**File identification**

Resolution of sanctioning procedure no. PS 20/2022, referring to the Catalan Health Institute (Viladecans Hospital)

**Background**

**1.** On 11/06/2021, the Catalan Data Protection Authority received a letter from a person for which he filed a complaint against the Viladecans Hospital, dependent on the Catalan Institute of Health (ICS), with reason for an alleged breach of the regulations on the protection of personal data. The complainant stated the following:

1.1 That the Viladecans Hospital had made public several URLs where by entering only the DNI, without any other verification, personal data of the patients could be obtained. Specifically, the name, address, CIP, date of birth, telephone and email.

1.2 That in order to certify the previous statement, he provided the following URLS in which, by clicking on the 'magnifying glass' option, the personal data mentioned was obtained:

https://ciutadania.metrosud.cat/ciutadania/FRM/frm_canvi_identificatiu.aspx
https://ciutadania.metrosud.cat/ciutadania/FRM/frm_canvi_data.aspx
https://ciutadania.metrosud.cat/ciutadania/

**2.** The Authority opened a preliminary information phase (no. IP 252/2021), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to 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 were susceptible to motivate the initiation of a sanctioning procedure.

**3.** In this preliminary information phase, on 06/14/2021, the Authority's Inspection Area made a series of checks via the Internet on the facts subject to the complaint. Thus, it was found that by accessing the Viladecans Hospital website ( http://www.viladecanshospital.cat/ca/default.aspx ), section 'Citizen care unit > Let's make it easy' in the options 'Claims, complaints and suggestions' and 'Change of identification data', by entering the DNI of the reporting person and clicking on the 'magnifying glass' option, the following personal data were obtained:

Regarding the first option: first name, surname, CIP number and telephone number.

Regarding the second option: name, surname, CIP number, telephone, home address, and date of birth.

It was also verified that in the same section 'Citizen care unit > Let's make it easy', in the options 'Information pending visits and tests / date change' and 'Check surgical waiting list', following the same access process, the CIP number of the reporting person could be obtained.

Afterwards, the instructor took care of the records and kept an automated copy of the personal data that had been accessed by entering the ID of the reporting person.

**4.** On the same date, 06/14/2021, the reported entity was required to confirm that by entering the ID of any patient in the routes specified in the previous point, they could be obtained, depending on the option selected ( "Claims, complaints and suggestions", "change of identifying data", "Request for external consultation reports", "request for clinical documentation / other test reports (not images)", "request for copy of 'image", "information pending visits and tests / change of date", "consult surgical waiting list", "change of identifying data", "request for change of specialist practitioner", "for any other type of consultation" ) the following personal data:

- Name, surname, CIP number and telephone number;
- Name, surname, CIP number, telephone, home address, and date of birth; or
- CIP number

The entity was also required to indicate in relation to which patients this data could be obtained and if other clinical or health data linked to the patient could be viewed.

**5.** On 07/06/2021 and within the framework of this preliminary information phase, the Authority's Inspection Area regained access to the Internet to carry out new checks on the facts subject to the complaint. Thus, it was found that when accessing the website of the Viladecans Hospital, section 'Citizen service unit > Let's make it easy', a message appeared that said 'Application temporarily out of service. Sorry for the inconvenience' and thus the data was no longer accessible.

**6.** On 07/19/2021, the Catalan Health Institute (Viladecans Hospital) complied with the request for information through a letter stating the following:

- That due to a technical error, a test environment was published on the Hospital de Viladecans website where, by entering the patient's ID card, the 'affiliation information' was retrieved, which, according to him, consisted of the name, CIP number , home address, telephone and email address; and that in no case were open data of the patients of the hospital or of any patient treated at the organization, but only of the 'active' patients of the Viladecans Hospital.
- That no data related to the patient's clinical and healthcare information could be viewed.
- That at the time of detection of the technical error , the web pages were depublished so that they cannot be accessed from the outside, that is, the Internet.
- He also stated that at the time of submission of the response to the request (19/07/2021), none of the reported URLs could be accessed.

**7.** On 20/04/2022, 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 (hereinafter, RGPD). Likewise, he appointed Mrs. (...), an official of the Catalan Data Protection Authority, as the person instructing the file. This initiation agreement was notified to the imputed entity on 04/22/2022.

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.

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

**proven facts**

The website of the Viladecans Hospital ( http://www.viladecanshospital.cat/ca/default.aspx ) allowed access to patients' personal data, following the route ' *Citizen care unit > Let's do it easy',* selecting one of the four options that will be specified below, and just entering the DNI and clicking on the ' *magnifying glass' option* , without requiring any additional data, password, or additional authentication measure .

