File identification

Resolution of sanctioning procedure no. PS 91/2022, referring to the Parc Taulí Health Corporation of Sabadell.

Background

1. On 10/10/2022, the Catalan Data Protection Authority received, by transfer from the AEPD, a letter from a person for which he filed a complaint against the Parc Taulí de Sabadell Health Corporation (hereinafter, the Corporation), due to an alleged breach of the regulations on the protection of personal data. Specifically, the complainant complained that a relative of his, who works for the Corporation, had been accessing his medical history for years without any authorization.

Together with the complaint, he provided the copy of the letter, which on 10/10/2022, the Corporation had addressed to him in response to his request for traceability of his medical history. In this response, the Corporation made it aware that during the last 5 years there were accesses to its shared clinical history (HC3) carried out by four doctors of the digestive service (on dates 11/10/2017, 31/10/ 2019, 27/04/2020 and 17/02/2022), that said accesses ' *are the result of an error because you do not have follow-up in this particular service and hospital'* and that, although they had not found the cause of the 'error, they promised to fix it.

2. The Authority opened a preliminary information phase (no. IP 357/2022), 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 information phase, on 10/25/2022 the Corporation was required to provide a copy of the access register corresponding to the medical history of the person reporting, and to provide detailed information on each of the accesses related to the 1st background (user and professional profile of the person who accessed it, modules accessed and justification for each access). The Corporation was also asked to report whether it had initiated any action in order to resolve any disciplinary responsibilities against those people who had improper access, if this was the case.

4. On 8/11/2022, the Corporation responded to the above-mentioned request through a letter in which it stated the following:

- Firstly, he provided an access log in which there are 4 accesses to the HC3 (database that depends on the Department of Health) of the complainant here - coincident with those contained in the office that the Corporation had addressed to the complainant (1st precedent)-. The 4 accesses are linked to four different specialist doctors, on the following dates and times (as specified in the table provided):

    - 11/10/2017, 10:12:08 a.m
    - 31/10/2019, 12:33:19h
    - 27/04/2020, 08:55:26h

- 02/17/2022, 3:58:31 p.m

- The following was then set out:

  That ' *accesses correspond to attempts to connect to the HC3 viewer or successful connection to this viewer as described in the table in the previous point* '. That ' *the patient's history was reviewed, verifying that: - The patient was not being treated by the profile of doctors that appeared in the audit. In fact, the only care in this Hospital were one-off visits to the emergency room on January 5 and 7, 2011 for illnesses that had nothing to do with the specialty of the digestive system.'*

  That ' *Information was requested from the three professionals who continued to work in this center on the date of the audit and none of them explained the access.'*

  That ' *an attempt was made to verify, through a query with information systems, if there was a similar history number that explained the access by mistake, a very difficult task that was done in a limited way and that did not provide more information.'*

  That ' *All of the above led to the conclusion of a possible typing error, a possible alternative since the profiles of professionals have access to all clinical histories.*

- Finally, the Corporation stated that, in view of the above, it was not considered necessary to carry out any disciplinary action.

5. On 5/12/2022, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the Corporation for an alleged infringement provided for in article 83.5.a), in relation to the article .5.1.a), 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 of these (hereinafter, RGPD).

6. On 18/01/2023, the person instructing this procedure formulated a resolution proposal, by which he proposed that the director of the Catalan Data Protection Authority admonish the Corporation as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1.a), both of the RGPD.

This resolution proposal was notified on the same date, 18/01/2023, and a period of 10 days was granted to formulate allegations.

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

proven facts

On 11/10/2017 at 10:12 a.m., 31/10/2019 at 12:33 p.m., 27/04/2020 at 8:55 a.m.; and 02/17/2022 at 3:58 p.m.; the HC3 (database that depends on the Department of Health) of the person reporting was accessed, without their consent and without these accesses being related to any assistance or diagnostic action. These 4 accesses are linked to four users with the profile of doctor/specialist in the digestive system service of the Parc Taulí de Sabadell Health Corporation.

