of variable probability and severity for the rights and freedoms of natural persons, the person responsible and the person in charge of the treatment will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk, which in its case includes, among others:* a) *the pseudonymization and encryption of personal data;* b) *the ability to guarantee the confidentiality, integrity, availability and permanent resilience of treatment systems and services;* c) *the ability to restore availability and access to data* d) *a process of regular verification, evaluation and assessment of the effectiveness of technical and organizational measures to guarantee the security of the treatment*
>
> *2. When evaluating the adequacy of the security level, the risks presented by data processing will be particularly taken into account, in particular as a result of the accidental or unlawful destruction, loss or alteration of data*

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

personal data transmitted, stored or otherwise processed, or unauthorized communication or access to said data.

3. Adherence to a code of conduct approved pursuant to article 40 or to a certification mechanism approved pursuant to article 42 may serve as an element to demonstrate compliance with the requirements established in section 1 of this article.

4. The person in charge and the person in charge of treatment will take measures to ensure that any person who acts under the authority of the person in charge or the person in charge and has access to personal data can only process said data following the instructions of the person in charge, unless they are obliged to do so under of the Law of the Union or Member States".

In accordance with the provisions of the first additional provision of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD), reference must be made to Royal Decree 3/2010, of January 8, which regulates the National Security Scheme (ENS) in the field of electronic administration, more specifically, its article 16 relating to authorization and access control:

"Access to the information system must be controlled and limited to duly authorized users, processes, devices and other information systems, restricting access to the permitted functions.

Section 4.2. *"Access control"* of Annex II ("Security measures") of the ENS, determines the following:

Access control covers the set of preparatory and executive activities so that a certain entity, user or process, may or may not access a system resource to perform a certain action.
(…)
The following will be required in all access control:
a) That all access is prohibited, unless expressly granted.
b) That the entity is uniquely identified [op.acc.1].
c) That the use of resources is protected [op.acc.2].
d) That the following parameters are defined for each entity: what access is required, with what rights and under what authorization [op.acc.4].
e) The persons who authorize, use and control the use will be different [op.acc.3].

f) That the identity of the entity is sufficiently authenticated [op.acc.5].
g) That both local access ([op.acc.6]) and remote access ([op.acc.7]) are controlled.

By complying with all the measures indicated, it will be guaranteed that no one will access resources without authorization. In addition, the use of the

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

system ([op.exp.8]) to be able to detect and react to any accidental or deliberate failure.

When systems are interconnected in which identification, authentication and authorization take place in different security domains, under different responsibilities, in cases where it is necessary, the local security measures will be accompanied by the corresponding collaboration agreements that define mechanisms and procedures for the attribution and effective exercise of the responsibilities of each system ([op.ext]).

And, specifically, the heading 4.2.2 *"Access requirements",* determines the following:

ICAT dimensions			
level	*low medium high*		
	apply =		=

Access requirements will be met as follows:
a) System resources will be protected with some mechanism that prevents their use, except for entities that enjoy sufficient access rights.

b) Access rights for each resource will be established according to the decisions of the person responsible for the resource, adhering to the system's security policy and regulations.
c) In particular, access to the system components and their configuration files or records will be controlled."

During the processing of this procedure, the fact described in the section on proven facts, related to the lack of implementation of an adequate access control, has been duly proven, which is constitutive of the violation provided for in article 83.4.a) of the RGPD, of the RGPD, which typifies as such the violation of *"the obligations of the responsible and of the manager (...)",* in this case those linked to the security of the treatment.

The conduct addressed here has been included as a serious infraction in article 73.f) of the LOPDGDD, in the following form:

"f) The lack of adoption of technical and organizational measures that are appropriate to guarantee a level of security adequate to the risk of the treatment, in the terms required by article 32.1 of Regulation (EU) 2016/679."

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

4. Article 77.2 LOPDGDD provides that, in the case of infractions committed by those in charge or in charge listed in art. 77.1 LOPDGDD, 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 . (...)".*

In the case dealt with here, CatSalut should not be required to adopt any corrective measures to correct the effects of the infringement, since in the previous information that preceded this sanctioning procedure (9th precedent), the entity informed this Authority that *"the moment the problem became known, it was solved immediately and nothing can be changed about the person participating in the study, this was specifically resolved on 07/21/2020, which was the day we became aware of the incident".*

For all this, I resolve:

1. Admonish the Catalan Health Service as responsible for an infringement provided for in article 83.4.a) in relation to article 32, 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 Service.

3. Communicate the resolution 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 the Decree

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

48/2003, of February 20, by which the Statute of the Catalan Data Protection Agency is approved, the accused entity can file, with discretion, an appeal for reinstatement before the director of the Catalan Authority of Data Protection, 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,