File identification

Resolution of sanctioning procedure no. PS 49/2022, referring to the Terrassa Mutual Assistance Foundation

Background

1. On 08/23/2021, the Catalan Data Protection Authority received a letter from a person in which he filed a complaint against Fundació Assistencial de Mútua de Terrassa (hereinafter, FAMT), on the grounds of a alleged breach of the regulations on personal data protection . Specifically, the complainant (Mrs. (...), who claimed to be a user of the FAMT within the framework of public health care, complained of alleged improper access to her medical history by an employee of the FAMT that identified with first and last names.

The complaint was accompanied by an email sent on 04/29/2021 by the FAMT to the complainant, through which he was informed that " *as a result of his complaint, we have carried out the relevant checks, and We confirm that, indeed, this illegitimate access has occurred on the part of said professional. For this reason, the corresponding disciplinary measures have been taken".*

2. The Authority opened a preliminary information phase (no. IP 334/2021), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure for application 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 29/11/2021 the reported entity was required to answer several questions relating to the reported events.

4. On 12/15/2021, the FAMT responded to this Authority's request in the following terms:

- That " two accesses to the Shared Clinical History of Catalonia [of the complainant] *have been identified , on 05/03/19 and 05/01/21",* carried out by the (...)(.. .).
- That " *we are not aware that the two accesses carried out on 03/05/19 and 01/05/21 coincide with an assistance act, or are legitimized by an administrative procedure".*
- That " *the Data Protection Commission of the entity (...), met to decide the measures to be taken regarding these accesses, and it was decided to initiate the corresponding disciplinary action against this worker for the access to this clinical history for purposes other than health care."*

The letter was accompanied by the following documentation:

a) Register of accesses to the medical history of the reporting person, which contains two accesses made by the (...)(...) - with the profile of " *nurse "* - on 05/03/2019 at 2:32 p.m. on 05/01/2021 at 2:34 p.m.

It is verified that the identity of this professional coincides with that identified by the complainant in his written complaint.

b) Certification of data protection training received on 05/04/2021 by this professional.

c) Certification issued by the Human Resources Department of the FAMT, attesting to the sanction that had been imposed on the (...)(...) in the context of the disciplinary proceedings initiated. Likewise, the Authority is also informed that the employee has been urged to repeat the data protection training.

5. On 28/07/2022 the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the FAMT for an alleged infringement provided for in article 83.5.a), in relation to the article 5.1.f); 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 07/29/2022.

6. 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.

7. On 02/09/2022 the FAMT made objections to the initiation agreement .

8. On 03/11/2022, the instructor of this procedure formulated a resolution proposal, by which she proposed that the director of the Catalan Data Protection Authority impose a fine of 2,000 on the FAMT (two thousand) euros as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1.f), both of the RGPD.

This resolution proposal was notified on 07/11/2022 and a period of 10 days was granted to formulate allegations.

9. On 11/15/2022 the accused entity paid 1,600 (one thousand six hundred) euros in advance.

10. On 21/11/2022, the FAMT presented a letter in which it set out the following:

- That *"the fine had been paid (...) taking advantage of the 20% reduction due to the fact of waiving any administrative action or appeal against the penalty, and for the voluntary payment by advance of this penalty, as provided for in art. 85.3 L39/15, which means that the penalty will be 1,600 (one thousand six hundred) euros""*.

- That *"it does not recognize the responsibility of the entity responsible for the treatment for how much security measures appropriate to the risk have been applied to the treatment".*

proven facts

A person with the profile of a nurse (...), who provided services at the Fundació Assistencianal de Mútua de Terrassa, accessed the medical history of the person reporting

here, without their consent, and without these accesses being related to any assistance or diagnostic action.

The 2 improper accesses carried out by this professional occurred on 05/03/2019 and 05/01/2021; and although the first of the accesses (03/05/2019) would already be prescribed, not so the last one (01/05/2021).

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 85.3 of the LPAC, the voluntary advanced payment of the proposed pecuniary penalty involves the application of a reduction. The effectiveness of this reduction is conditioned on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction and entails the termination of the procedure.

In this regard, it should be noted that the accused entity made objections to the initiation agreement and, as indicated in the background, has not made any objections to the proposal, relying on the option to reduce the amount of the penalty consisting of the voluntary advance payment of the pecuniary penalty, with the effects indicated above.

Having said that, it is considered appropriate to reiterate below the most relevant of the reasoned response that the instructing person gave to the allegations that the FAMT presented to the initiation agreement.

2.1. On the violation of the duty of confidentiality.

In its statement of objections to the initiation agreement, the FAMT linked the alleged facts to a possible violation of security measures (art. 32 RGPD) and, in order to distort the commission of this violation , related the set of technical and organizational measures implemented in his organization in order to comply with data protection regulations, highlighting those aimed at controlling access to the database of clinical histories, verification by third parties of the security measures applied (such as external audits), as well as those related to staff training. In this same line of defense, the FAMT emphasized that it adheres to the Code of Conduct of the Catalan Union of Hospitals and that it follows all the recommendations of this Standard Code.