Although of these 4 accesses, the first and second (of 11/10/2017 and 31/10/2019) would already be time-barred (the first of them long before a complaint was lodged with the Authority; and the second, a few days later), not so the other two accesses made on 27/04/2020 and 17/02/2022), respectively.

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. The accused entity has not made allegations in the resolution proposal, but it did so in the initiation agreement. Regarding this, it is considered appropriate to reiterate below the most relevant part of the motivated response of the instructing person to these allegations.

2.1. In relation to the Corporation's allegation that "the healthcare reality of hospitals and the complexity of information systems do not allow a doctor (for example) to have access only to the patients he usually visits, because he can receive inter -consultations, staying in the emergency room, being an imaging diagnostic specialist or other situations that determined a default access to any patient who had a medical history in our center. We have evidence that this way of proceeding is the usual in the hospital centers of Catalonia", the instructing person has made it clear that, during the preliminary information phase, the Corporation recognized that the reported accesses had no medical justification, since the reporting person was not being treated by the "profile of practitioners" (digestive system doctors) who, as determined in the audit, had accessed the HC3, adding that the medical assistance that the Corporation had provided to the complainant here dated back to January 2011 'for illnesses that had nothing to do with the specialty of the digestive system'.

2.2. In relation to the Corporation's allegation that "in order to control access, monthly audits have been carried out since 2017" where a significant number of accesses are reviewed to determine if there has been some incorrect"" and that this subsequent control of the accesses made "cannot prevent there being an error in accessing certain stories by typing in a story number incorrectly which is what we believe happened", the instructing person has considered that the fact that there were four accesses to the complainant's HC3 (even though, as has been shown in the proven facts, two of the accesses have not been imputed due to prescription) using the codes of user of four different professionals who worked at the Corporation, all of them from the same (digestive) Service, allows us to question this version that attributes to specific errors the cause of these different accesses to the same HC3.

According to what has been explained, these allegations do not allow the reality of the imputed facts to be distorted, nor their legal assessment.

3. In relation to the facts described in the proven facts section, relating to the principle of legality, it is necessary to go to article 5.1.a) of the RGPD which establishes that *"the data personal they will be treated lawfully, loyally and transparently in relation to the interested party (lawfulness, loyalty and transparency* ".

For its part, article 6 of the RGPD provides the following regarding the legality of the treatment:

"1. The treatment will only be lawful if at least one of the following conditions is met:

a) the interested party gives his consent for the treatment of his personal data for one or several specific purposes;

b) the treatment is necessary for the execution of a contract in which the interested party is a party or for the application at the request of this pre-contractual measures;

c) the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment;

d) the treatment is necessary to protect the vital interests of the interested party or another natural person;

e) the treatment is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment;

f) the treatment is necessary for the satisfaction of legitimate interests pursued by the person responsible for the treatment or by a third party, provided that these interests do not prevail over the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a child.

The provisions in letter f) of the first paragraph shall not apply to the processing carried out by public authorities in the exercise of their functions.

2. Member States may maintain or introduce more specific provisions in order to adapt the application of the rules of this Regulation with respect to treatment in compliance with paragraph 1, letters c) and e), setting more precisely specific treatment requirements and other measures that guarantee legal and equitable treatment, including other specific situations of treatment pursuant to chapter IX.

3. The basis of the treatment indicated in section 1, letters c) and e), must be established by:

a) the Law of the Union, or

b) the Law of the Member States that applies to the person responsible for the treatment (…)."

For its part, article 9 of the RGPD, relating to the treatment of special categories of data -such as health data-, determines the following:

"1. The processing of personal data that reveal ethnic or racial origin, political opinions, religious or philosophical convictions, or trade union affiliation is prohibited, and the processing of genetic data, biometric data aimed at uniquely identifying a natural person, data relating to health or data relating to the sexual life or sexual orientation of a natural person.

