apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 54/2021, referring to the Department of Health of the Generalitat of Catalonia.

Background

1. On 06/30/2021, the Catalan Data Protection Authority received a letter from a person who filed a complaint against the Department of Health, on the grounds of an alleged breach of the regulations on data protection personal data.

In particular, the complainant stated that he had detected certain security vulnerabilities on the website that the Department of Health has made available to citizens to request vaccination appointments (https://vacunacovid.catsalut.gencat.cat), already which *"allows very easy access by unauthorized third parties to vaccination data, health card, mobile phone, email, full name, appointment for vaccination, etc. To do this, you only need to have the victim's ID number (or health card). No other extra step is required to verify authenticity, nor receive any verification SMS (apart from the initial)".*

The reporting person detailed in his writing the way in which information from third parties could be accessed, and literally indicated the following steps to follow:

"1.(...)
2.(...)
3.(...)
4.(...).
5.(...)
6.(...)
7.(...)

In short, the complainant stated that once the user was validated on the website https://vacunacovid.catsalut.gencat.cat, making certain calls to the API (application programming interface) of the website through the console browser, third-party data could be accessed.

Along with his writing, the complainant provided screenshots in which he documented each of the steps he had taken to access information from third parties. In the documentation provided, the data of these third parties had been anonymized.

This complaint was assigned no. IP 264/2021.

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

2. The Authority opened a preliminary information phase, 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 October 1, of the common administrative procedure of public administrations (from now on, LPAC), to determine if the facts were likely to motivate the initiation of a sanctioning procedure.

3. On 07/05/2021, the Authority received a notification from the Department of Health of a security breach of personal data, in accordance with the provisions of article 33 of the RGPD, consisting in a possible cyberattack on the *"K2 vaccination platform",* following the detection of an unusual volume of inquiries on said platform.

4. In the preliminary information phase initiated following the complaint, on 07/09/2021 the Department of Health was required to comply with the following:

- Report on the vulnerability detected by the reporting person (1st precedent), the circumstances that would have led to it and if it had already been amended.
- Indicate whether, prior to the launch of the https://vacunacovid.catsalut.gencat.cat platform, a risk analysis had been prepared regarding the processing of personal data through this channel. If so, provide a copy.

5. On 07/22/2021 the Authority received a letter from the Department of Health supplementing the notification of the security breach it had made on 07/05/2021.

In the aforementioned written statement, the Department of Health described the security breach as *"the attack consists of making sequential ID requests, taking advantage of a shortcoming in the validation of the requests, skipping the waiting queue and directly requesting the node" .*

6. On the same day 07/22/2021, the Department of Health responded to the information request of 07/09/2021 (4th precedent), through a letter in which it set out the following:

- That *"the vulnerability described in the file was identified on July 1 following the security incident notified in file NVS 67/2021 produced against the website (https:// vacunacovid.catsalut.gencat .cat)",* which consists of *"the return of information linked to a person validating only the CIP or DNI. The information that was initially returned was: DNI, CIP, first and last name, mobile phone, email address, day and time of the appointment, place of vaccination, type of vaccine".*

- That *"the following containment, mitigation and improvement measures have been adopted:*
  • Expand the verification code from 6 numeric digits to 6 alphanumeric digits • Move the validation of the Frontend code to the node. • Application of IP banning measures by number of requests per minute (maximum of 500 requests from Spain and 50 per minute from abroad)

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

• Blocking by a commitment indicator identified in the User Agent of the request attacking

• Blocking of known attacking IPs • Encrypting the response • Contacting the abuse service of the attacking IP providers

• Restrict the information that the application returns when making a request, leaving only the information regarding the appointment (date, time and place of vaccination and type of vaccine)".

- That *" individual cases were difficult to detect but mass requests activated the control and monitoring system".*
- That *"with respect to the risk analysis, due on the one hand to the urgency of starting the vaccination process and on the other hand, the need to include the maximum volume of population in the vaccination process in the shortest time possible, security tests were carried out because an in-depth risk analysis was not carried out".*

7. On 07/14/2021, the Catalan Data Protection Authority received another letter of complaint against the Department of Health, due to an alleged breach of the regulations on personal data protection.

Specifically, the reporting entity stated that a news item had been published in a digital media (https:// www.(...)) in which it was indicated that *"the autocita website to receive the vaccine against the coronavirus of the Generalitat of Catalonia, has exposed personal data of the citizens who have made use of this platform to unauthorized third parties".*

This complaint was assigned no. IP 283/2021

8. On 09/22/2021, the Department of Health was required to comply with the following:

- Report if the security problem covered in the indicated news was the same as the security vulnerability referred to by the Department of Health in its office dated 07/22/2021, in response to request that this Authority had addressed to him in the framework of the previous information initiated following complaint no. IP 264/2021. And, in case this was not the case, answer the following:

- Report in detail about the security problem to which the news would be referring, the circumstances that would have led to it and whether it has already been amended.

