apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 82/2020, referring to the Catalan Health Institute.

Background

1. En data 03/03/2020 va tenir entrada a l'Autoritat Catalana de Protecció de Dades, per remissió de l'Agència Espanyola de Protecció de Dades, un escrit d'una persona pel qual formulava denúncia contra l'Institut Català de Health (henceforth, ICS), due to an alleged breach of the regulations on the protection of personal data. In particular, the complainant stated that, in response to a request regarding the traceability of his medical history, on 10/09/2019 the Territorial Office of Citizen Assistance of the Territorial Management of Camp de Tarragona of the ICS (henceforth, OTAC) sent him an email (from the address (...)@gencat.cat), in which he attached the requested documentation in a file in ZIP format, protected with password However, the reporting person testified that the password to access said ZIP file ("(...)") was indicated in the same e-mail message.

The reporting person provided various documentation about the events reported.

2. The Authority opened a preliminary information phase (no. IP 80/2020), 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 04/06/2020 the reported entity was required to inform, among others, whether it had considered, as a security measure, that in the same message of e-mail in which an encrypted file is sent that may contain special categories of data, include your password. In turn, the reported entity was required to provide a copy of the risk analysis, regarding the sending of e-mails that incorporated files containing special categories of data.

4. On 06/19/2020, the ICS responded to the aforementioned request in writing in which it stated, among others, the following:

- That the file that was attached to the reporting person contained information on the traceability of access to their clinical information in the requested period.
- That for the transmission of sensitive information, which requires the encryption of the document, the Document Encryption Protocol is followed, by which the "Operational Manual" is applied

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

in the transmission of documents in compliance with the LOPD". Section 3 explains the file encryption procedure, whereby the password to open the encrypted documents will be plus and year of sending the mail in the following format: MM/YY.

- That the "Instruction 3/2018, on the use of information and communication technologies in the Administration of the Generalitat of Catalonia" is also followed which, in point 9.7 establishes that the "information must encrypt when there is a regulatory requirement or when the sensitivity of the information requires it. In the latter case, each department, body or entity will establish the classification of its information in accordance with the cyber security regulatory framework."
- That according to the "Protocol for the exercise of rights over personal data", the response to requests for the exercise of these rights must be sent registered, certified and with notice of reception.
- That the complainant submitted the request for traceability of access to his clinical history on 05/13/2019. And on 31/07/2019 he submitted a claim to the Citizen Service Unit of Hospital Joan XXIII in relation to the previous request.
- That taking into account the delay in the response to your request, and the manifestation of some impatience on the part of the user, once the traceability of the accesses of the ICS professionals to your clinical history during the requested period, in order to speed up the response, it was sent by email and with the intention of facilitating the opening of the encrypted document, a quick password was set and indicated in the same email.

- That at the same time, the shipment was made by certified mail with acknowledgment of receipt, as established by the protocol. The OTAC generally sends the response to the exercise of rights by ordinary certified mail with acknowledgment of receipt in order to guarantee the maximum protection of sensitive data.
- That the procedure used in the case of the complainant was timely and motivated due to the need to respond to the request that had been delayed.
- That the OTAC follows the cyber security regulatory framework which establishes the risks in cases of non-observance of diligent actions and the appropriate procedures for security in the transmission of sensitive information.
- That there is no risk analysis, given that in the shipping procedure of sensitive information, the encryption of documents is always considered.

In accordance with the antecedents that have been related so far and with the result of the investigative actions carried out in the framework of the previous information, it is agreed to initiate this sanctioning procedure. In the following sections, all the information required by article 64.2 of the LPAC is indicated.

5. On 15/12/2020, 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 the article 32; 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 (in

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

forward, GDPR). This initiation agreement was notified to the imputed entity on 12/21/2020.

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 its interests.

The deadline has passed and no objections have been submitted.

proven facts

As a result of the reported events consisting of the fact that the ICS sent the reporting person an email on 09/10/2019, in which an encrypted file was attached containing information on the traceability of access to their clinical information and where it was also indicated what the password was to decrypt it, it was found that during an indeterminate period, but which in any case would include until 19/06/2020, the ICS had not carried out a risk analysis to determine the appropriate technical and organizational measures to ensure the security of the data sent by e-mail, and in particular, when the sending concerned special categories of data.

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 refer 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 that an adequate security of personal data is guaranteed, including protection against unauthorized or illegal treatment 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:

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

> "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 treatment manager will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk (...).
> 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 unauthorized communication or access to said data. (...)"

This implies having to carry out an assessment of the risks involved in each treatment, to determine the security measures that need to be implemented, which must be documented.

From the perspective of the regulations on data protection, the risk analysis must take into account, among others, the threats to the treatment, the impact on the affected persons or the type of risk, depending on the type of data, the number of people affected or the variety of treatments, among others.

In the present case, the accused entity had to analyze the risks involved in sending data via e-mail and, in particular, of special categories of data. And based on these risks, determine the need to implement the appropriate technical and organizational measures to guarantee their safety.

During the processing of this procedure, the fact described in the proven facts section, which is constitutive of the violation provided for in article 83.4.a) of the RGPD, which typifies the violation of "the obligations of the person in charge and of the person in charge in accordance with articles 8, 11, 25 to 39, 42 and 43", among which there is that provided for in article 32 RGPD.

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

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:

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

> "(...) 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 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".

By virtue of this power, the ICS should be required to carry out a risk analysis of in accordance with article 32 of the RGPD, to determine the appropriate technical and organizational measures to guarantee the security of the data sent by email.

Once the corrective measure described has been adopted, within the period indicated, the ICS must inform the Authority within the following 10 days, without prejudice to the Authority's inspection powers to carry out the corresponding checks .

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 32, both of the RGPD.

2. Require the ICS to adopt the corrective measures indicated in the 4th legal basis and certify to this Authority the actions taken to comply with them.

3. Notify this resolution to the ICS.

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

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

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 what they provide
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,