2. Section 1 will not apply when one of the following circumstances occurs:

a) the interested party gives his explicit consent for the treatment of said personal data with one or more of the specified purposes, except when the Law of the Union or of the Member States establishes that the prohibition mentioned in section 1 cannot be lifted by the interested party;

b) the treatment is necessary for the fulfillment of obligations and the exercise of specific rights of the person responsible for the treatment or of the interested party in the field of labor law and of social security and protection, to the extent that this is authorized by the Law of the Union of the Member States or a collective agreement in accordance with the Law of the Member States that establishes adequate guarantees of respect for the fundamental rights and interests of the interested party;

c) the treatment is necessary to protect the vital interests of the interested party or another natural person, in the event that the interested party is not physically or legally able to give their consent;

d) the treatment is carried out, within the scope of its legitimate activities and with due guarantees, by a foundation, an association or any other non-profit organization, whose purpose is political, philosophical, religious or trade union, provided that the treatment refers exclusively to current or former members of such organizations or persons who maintain regular contact with them in relation to their purposes and provided that personal data is not communicated outside of them without the consent of the interested parties;

e) the treatment refers to personal data that the interested party has made manifestly public;

f) the treatment is necessary for the formulation, exercise or defense of claims or when the courts act in the exercise of their judicial function;

g) the treatment is necessary for reasons of an essential public interest, on the basis of the Law of the Union or of the Member States, which must be proportional to the objective pursued, essentially respect the right to data protection and establish measures adequate and specific to protect the fundamental interests and rights of the interested party;

h) the treatment is necessary for the purposes of preventive or occupational medicine, evaluation of the worker's labor capacity, medical diagnosis, provision of health or social assistance or treatment, or management of health and social care systems and services, on the basis of the Law of the Union or of the Member States or by virtue of a contract with a health

professional and without prejudice to the conditions and guarantees contemplated in section 3;

i) the treatment is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health, or to guarantee high levels of quality and safety of health care and medicines or sanitary products, on the basis of the Law of the Union or of the Member States that establishes appropriate and specific measures to protect the rights and freedoms of the interested party, in particular professional secrecy,

j) the treatment is necessary for archival purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with article 89, paragraph 1, on the basis of the Law of the Union or of the Member States, which must be proportionate to the objective pursued, essentially respect the right to data protection and establish appropriate and specific measures to protect the fundamental interests and rights of the interested party.

3. The personal data referred to in section 1 may be processed for the purposes mentioned in section 2, letter h), when its treatment is carried out by a professional subject to the obligation of professional secrecy, or under his responsibility, in agreement with the Law of the Union or of the Member States or with the rules established by the competent national organisms, or by any other person also subject to the obligation of secrecy in accordance with the Law of the Union or of the Member States or of the rules established by the competent national bodies.

4. Member States may maintain or introduce additional conditions, including limitations, with respect to the processing of genetic data, biometric data or health-related data."

And, article 9 of the LOPDGDD, referring to the special categories of data, among which are health data, determines in its section 2 the following:

"2. The data treatments provided for in letters g), h) ii) of article 9.2 of Regulation (EU) 2016/679 based on Spanish law must be protected by a rule with the rank of law, which can establish requirements additional information regarding its security and confidentiality. In particular, this rule can protect the processing of data in the field of health when this is required by the management of health and social assistance systems and services, public and private, or the execution of a contract insurance of which the affected person is a party."

The health legislation, applicable to the case, regulates the use of the clinical history in the following terms:

Article 11 Law 21/2000, of December 29, on the rights of information concerning the patient's health and autonomy, and clinical documentation:

"1. The clinical history is an instrument primarily intended to help guarantee adequate assistance to the patient. For this purpose, the care professionals of the center who are involved in the diagnosis or treatment of the patient must have access to the clinical history.

2. Each center must establish the mechanism that makes it possible that, while assistance is provided to a specific patient, the professionals attending to him can, at all times, have access to the corresponding clinical history.