As evidenced by the instructor in the resolution proposal, the penalty in this procedure is not the lack of implementation of security measures, but the fact that the confidentiality of the data has been violated, an obligation provided for in article 5.1.f) of the RGPD and 5 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD), and which has a different content to the obligations described in articles 25 and 32 of the RGPD, linked with security measures. In other words, one thing is the obligation of the person responsible or in charge of the treatment to implement the relevant technical and organizational measures in order to avoid the loss, destruction or accidental damage of the data or their improper treatment authorized or illegal;

and another is the duty of confidentiality incumbent on those in charge, in charge and all the people who provide service in their organizations in relation to the data subject to treatment. Therefore, a violation of the confidentiality of the data can occur, as is the case we are dealing with here, regardless of whether the person responsible or in charge of the treatment has implemented adequate security measures.

2.2. On the responsibility of the FAMT in the alleged events.

Secondly, in its written statement of objections to the initiation agreement, the imputed entity questioned the attribution of responsibility for the commission of an infringement for acts that would have materially carried out one of his employees - who, as part of the internal investigation launched by the FAMT, acknowledged having improperly accessed the complainant's medical history and apologized for their actions; and invoked in this sense the judgment of the Supreme Court no. 188/2022 of 02/15/2022, on which basis of third party law is pronounced in the following terms:

" *On security measures in the field of data protection and legal entities.*
The obligation to adopt the necessary measures to guarantee the security of personal data cannot be considered an obligation of result, which implies that in the event of a leak of personal data to a third party there is responsibility regardless of the measures adopted and the activity deployed by the responsible for the file or treatment (...).

In this regard, it must be said, first of all, that, as explained in the preceding legal basis, this procedure does not allege a violation of security measures, but of the duty of confidentiality.

Secondly, it should be noted that, in fact, according to FAMT's allegations, the commission of the offense charged here would be materially attributable to a specific person who provides services in its organization. However, according to what is provided for in the RGPD and particularly in article 70 of the LOPDGDD, the responsibility for breaches of the data protection regulations falls, among others, on those responsible or in charge of the treatments, and not about their employees. And in this regard, it is necessary to bring together the same judgment invoked by the FAMT (no. 188/2022), which is pronounced in the following terms:

Finally, it is appropriate to remember that legal entities are responsible for the actions of their employees or workers. An objective responsibility is therefore not established, but if the lack of diligence of its employees is transferable to the legal entity, in this sense STC 246/1991, of December 19 fj 2.
This Supreme Court in its STS nº 196/2020, of February 15, 2021 (rec. 1916/2020) has had the opportunity to address the responsibility of an Administration for breach of the duty of security of personal data by acts of employees. In it, the opinion of the Trial Chamber was shared when it affirmed that "[...] the responsibility of the Administration holding and in charge of the file [City Council of San Sebastián] cannot be excused in its diligent action, separately from the action of its employees or positions, but it is the "culpable" action of these, as a result of the violation of the aforementioned obligations to protect the reserved character of personal data that grounds the responsibility of the former in the sanctioning scope of whose application it is; by acts "own" by their employees or positions, not by third parties[...]". Adding further that "The above does not mean, of course, that we are projecting on the recurring City Council a principle of objective responsibility, nor that the principle of presumption of innocence is violated, nor that we give a lucky chance of inversion of the

burden of prueba. It simply happens that, being admitted in our Administrative Law, the direct responsibility of legal entities, which are recognized, therefore, as infringing capacity, the subjective element of the infringement is embodied in these cases in a different way to how it happens regarding of natural persons so that, as indicated by the constitutional doctrine that we have previously reviewed - SsTC STC 246/1991, of December 19 (FJ 2) and 129/2003, of June 30 (FJ 8) - direct blameworthiness derives of the legal property protected by the rule that is infringed and the need for said protection to be really effective and by the risk that, consequently, must be assumed by the legal entity that e is subject to compliance with said rule".

2.3 On the penalty to be imposed.

In the last section of its statement of objections to the initiation agreement, the FAMT called for the Authority, in the event that it considered that an infringement had been committed, to impose corrective measures in lieu of a fine administrative

The analysis on the imposition of a financial penalty, as well as the mitigating and aggravating ones that come together in the present case, will be carried out in the 4th legal basis.

In view of all the above, the allegations made by the FAMT in this procedure cannot succeed.

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, determining that personal data will be " *treated as such way to guarantee security data adequacy _ personal , including the protection against unauthorized or illegal treatment and against it loss , destruction or accidental damage , through the application of measures technical or organizational appropriate ".*

On the other hand, the LOPDGDD, establishes the following in its article 5, relating to the duty of confidentiality:

> *"1. Those responsible and in charge of data processing as well as all the people who intervene in any phase thereof are subject to the duty of confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.*
> *2. The general obligation indicated in the previous section is complementary to the duties of professional secrecy in accordance with its applicable regulations (...)"*

During the processing of this procedure, the fact described in the proven facts section, which is considered constitutive of the violation provided for in article 83.5.a) of the RGPD, which typifies the violation of *" the principles básicos para el tratamiento ",* among which the principle of confidentiality is at the top.