Options:
- Option ' *Complaints complaints and suggestions'* : the name, surname, CIP number and telephone.
- Change *of Identification Data'* option : name, surname, CIP number, telephone, home address, and date of birth.
- Option ' *Information pending visits and tests / change of date'* and option *'Check surgical waiting list'* : the CIP number

This situation was maintained for an indeterminate period of time that, at least, starts from 06/14/2021, the date on which the Authority's Inspection Area carried out checks via the Internet and confirmed the accessibility of a patient's personal data by entering their ID as the only access requirement; and until an undetermined date but in any case prior to 07/06/2021, the date on which the Inspection Area carried out new checks and found that it was no longer possible to access the route mentioned in the first paragraph of this section.

**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 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 to initiate this procedure, this resolution should be issued without a previous resolution proposal, given that the The imputed entity has not submitted allegations to the initiation agreement.

This agreement contained a precise statement of the imputed liability.

**3.** With regard to the fact described in the proven facts section, relating to data security, it is necessary to go to article 32 of the RGPD, which provides:

*"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 measures appropriate technical and organizational*

*techniques to guarantee a level of security adequate to the risk , which if applicable includes , among others :*

a) *the pseudonymization and encryption of personal data;*
b) *the ability to guarantee the confidentiality, integrity, availability and permanent resilience of the treatment systems and services;*
c) *the ability to quickly restore availability and access to personal data in the event of a physical or technical incident;*
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.*
3. *Adherence to a code of conduct approved in accordance with article 40 or a certification mechanism approved in accordance with 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 data controller will take measures to ensure that any person who acts under the authority of the data controller or the data controller and has access to personal data can only process said data following the instructions of the data controller, unless they are required to do so by virtue of law of the Union or of the Member States".*

Likewise, 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 the guarantee of digital rights, 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, in its article 16:

*"Article 16.* ***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 permitted functions. "*

Section 4.2.5 *" Mechanism of authentication "* of Annex II ("Security measures") of the ENS, determines the following:

*"The authentication mechanisms in front of the system will be adapted to the system level, taking into account the following considerations, and the following authentication factors can be used:*

*- "something that is known": password or agreed keys.*

*- "something you have": logical components (such as software certificates) or physical devices (in English, tokens)*

*- "something that is": biometric elements.*

*The above factors can be used in isolation or combined to generate strong authentication mechanisms.*

*(…)*

*LOW level*
*a) As a general principle, the use of any will be accepted authentication mechanism _ supported by a single factor.*
*b) In the case of using " something known " as a factor , they will be applied rules basic quality of the same .*
*c) The security of the credentials will be taken care of so that:*
*1. The credentials will be activated once they are under the effective control of the user .*
*2. Credentials they will be under the exclusive control of the user .*
*3. The user will acknowledge that he has received them and that he knows and accepts the obligations involved tenure , in particular, the duty of diligent custody , protection of su confidentiality and information immediate in case of loss .*
*4. Credentials will be changed with a frequency marked by the organization 's policy , depending on the category of the system accessed .*
*5. Credentials will be withdrawn and will be disabled when the entity (person, team or process ) that authenticates ends relationship with the system.*
*(...)"*

Also article 9.4 of Law 21/2000, of December 29, on the rights of information concerning the patient's health and autonomy, and the clinical documentation, determines that *"health centers must take the technical measures and adequate organizational measures to protect the personal data collected and prevent their destruction or accidental loss, and also access, alteration, communication or any other processing that is not authorized".*

During the processing of this procedure, the fact described in the section on proven facts has been duly proven, recognized, in addition, by the entity denounced in its allegations in the preliminary information phase (IP 252/ 2021), when he admits to having committed ' *a technical error* ' by publishing ' *a test environment where by entering a patient's ID, affiliation information (names, CIP, address, phone and email address) was retrieved.'*

This fact is constitutive of the violation provided for in article 83.4.a) of the RGPD, which typifies the violation of *" the obligations of the responsible person and of the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43"* between which have the obligation described in article 32 referring to the security of the treatment.

In turn, this conduct 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".*

**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 present case, the ICS should not be required to adopt corrective measures in order to correct the effects of the infringements, since it is a fait accompli and, moreover, the ICS, at the time of detection of the error, proceeded to depublish the web pages. At the same time, he stated that at the time of submission of the response to this Authority's request (19/07/2021), it was no longer possible to access any of the reported URLs.

For all this, I resolve:

**1.** To warn 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.

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 legal basis 4.

**2.** Notify this resolution at the Institute Health Catalan . _

**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 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,