3. The clinical history can be accessed for epidemiological, research or teaching purposes, subject to the provisions of Organic Law 15/1999, of December 13, on the protection of personal data, and the Law of State 14/1986, of April 25, general health, and the corresponding provisions. Access to the clinical history for these purposes obliges the preservation of the patient's personal identification data, separate from those of a clinical care nature , unless the patient has previously given consent.

4. The staff who take care of the administration and management tasks of the health centers can access only the data of the clinical history related to said functions.

5. The personnel in the service of the Health Administration who perform inspection functions, duly accredited, can access the clinical histories, in order to check the quality of the assistance, the fulfillment of the patient's rights or any other obligation of the center in relation to patients or the Health Administration.

6. All staff who use their powers to access any type of clinical history data remain subject to the duty of confidentiality."

In turn, article 16 of Law 41/2002, of November 14, " *basic regulation of patient autonomy and rights and obligations in the field of information and clinical documentation* ", provides:

"1. The clinical history is an instrument primarily intended to guarantee adequate assistance to the patient. The healthcare professionals of the center who carry out the diagnosis or treatment of the patient have access to the patient's clinical history as a fundamental tool for their adequate assistance.

2. Each center will establish the methods that enable access to the clinical history of each patient at all times by the professionals who assist them.

3. Access to clinical history for judicial, epidemiological, public health, research or teaching purposes is governed by the provisions of current legislation on the protection of personal data, and Law 14/1986, of April 25, General of Health, and other rules of application in each case. Access to the clinical history for these purposes requires the preservation of the patient's personal identification data, separate from those of a clinical and healthcare nature , so that, as a general rule, anonymity is ensured, unless the patient himself has given his consent to don't separate them.

The investigation cases provided for in Section 2 of the Seventeenth Additional Provision of the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights are excluded.

Likewise, cases of investigation by the judicial authority are excluded in which the unification of identifying data with clinical care is considered essential , in which cases the judges and courts in the corresponding process will follow. Access to clinical history data and documents is strictly limited to the specific purposes of each case.

When it is necessary for the prevention of a serious risk or danger to the health of the population, the health administrations referred to in Law 33/2011, of October 4, General Public Health, will be able to access the identifying data of patients for epidemiological or public health protection reasons. Access must be carried out, in any case, by a healthcare professional subject to professional secrecy or by another person subject, likewise, to an equivalent obligation of secrecy, with prior motivation on the part of the Administration that requested access to the data.

4. The administration and management staff of the health centers can only access the clinical history data related to their own functions.

5. Duly accredited health personnel who carry out inspection, evaluation, accreditation and planning functions have access to clinical records in the fulfillment of their functions of checking the quality of care, respect for patient rights or any other obligation of the center in relation to patients and users or the health administration itself.

6. The personnel who access the clinical history data in the exercise of their functions are subject to the duty of secrecy.

7. The Autonomous Communities will regulate the procedure so that there is a record of access to the clinical history and its use".

During the processing of this procedure, it has been duly proven that personnel of the accused entity accessed the HC3 of the person making the complaint without these accesses being protected by any legal basis, a fact that is considered constitutive of the offense provided for in article 83.5.a) of the RGPD, which typifies the violation of the " principles basics for treatment , including the conditions for consent pursuant to articles 5, 6, 7 and 9", among which the principle of legality is at the forefront.

The conduct addressed here has been included as a very serious infraction in article 72.1.e) of the LOPDGDD, in the following form:

"The processing of personal data of the categories referred to in article 9 of Regulation (EU) 2016/679, without any of the circumstances provided for in the aforementioned precept and article 9 of this Organic Law"

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, given that it is a fait accompli, it is considered unnecessary to propose the adoption of corrective measures.

For all this, I resolve:

1. Admonish the Parc Taulí de Sabadell Health Corporation as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1.a), 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 Parc Taulí Health Corporation of Sabadell.

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,