9. On 08/10/2021, the Department of Health responded to this second request by means of a letter stating the following:

- That the security problem that was echoed in the indicated news is the same to which the security vulnerability detected in the framework of the previous information initiated following complaint no. IP 264/2021, insofar as the dates of publication coincide and

that the same news includes the literal content of the press release made by the Department of Health in the sense that the security breach had been communicated to the Authority through the corresponding security breach notification that gave rise to the file NVS 67/2021.

10. On 27/10/2021, the director of the Catalan Data Protection Authority agreed to initiate disciplinary proceedings against the Department of Health for two alleged violations: an violation provided for in article 83.5.a), in relation to article 5.1.f); and, another violation provided for in article 83.4.a), in relation to article 35; all of them from 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 10/27/2021.

In the initiation agreement, the accused entity was granted a period of 10 working days to formulate allegations and propose the practice of evidence that it considered appropriate to defend its interests. This deadline was exceeded without the Department of Health formulating allegations.

11. On 21/12/2021, the instructor of this procedure formulated a resolution proposal, in which she proposed the modification of the legal classification of the imputed facts that had been carried out in the initiation agreement and that of in accordance with the provisions of article 89.3 of the LPAC. The instructor, after carefully evaluating the documentation included in the actions, estimated that the two imputed events constituted, each of them, a breach of data security. In view of the above, in the resolution proposal the instructor
proposed that the director of the Catalan Data Protection Authority admonish the Department of Health as responsible for the infringement provided for in article 83.4.a) in relation to article 32 of the RGPD.

This resolution proposal was notified on 12/21/2021 and a period of 10 days was granted to formulate allegations.

12. The deadline has been exceeded and no objections have been submitted.

proven facts

1. From an undetermined date, but in any case until 30/06/2021, the information systems of the Department of Health allowed that, once the user was validated on the website https://vacunacovid.catsalut.gencat.cat (website that the Department had made available to the public in order to request a vaccination appointment), by calling the API of the web, this could access data of other users of the health system (such as the DNI, the CIP, first and last name, mobile phone, email address, date and time of the appointment, place of vaccination and type of vaccine).

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

2. In relation to the data processing linked to the launch of the website https://vacunacovid.catsalut.gencat.cat, the Department of Health did not carry out a risk analysis to determine the appropriate technical and organizational measures to ensure data security.

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 relation to the facts described in points 1 and 2 of the proven facts section, relating to data security, it is necessary to refer to article 32 of the RGPD, which provides that:

> *"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 resilience of the 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 the technical and organizational measures to guarantee the security of the treatment.*
> 2.
>
> When evaluating the adequacy of the level of security, particular consideration will be given to the risks presented by data processing, in particular as a result of the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the unauthorized communication or access to said data. (...)"

As has been said, with respect to the conduct described in points 1 and 2 of the proven facts section, it is considered that in the course of this procedure it has been proven that the Department of Health has violated the security measures detailed below separately, citing the precepts that regulate them:

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

2.1.- In relation to the proven fact 1:

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), it is necessary to mention what is established by Royal Decree 3 /2010, of January 8, which regulates the National Security Scheme (ENS) in the field of electronic administration, and specifically its section 4.2.2 *"Access requirements"* of Annex II *("Security measures"):*

> *"The access requirements will be met with what is indicated below:*
> *a) The resources of the system will be protected with some mechanism that prevents their use, except for the entities that enjoy sufficient access rights".*

2.2.- In relation to the 2nd proven fact:

At this point, express reference must be made to what is provided for in paragraph 2 of article 32 of the RGPD already transcribed, which obliges the person responsible for the treatment to carry out a risk analysis of those treatments that he plans to carry out, to purpose and effect of determining the security measures to be implemented.

In accordance with what has been explained, the facts collected in points 1 and 2 of the section on proven facts constitute the violation provided for in article 83.4.a) of the RGPD, which typifies as such, the violation of *"the obligations of the person in charge and of the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43",* among which there is that provided for in article 32.

These behaviors have been collected as a serious infringement 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."*

3. 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."*

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

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 (...)".*

By virtue of this faculty, and with regard to proven fact 2, the Department of Health should be required so that as soon as possible and in any case within the maximum period of 1 month from the day after the notification of this resolution, accredit this Authority to have carried out a risk analysis in accordance with article 32 of the RGPD, in order to determine the appropriate technical and organizational measures to guarantee the security of the data processed through the https://vacunacovid.catsalut.gencat.cat platform.

With regard to proven fact 1, it is not necessary to require the adoption of any corrective measures, since the Department of Health accredited this Authority, within the framework of NVS 67/2021, to have taken the appropriate measures to solve the security incident detected on the https://vacunacovid.catsalut.gencat.cat platform.

For all this, I resolve:

1. Admonish the Department of Health as responsible for the infringement provided for in article 83.4.a) in relation to article 32, both of the RGPD.

2. Require the Department of Health to certify to this Authority that it has carried out the action indicated in the 3rd legal basis, within the period indicated.

3. Notify this resolution to the Department of Health.

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

5. 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

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

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.