The conduct addressed here has been included as a very serious infraction in article 72.i) of the LOPDGDD, in the following form:

> *"i) The violation of the duty of confidentiality established by article 5 of this Organic Law"*

4. As the FAMT does not fit into any of the subjects provided for in article 77.1 of the LOPDGDD , the general sanctioning regime provided for in article 83 of the GDPR applies.

Article 83.5 of the RGPD provides for the infractions provided for there, they are sanctioned with an administrative fine of 20,000,000 euros at most, or in the case of a company, an amount equivalent to 4% as maximum of the overall total annual business volume of the previous financial year, opting for the higher amount.

As has been advanced, the FAMT advocated the substitution of the administrative fine sanction for the imposition of corrective measures.

In the present case, as explained by the instructor in the resolution proposal, this possibility provided for in article 58.2.d) of the RGPD should be ruled out since, as will be seen, the nature of the imputed facts makes the imposition of measures In this same line, the imposition of a warning in lieu of a financial penalty is also not appropriate, an eventuality that is also provided for in letter b) of the same precept, and this because it is considered that the violation of the principle of confidentiality with respect to data of special protection (health data) affects the most intimate and private sphere of people.

Having said that, it is necessary to determine the amount of the administrative fine to be imposed. According to the provisions of article 83.2 of the RGPD, and also in accordance with the principle of proportionality enshrined in article 29 of Law 40/2015, as indicated by the instructor in the resolution proposal, the sanction should be imposed of 2,000 (two thousand) euros. This quantification of the fine is based on the weighting between the aggravating and mitigating criteria indicated below.

On the one hand, we appreciate the following circumstances that operate as mitigating criteria:

- The limited number of accesses over time (art. 83.2.a/ RGPD and 76.2.a/ LOPDGDD)
- Lack of intentionality (art. 83.2.b RGPD).
- The degree of responsibility of the person in charge or of the person in charge of the treatment, taking into account the technical or organizational measures that have been applied under the provisions of articles 25 and 32 of the RGPD (art.83.2.c RGPD).
- FAMT's adherence to the code of conduct of the Unió Catalana d'Hospitals (art. 83.2.j RGPD).
- The lack of benefits obtained as a result of the commission of the offense (art. 83.2.k RGPD and art. 76.2.c LOPDGDD).
- The initiation by the FAMT, as soon as it became aware of the improper access carried out by one of its employees, of a disciplinary procedure in order to clear any responsibilities (art. 83.2.k RGPD).

On the contrary, as aggravating criteria, the following elements must be taken into account :

- Damage or damages caused. Access to a person's health data, without their consent and without legal authorization, is in itself a detriment to the affected person, since it is data that, as has been said before, affects the most intimate and private sphere of people (83.2.a of the RGPD).

- The previous offenses committed. It should be noted that the FAMT has previously been sanctioned by this Authority -PS 28/2012, PS 13/2020, PS 27/2020, PS 50/2020, PS 45/2021-.
- The linking of FAMT's activity with the processing of personal data (art. 83.2.k/ of the RGPD and 76.2.b/ of the LOPDGDD).

5. On the other hand, in accordance with article 85.3 of the LPAC and as stated in the initiation agreement, if before the resolution of the sanctioning procedure the accused entity acknowledges its responsibility or does the voluntary payment of the pecuniary penalty, a 20% reduction must be applied on the amount of the provisionally quantified penalty. If the two aforementioned cases occur, the reduction is applied cumulatively (40%).

As has been advanced, the effectiveness of the aforementioned reductions is conditional on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction (art. 85.3 of the LPAC, in *fine)* .

Well, as indicated in the antecedents, the accused entity has paid 1,600 (one thousand six hundred) euros in advance, corresponding to the amount of the penalty resulting once the 20% reduction has been applied.

6. Given the findings of the violations provided for in art. 83 of the RGPD in relation to privately owned files or treatments, article 21.3 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, empowers the director of the Authority for the resolution declaring the infringement to establish the appropriate measures so that its effects cease or are corrected. However, as indicated by the instructor in the resolution proposal, in the present case no measure should be required to stop or correct the effects of the infringement, given that it is an isolated and specific event, with which would have consummated the effects of the infringement.

For all this, I resolve:

1. To impose on the Mutual Aid Foundation of Terrassa the sanction consisting of a fine of 2,000 (two thousand) euros, as responsible for an infringement provided for in article 83.5.a) of in relation to article 5.1.f), 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 6th legal basis.

2. Declare that the Fundació Assistencial Mútua de Terrassa has made the advanced payment of 1,600 (one thousand six hundred) euros, which corresponds to the total amount of the penalty imposed, once the percentage of deduction of 20% corresponding to the reduction has been applied of the voluntary advanced payment provided for in article 85 of the LPAC.

3. Notify this resolution to the Mutual Assistance Foundation of Terrassa.

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,